

D.E.P.A.R.T.

Digital education

Guide for parents



Co-funded by
the European Union

Developed by the SMART EDUCATIONAL PROJECTS Association, VISION TREE and ESSENIA within the Erasmus+ DEPART project – Digital education for parents at risk of technological exclusion

Erasmus+ Programme – Strategic Partnership

Project No. 2025-1-RO01-KA220-ADU-000353764 (DEPART)

Project coordinated by: SMART EDUCATIONAL PROJECTS Association



<https://departproject.eu/>

Partnerships



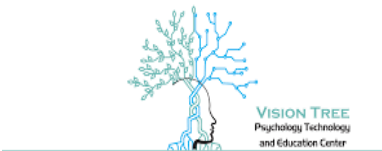
<https://www.sep-ngo.eu/>



<https://www.esseniauetp.it/>



<https://danmar-computers.com.pl/>



<https://visiontree.be/>



<https://www.erasmuspluscourses.com/>

“The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the National Agency and Commission cannot be held responsible for any use which may be made of the information contained therein”.

TABLE OF CONTENTS

Introduction	6
How to use this guide	7
CHAPTER I	9
1. Information and data literacy	9
1.1 What is information literacy	9
1.2 The role of information in everyday life	10
1.3 Types of information in the online environment	12
1.4 Challenges of the digital information environment	16
2. Search for information on the internet	20
2.1 Search engines	21
2.2 Use of keywords.....	23
2.3 Searching for information using artificial intelligence	24
2.4 Analyzing search results.....	26
3. Storage and management of information.....	28
3.1. Saving information.....	28
3.2. Organization of digital files: folders and document naming	31
4. Utility Apps – Digital Tools for Everyday Life	33
4.1. Categories of Frequently Used Utility Applications	34
4.2. Use of utility applications in daily activities.....	35
4.3. Safe use of apps	36
5. Use of videoconferencing services	38
5.1 What is a video conference	38
5.2 Video conferencing platforms	39
5.3 How we participate in an online meeting	39
5.4 Basic rules for participating in video conferences	40
6. Online shopping.....	42
6.1 What is online shopping	42
6.2 Online Shopping Platforms.....	43
6.3 Advantages of online shopping.....	44
6.4 Safety of online shopping	44
7. Online games, betting, and associated risks	46
7.1 Online games and child safety.....	46
7.2. Risks of online betting for children and teenagers	49
8. Disinformation online	53
8.1. What is disinformation	53
8.2. How we recognize fake news	55
8.3. Strategies to counter disinformation	58
Recap: the main ideas of the chapter	60
How can we use this knowledge in everyday life	61

Quick Self-Assessment Test	62
CHAPTER II.....	64
1. Effective communication in the online environment	64
1.1 What is online communication	64
1.2 Forms of online communication	65
Synchronous communication (real-time).....	65
Asynchronous communication (not in real time)	65
1.3 Choosing the right communication tool	66
1.4 Communication etiquette in the digital world.....	67
1.5 Managing conflict and disagreements online	68
1.6 Communicating with schools and teachers digitally	69
1.7 Using emojis and media effectively.....	69
1.8 The importance of digital accessibility	70
2. Social networks: what they are, how they work and their usefulness	72
2.1 What are social networks	72
2.2 How social networks work	73
2.3 Benefits of social networks	74
2.4 Risks and challenges of social networks	74
2.4.1 Privacy risks	74
2.4.2 Misinformation	77
2.4.3 Cyberbullying.....	80
2.4.4 Comparison and self-esteem issues	84
2.4.5 Time consumption	87
2.4.6 Exposure to inappropriate content	90
2.4.7 Summary: Risks at a glance	93
3. Social media profiles	95
3.1 What is a social media profile	95
3.2 What information is included in a profile	95
3.3 Public vs. private profiles.....	95
3.4 Managing and updating your profile.....	96
3.5 Guiding your child's first profile.....	97
3.5.1 5 finger tools for strong standing for CyberHealth	98
3.6 Fake accounts, bots and impersonation	100
3.7 Online image and reputation management.....	101
3.8 Advanced profile security	102
3.9 Platform-specific profile differences.....	104
4. Digital footprint	106
4.1 What is a digital footprint	106
4.2 Why does your digital footprint matter	106
4.3 Managing your digital footprint.....	107
4.4 Your children's digital footprint.....	107

4.5 The persistence and permanence of the footprint.....	108
4.6 The footprint and future opportunities	109
4.7 Auditing and cleaning up old footprints	110
4.8 Digital shadows: the footprint left by others	111
5. Social media addiction	113
5.1 What is social media addiction	113
5.2 Signs of excessive social media use	113
5.3 The psychology behind social media engagement	113
5.4 Effects on parents and family life.....	114
5.5 Children and social media addiction	114
5.6 Strategies for healthier social media habits	115
For parents.....	115
For families.....	115
5.7 Social media, blue light and sleep deprivation	116
5.8 Assessing dependency: the difference between habit and addiction	117
5.9 Implementing a family digital detox.....	118
5.10 When and how to seek professional help	119
6. Digital parenting: guiding your child’s online communication.....	120
6.1 Why digital parenting matters	120
6.2 Talking to your children about online communication	120
6.3 Setting boundaries together	121
6.4 Parental control tools.....	121
6.5 Creating a safe zone for disclosure	122
6.6 The “monitoring vs. trust” dilemma	123
6.7 Handling online stranger danger.....	124
6.8 Teaching digital empathy and kindness.....	126
6.9 Building digital resilience and critical thinking	127
Recap: the main ideas of the chapter	129
Quick Self-Assessment Test	130
How can we use this knowledge in everyday life	132
CHAPTER III.....	133
1. Antivirus software – necessity or fad	133
1.1 What is an antivirus and how it works.....	134
1.2 Common myths: “I don’t need it if I’m careful”.....	138
1.3 Built-in security vs. third-party software	142
1.4 Mobile security: protecting smartphones and tablets	144
1.5 Keeping system software updated: the first line of defence	147
2. The importance of passwords in securing accounts	150
2.1 Anatomy of a strong password	151
2.2 The risks of password reuse across multiple sites	153
2.3 2FA and MFA: The essential layers of security.....	156

2.4 Digital Vaults and Passkeys: Management without the memory load	159
2.5 Teaching children how to create and hide their “secret keys”	163
3. Protecting your family’s online data	166
3.1 Personal Data: What it is, How it is Collected and Why it Matters	167
3.2 Phishing and Social Engineering: how hackers “trick” families	172
3.3 Public Wi-Fi risks and the use of VPNs	175
3.4 Privacy on the Internet, in the Cloud and on Connected Home Devices	179
3.5 Recognizing secure websites (HTTPS vs. HTTP)	186
4: Internet usage control for parents and children	189
4.1 Establishing a family digital understanding	190
4.2 Parental Controls within the European Regulatory Landscape	193
4.3 Monitoring vs. Spying: finding the right balance of trust	199
4.4 Managing screen time across different ages	203
4.5 Leading by example: parental digital habits	205
5. Risks for minors on the Internet	208
5.1 Cyberbullying and online harassment	209
5.2 Grooming: recognizing the signs of “stranger danger” 2.0	214
5.3 Inappropriate content, algorithmic rabbit holes, and radicalization vectors	218
5.4 Predatory architecture: dark patterns and behavioural manipulation in gaming ecosystems	223
5.5 Building digital resilience: what to do when something goes wrong	225
6. Recap: the main ideas of the chapter	229
7. Quick Self-Assessment Test	230
8. How can we use this knowledge in everyday life	232
8.1 Technical Glossary of Family Digital Safety	232
Letter A	232
Letter B	232
Letter C	233
Letter D	234
Letter E	234
Letter F	235
Letter G	235
Letter H	235
Letter I	236
Letter K	236
Letter M	236
Letter P	237
Letter Q	237
Letter R	238
Letter S	238
Letter T	239

Letter V.....	239
Letter W.....	240
Letter Z.....	240
Bibliography	241
Chapter I	241
Chapter II	243
Chapter III	245

Introduction

Digital technology is part of the daily lives of many families. The internet is used to find information, communicate, participate in educational activities, or access various online services. At the same time, the use of technology can sometimes raise questions or difficulties, especially for parents who want to support their children in the responsible use of the digital environment.

This guide was created as part of the Erasmus+ project DEPART – Digital Education for Parents at Risk of Technology Exclusion (Project No. 2025-1-RO01-KA220-ADU-000353764), funded under the Erasmus+ Programme, KA220 – Cooperation Partnerships in Adult Education, to help parents develop the digital skills needed to use the internet and online applications safely, effectively, and responsibly.

The guide's content is based on the European DigComp framework – the Digital Competence Framework for Citizens. The guide is divided into three main chapters, developed by the DEPART project partners:

- **Chapter I – Information literacy and the use of online services**, developed by SMART EDUCATIONAL PROJECTS Association (Romania), the project coordinator;
- **Chapter II – Communication and collaboration in the online environment**, developed by Vision Tree – Centre for Psychology and Technology Education (Brussels, Belgium);
- **Chapter III – Digital security for the family**, developed by Essenia UETP - University and Enterprise Training Partnership s.r.l. (Salerno, Italy).

This guide can be used both individually by parents as informational material, and in educational activities or training workshops. By going through this material, readers can gain the knowledge and skills to use technology with more confidence and to support their children in the responsible use of the digital environment.

How to use this guide

This guide has been designed to be easy for parents to go through and use. Each chapter includes simple explanations, everyday-life examples, and hands-on activities to help readers better understand how the digital environment works.

To make reading and learning easier, the guide uses several types of boxes and icons to highlight important information.

 **Tip.** This icon marks helpful recommendations that can help you use technology more efficiently and safely.

 **Activity.** The sections marked with this icon include simple exercises that help readers reflect on their own experience or apply the information presented.

 **Step-by-step guide.** This icon indicates structured explanations that show the steps required to perform an action, such as attending an online meeting or making an online purchase.

 **Attention:** This icon highlights situations in which it is important to be more cautious when using the internet or digital applications.

Readers can go through the guide in its entirety or consult only the chapters that interest them. The proposed activities can be carried out individually or in training workshops dedicated to parents.

 **Note for the reader:** This guide can be used in two ways:

- **As a parent reading on your own:** you can go through the chapters that interest you, at your own pace. The activities can be tried individually, as a family, or together with other parents.
- **As a participant in an organized workshop:** the same content is covered together with a trainer, as part of the DEPART project's workshops. Trainers have a separate Methodological Guide (available on the project platform), which proposes two 3-hour workshops to cover this chapter in full.

- **For trainers:** if you are delivering this material in a workshop, we recommend distributing a printed copy of this guide (Part I) to participants and using the Methodological Guide (Part II) in parallel. The two documents are complementary: this guide provides the content, the Methodological Guide provides the facilitation script.

CHAPTER I

1. Information and data literacy

1.1 What is information literacy

Today we use the internet almost every day. We are looking for information about schools, health, public services, or children's activities. Many times, when we have a question, the first thing we do is look it up on the internet.

The internet gives us access to a lot of information. In a few seconds, we can find articles, videos, or explanations on almost any topic.

However, not all information on the internet is accurate or reliable. Some may be incomplete, outdated, or even false. That is why it is important to know **how to find information and verify its accuracy**.

These skills are part of what we call **information literacy**.

In short, information literacy means knowing:

- where to look for information;
- how to find the information we need;
- how to verify that the information is correct;
- how to use information in everyday life.

These skills are useful for everyone who uses the internet. For parents, they are especially important when looking for information about their children's education or activities.

Why is information literacy important?

If we know how to use information on the internet correctly, we can:

- find the information we need faster;
- avoid false or misleading information;
- make better decisions for ourselves and our family;
- use the internet in a safer way.

✓ Signs that we are using information on the internet correctly

We use online information correctly when:

- we do not immediately believe everything we read
- we verify the information in several places
- we choose sites that seem serious and trustworthy
- we ask ourselves questions when something seems unclear or exaggerated
- we think about whether the information is useful for our needs

Example from everyday life

A parent is seeking information about a kids' camp. They go online and come across several websites offering various details.

To make a good decision, the parent compares information from multiple sources and verifies their trustworthiness.

Activity

Think of a recent situation in which you searched for information online.

Answer the following questions:

1. What information have you been looking for?
2. Where did you look for this information?
3. How did you choose the information that you considered correct?

1.2 The role of information in everyday life

In everyday life, we need information to make decisions and solve different problems. In the past, information was mostly found in books, newspapers or public institutions.

Today things have changed. The Internet allows us to find information very quickly, using our mobile phone, tablet or computer.

We can search for information using:

- search engines;
- online apps and platforms;
- AI-powered tools.

Through the internet we can find information about:

- children's school activities;
- educational programs or courses;
- public services or institutions;
- health and lifestyle;
- different products or services.

The internet can help us quickly find answers to many questions. However, we must bear in mind that not all information is accurate or verified.

Sometimes we can find incomplete or outdated information. That's why it's important to compare information from multiple sources.

Why is access to information important?

Access to information helps us to:

- make better-informed decisions;
- learn new things;
- find solutions to the problems of everyday life;
- use technology more efficiently.

When the internet helps us in our daily lives

The Internet can help us when we want to:

- find out the program of an institution;
- find information about the child's school;
- look for a doctor or a pharmacy;
- compare products before buying;
- find ideas for educational activities;
- participate in an online meeting.

Example from everyday life

A parent searches the internet and finds several websites with different information.

To choose the right option, the parent compares the available information, checks the program organizers, and reads the opinions of other participants.

Activity

Think of a recent situation where you used the internet to find information.

1. What information have you been looking for?
2. What tool did you use (phone, computer, app)?
3. How did you verify that the information is correct?

1.3 Types of information in the online environment

On the internet, we can find information in many different forms. Not all information is presented only in text form. Sometimes we find images, videos, or interactive applications that help us understand a topic more easily.

For example, when we want to learn something new, we can read an article, but we can also watch a video or a step-by-step explanation.

In the online environment, information most often appears in the following forms:

Information in text format

This is the most common information on the internet. We find them in the form:

- articles on websites;
- online news;
- guides and explanations;
- blogs or information pages.

This type of information is useful when we want to read more detailed explanations about a topic.

Visual information

Some information is presented through images or graphs. They help us understand certain things more easily.

Examples of visual information:

- photos;
- maps;
- graphs;
- infographics.

For example, navigation apps use maps to show us the route to a specific destination.

Video or audio information

On the internet, we find a lot of videos or audio recordings. They are useful when we want to see or hear explanations about a specific topic.

Example:

- *video tutorials;*
- *online courses;*
- *presentations;*
- *podcasts.*

Sometimes it's easier to learn something by watching a video than by reading a long text.

Interactive information

Some websites or apps allow us to interact directly with information. For example, we can fill out online forms or use educational applications or tools to help us calculate or plan different activities.

These tools help us use information more actively.

Why is it important to understand the types of information online?

If we know in what form information appears on the internet, it is easier for us to:

- we find the information we need;
- we choose the way that seems easiest to understand;
- we use digital resources more efficiently.

How to choose the type of information that suits us

Not all of us learn in the same way. Sometimes:

- a **text** is useful when we want more detailed explanations;
- an **image** helps us quickly understand a piece of information;
- a **video** is best suited when we want to see the concrete steps.
- an **interactive app** is useful for practicing.

It is good to choose the form of information that is easier for us to understand.

If we want to...**We can use...**

To understand a detailed explanation text

Let's see how something is done Video

We quickly find a location Map

We fill out an application Online form

 Example from everyday life

A parent wants to learn how to use an app for video conferencing.

On the internet, you can find:

- An article explaining the steps.
- A video showing how to use the app.
- An image with the main functions.

By combining this information, the parent can more easily understand how the application works.

 Activity

Think of a situation where you learned something using the internet.

1. Have you read an article?
2. Watched a video?
3. Have you used an app?

Which of these methods helped you most in understanding the information?

The difference between information, opinion, and advertising

On the internet, we can come across several types of content. Sometimes they can be confused, and this can make it more difficult to understand the information.

That is why it is useful to know the difference between **information, opinion and advertising**.

Information

The information is based on verifiable data or facts.

Example:

An institution's schedule, information about a course, or details about a public service.

Opinion

Opinion is a person's point of view.

Example:

Someone may write in an article that a certain app is very good or that a certain product is useful for children. This is an opinion, not necessarily a verified fact.

Advertisement

Advertising is content created to promote a product or service.

Examples of advertisements can be:

- *sponsored ads*
- *product recommendations;*
- *promotional items*

Covert advertising – sponsored content by influencers, paid partnerships, and branded content that looks like regular posts or recommendations. This is the most problematic type, as children and teenagers often do not recognise it as advertising

It is important to recognize these differences in order to better understand the information we read online.

Activity

Look at three examples of online content (article, post, or advertisement).

Try to identify:

- which is fact-based information;
- which represents an opinion;
- which is an advertisement.

How did you realize the difference?

1.4 Challenges of the digital information environment

The Internet gives us quick access to a lot of information. This is a great advantage, but it can also bring some difficulties.

Sometimes it's hard to choose the information that is really useful or accurate. There is a lot of content on the internet, and not all information is verified.

That's why it's important to learn how to use information responsibly.

Too much information

When we search for something on the internet, we can sometimes find hundreds or even thousands of results. This can be confusing.

For example, if we search for information about an educational app, we can find different articles, advertisements, videos, and opinions.

In such situations, we must choose the information that seems most relevant.

Different sources of information

On the internet, they can publish information:

- official institutions;
- organisations;
- companies;
- individuals.

Not all of these sources have the same level of credibility. That is why it is important to check who published the information.

False or misleading information

Sometimes, false information can appear on the internet or be presented in a way that can be misleading.

This information can be quickly shared on social networks or on different websites.

That's why it's important to verify information before believing or sharing it.

⚠ Common challenges when using the internet

On the internet we can face:

- too much information on the same topic;
- sites that are not trustworthy;
- incomplete or outdated information;
- false or exaggerated information.

The development of digital skills helps us to better manage these situations.

✓ Checklist: How to check information on the internet

Before we believe or share information, it is good to check a few things:

- Who published the information? Is the author identified and do they have relevant expertise or credentials?
- Does the site seem serious and trustworthy?
- Does the article have a publication date?
- Does the information appear on other sites?
- Does the title seem exaggerated or alarming?
- Does the site contain excessive advertisements, pop-ups or promotional content that seems designed to sell rather than inform?

If the answer to several questions is "no", it is good to be careful and look for additional information.

Example from everyday life

A parent is looking for information about an educational app for kids.

After searching, a lot of results appear: articles, blogs, videos and advertisements.

Some sites present the app in a very positive way, and others offer critical opinions. To better understand the situation, the parent compares the information from several sources and checks if it comes from trusted sites.

Activity

Search online for a specific topic that is relevant to your family (for example: "best summer camps for children aged 8-12" or "symptoms of a cold vs. flu in children") where you searched for information on the internet and found a lot of results.

1. Which information did you find most useful and why? What made you trust one source more than another?
2. Check the source: how did you verify that the information was reliable? Did you check who published it, when, and whether other sources confirmed it?
3. What difficulties did you encounter?



5 Important Things About Internet Information

When searching the internet for information, it's good to keep a few simple things in mind.

✓ **Not all information on the internet is accurate.**

Anyone can publish information online, and sometimes it can be incomplete or wrong.

✓ **It is good to check the information from several sources.**

If the same information appears on more than one trusted site, it is more likely to be correct.

✓ **The first search results are not always the best.**

Sometimes these can be advertisements or promoted pages. Keep in mind: the very first result on Google is now usually an AI-generated summary, followed by sponsored (paid) content, and then suggested searches. Scroll down to find organic, independent results.

✓ **Very dramatic headlines can be misleading.**

Some sites use exaggerated headlines to grab attention. Examples: "5 ways to boost your confidence in 1 week", "Doctors don't want you to know this!", "You won't believe what happened next!".

✓ **It is good to talk to children about the information found online.**

This way, we can help them learn to use the internet in a responsible way.



Reflection exercise for parents: How do we use the internet?

Think about how you use the internet in your daily life.

Check the situations that suit you:

- I'm looking for information about the school or activities for children.
- Sometimes it's hard for me to choose between multiple sites.
- I happened to find contradictory information.

- I prefer videos over long texts.
- Sometimes I'm not sure if a piece of information is correct.

If you have ticked off one or more situations, it means that developing information literacy skills can help you use the internet more effectively.

The rule of 3 checks

To quickly verify information found on the internet, we can use three simple questions:

1) **Who published the information?**

Is it an official website or an unknown source?

2) **When was the information published?**

Some information may be old and no longer current.

3) **Does it appear on other trusted sites?**

Apply the 5-Finger Rule: look for at least 5 independent sources that confirm the information. If the same information appears in more than one credible source, it is more likely to be correct.

This check only takes a few minutes and can avoid a lot of confusion.

Activity

Search for "outdoor activities for children aged 10-16 in winter" and find at least one article or post about it.

Apply the rule of 3 checks:

1. Who published the information?
2. When was it published?
3. Does it appear on other sites as well?

What conclusion did you draw from this information?

2. Search for information on the internet

In everyday life, we use the internet to find information about many things, such as children's activities, schools, health, public services, and products.

When searching the internet for information, it is important to know that not all results are the same. Some results are informative articles, others are pages of institutions or organizations, and some are paid advertisements, and AI-generated summaries.

For this reason, it is useful to learn a few simple things about how the internet search works and how we can identify the most useful information.

Usually, to find the information we want, we use **search engines** or **tools based on artificial intelligence**.

These tools help us find information quickly. However, to get good results, we need to know **how to formulate a search correctly and how to choose useful information**.

2.1 Search engines

Search engines are tools that help us find information on the internet.

One of the most well-known search engines is Google Search, but there are other widely used search engines as well, such as Microsoft Bing, DuckDuckGo (which does not track your searches), and Brave Search. Each works differently and may show different results.

When we enter a word or phrase into a search engine, it analyzes millions of web pages and shows us the results that seem the most relevant.

Search engines use automated programs that analyze millions of web pages. These programs try to identify pages that contain information relevant to the words entered by the user.

The results are then sorted into a list. Usually, the first results are considered the most relevant to that search. However, this does not always mean that they are the most complete or the most reliable.

For this reason, it is useful to open up more results and compare the information.

Results may now include an AI Overview (an AI-generated summary at the very top of the page), followed by:

- web pages with information;
- news articles;
- images;
- videos.
- maps;
- advertisements for products or services.

How an internet search works

When we search for something on the internet:

1. we enter a word or phrase into the search engine, or we type a question into an AI-powered chatbot (such as ChatGPT, Google Gemini, or Microsoft Copilot);
2. the search engine searches for relevant pages;
3. we are shown a list of results.

Usually, the first results are considered the most relevant to our search.

The difference between organic results and ads

When we use a search engine, the results shown may come from different sources.

Some results are **organic results**, and others are **paid ads**.

Organic results

Organic results are web pages that the search engine considers relevant to the search query.

These may include:

- Informative articles
- Institutions' websites
- Educational Pages
- Blogs or guides

Advertisements

Some results are paid by companies or organizations to appear at the top of the page (note: these now typically appear below the AI-generated summary at the top, but above the organic results) .

These results are usually marked with mentions such as:

- "Ad"
- "Sponsored"

The presence of an advertisement does not necessarily mean that the information is wrong. However, it is important to know that these pages appear in the top positions because they are promoted through advertising.

That is why it is good to analyze several results before choosing a source of information.

💡 Understanding the AI Overview (AI Summary)

Since 2024, Google and other search engines have added an "AI Overview" – a summary generated by artificial intelligence that appears at the very top of search results. While this can be useful for quick answers, it is important to know that: (1) AI summaries can contain errors; (2) they do not always include sources you can verify; (3) they are not written by a human expert. Always scroll down to read the original articles and check the actual sources.

Activity

Do an internet search for: "educational activities for children".

Notice the first results.

Try to identify:

- Which results are ads.
- which are organic results.

How did you figure it out?

How to search for information on the internet – step by step

If we want to find information online, we can follow a few simple steps.

Step 1. We open the browser on our phone or computer.

Step 2. We access a search engine (e.g. Google).

Step 3. We introduce a few words that describe what we are looking for.

Step 4. We analyze the first results displayed.

Step 5. We open 2–3 different sites to compare information.

 It's good not to rely on just one site. Comparing multiple sources helps us better understand the information.

2.2 Use of keywords

To find the information you want, it's important to use **the right keywords**.

Keywords are the words or phrases that we enter into a search engine.

Example

General search: "activities for kids."

More specific search: "educational activities for 10-year-olds."

The clearer the search, the more relevant the results will be.

Tips for a more efficient search

- Use simple, clear words.
- Add important details (e.g. your child's age)
- Try several search options.

Examples of more efficient searches

Sometimes the search results depend a lot on how we phrase the question.

General Search

Clearer search

Activities for children	Educational activities for children 8 years old
Doctors	pediatrician in Paris
Children's Games	Online Educational Games for Kids

- The clearer the words we use, the more suitable the search engine can offer us results.

Sometimes it's helpful to rephrase your search if the results aren't very relevant.

For example, if a search produces too many general results, we can add additional details, such as:

- *Child's age*
- *the city or area where we live*
- *the type of activity or service you are looking for*

Using more specific terms, the search engine can provide results closer to what we are looking for.

2.3 Searching for information using artificial intelligence

In addition to search engines, we can also find information using **artificial** intelligence-based tools. Social media platforms like YouTube, TikTok, and Instagram are also widely used to find information, though these prioritise engaging content over verified accuracy.

These apps work like digital assistants. We can ask them questions, and they try to give a clear and short answer.

Examples of such tools include:

- ChatGPT
- Microsoft Copilot
- Google Gemini

These tools can be useful when we want to:

- quickly understand a topic;
- receive simple explanations;
- find ideas or suggestions.

⚠ Caution

Sometimes AI tools can provide incomplete or wrong information. That's why it's good to check the information on other sites as well. Also, if you need to share personal or sensitive information while using AI tools, consider using a paid subscription (not necessarily the most expensive plan), as paid plans typically offer stronger privacy protections than free versions.

Examples of questions we can ask an AI assistant

AI-powered tools can be handy when we need simple explanations or ideas. ⚠ Important: never share sensitive personal information with AI tools (such as your medical details, home address, financial information, or personal identification numbers).

For example, we can ask:

- "What educational activities are suitable for 10-year-olds?"
- "How can I help my child learn better for exams?"
- "What are the advantages of reading for children?"

These tools can provide quick explanations, but it's good to check the information on other sites as well.

AI-based tools can be especially useful when we want simple explanations or general ideas about a topic.

However, these systems generate responses based on information available online and cannot always guarantee absolute accuracy.

For this reason, when using such tools for important topics, it is good to check the information in other sources as well.

2.4 Analyzing search results

After doing an internet search, it is important to analyze the results.

Not all sites offer reliable information. That's why we need to check a few things:

- who published the information;
- Whether the site belongs to an institution or organization.
- when the information was published;
- if the information appears on other sites.

✓ How to recognize a trusted site

When reading information on the internet, it is good to check a few simple things:

- the site belongs to a known institution or organization;
- the article has an author and a date of publication;
- the site uses a secure connection – look for "https://" at the start of the web address and a padlock icon in the browser bar; you can also click the padlock to view the site's digital certificate and check who owns the domain;
- the information is presented clearly and substantiated (there is a link to a study, a research paper, an official report, or another credible source that supports the information presented);
- The site doesn't contain a lot of ads or exaggerated headlines.

If a site seems unreliable or contains conflicting information, it's a good idea to check other sources as well.

Sometimes it is also useful to observe the way the information is presented.

Trusted sites usually offer:

- clear and balanced explanations
- author or organization information
- sources or references for the information presented

On the other hand, less credible sites may have:

- very dramatic titles and clickbait headlines (e.g. "Incredible news: Chocolate is more dangerous than cigarettes!", "One thing no one is telling you about weight loss", "Doctors HATE this simple trick!")
- many advertisements or pop-ups
- incomplete or difficult to verify information

Observing these elements can help us choose the most appropriate sources.

Example from everyday life

A parent wants to find information about an educational platform for children.

After entering the keywords into the search engine, several results appear: articles, videos, and advertisements.

To choose the right information, the parent checks several sites and compares the information.

Activity

Search the internet for information about an educational activity for children.

Answer the following questions:

1. What keywords did you use?
2. What types of results appeared (articles, images, videos)?
3. How did you choose the sites that you find useful?

Common mistakes when looking for information on the internet

When we use the internet to search for information, it is normal to sometimes encounter difficulties.

Here are some common mistakes:

- Read only the first result in the search list, or relying only on the AI-generated summary, or clicking on the first sponsored/paid result
- Relying only on the title of an article
- Sharing information without source verification
- Using keywords that are too general

To avoid these situations, it is helpful to read the information carefully and compare at least 5 independent sources before drawing a conclusion.

Activity

Search the internet for information about an educational activity for children.

Try answering the following questions:

- What keywords did you use?
- What types of results appeared (articles, videos, ads)?
- Which sites did you find the most useful?

Discuss or write down what was easy and what was more difficult during the search.

3. Storage and management of information

3.1. Saving information

In our daily lives, we use more and more digital information: documents, photos, videos, messages, and work files. Sometimes we don't even realize how important this data is until we lose it. For this reason, it is very useful to know how we can save information correctly and safely. There are several methods we can use to keep the data so we can use it in the future.

Saving information directly to our computer or laptop is the most common storage method. When we create a document or download a photo, it is saved to the device's internal memory. Typically, our computer uses a hard disk drive (HDD) or SSD to store our files. The advantage of this method is simplicity: files are easy to find and can be opened quickly. However, there is also a risk. If our device breaks down or is infected with a virus, our information may be lost.

Storing data on external storage devices.

- Among the best known are ***USB sticks and memory cards***. They are small, easy to carry, and can hold a large amount of information. For example, we can copy important photos, work documents, or personal projects to a stick. Thus, if we need to use these files on another computer, we can quickly move them.
- Another method is to use ***external hard drives***. They resemble our computer's internal memory, but they are separate devices that connect via USB cable. External hard drives can store large amounts of data and are often used to archive important information, such as collections of

photos, videos, or documents. Note: any external device can be damaged, lost or stolen. For critical files, keep a second backup copy on a different device or in cloud storage.

- Some people also use **optical discs**, such as CDs or DVDs. Although they are no longer as popular as they once were, they can still be useful for retaining information in the long run. For example, family photos or important documents can be saved to a DVD and kept in a safe place.

Cloud storage is increasingly prevalent. Today we use our phone, computer or tablet more and more often to keep photos, documents, videos or different files. Sometimes, however, the device's memory fills up or there is a risk of losing information if technical problems occur. For this reason, a modern solution called **cloud storage has emerged**.

Cloud storage means that files are not only saved on our phone or computer, but also on the internet, on special servers. Basically, the information is kept in an online space. To use this service, we create an account and can upload different files there. After that, they can be opened at any time, from almost any device connected to the internet.

There are several services that offer cloud storage. Among the most well-known are **Google Drive** and **Dropbox**. These platforms allow us to save files online, organize them into folders, and access them from different devices. For example, a photo taken with our phone can be automatically uploaded to our Google Drive or Dropbox account and then viewed on our computer or tablet.

A big **advantage of the cloud is easy access to information**. If we save a document in the cloud from our home computer, we can also open it later from our phone or another computer. This is very useful for people who work in several places or for those who want to always have important documents at hand.

Another advantage is that **we no longer take up the memory space of the phone or computer**. Often, photos or videos take up a lot of space. If we save them in the cloud, the device remains freer and can work better. In addition, many services offer us a certain amount of space for free, and if we need more space we can choose a paid subscription.

The cloud is also useful for **keeping information safe**. Some apps can automatically save important photos or documents to the online space. If our phone gets lost or our computer crashes, our files don't go away. They can be easily recovered by logging into our personal account.

Another benefit is *easier collaboration between people*. For example, multiple people can work on the same document, each adding information or making changes. This is useful at work and in other situations where people need to work together.

Although cloud storage offers many benefits, it also presents *certain risks*. One of these is related to **data security**: since files are stored online, unauthorized individuals could try to access our account. That's why it's crucial to use strong passwords and avoid sharing them with others.

Another possible drawback is the need for an internet connection.. To upload or download files from the cloud, we need an internet connection. If we don't have internet access or it is very slow, using the cloud can become more difficult.

Sometimes, technical problems with online services *can also occur*. While these situations are rare, platforms may have bugs or maintenance periods, and access to files may be temporarily limited.

To use the cloud safely, it is good to follow a few simple rules. First of all, we must use strong passwords and not share them with other people. Secondly, it is good to keep copies of our most important files on other devices, such as a USB stick or external hard drive.

3.2. Organization of digital files: folders and document naming

When we use our computer or phone, we gather many files over time: documents, photos, videos or different materials downloaded from the internet. If these files are saved randomly, it becomes difficult to quickly find what we need. That's why it's helpful to know how to organize our digital files in a simple and clear way.

An easy way to tidy up is to use *folders*. A folder is like a folder where we can keep multiple documents. Just as in an office, we use files to separate different documents; we can do the same on the computer. Each folder can contain smaller files or other folders.

For example, we can create a folder called *"Personal Documents"* to save important documents, such as requests, contracts, and other documents. We can also have a folder called *"Photos"* to keep photos taken with the phone or camera. We can also create a folder for *work projects*, one for *invoices*, or one for *files downloaded from the internet*.

For even better organization, we can create **subfolders within the folders**. These are smaller folders inside a main folder. For example, in the "Photos" folder, we can have subfolders for each year: "Photos 2025", "Photos 2026". Inside them, we can create other subfolders for different important moments, such as "Vacation", "Holidays", or "Family events".

This way of organizing helps us find a file much faster. Instead of searching through dozens or hundreds of documents, we can go directly to the right folder.

Equally important is the **correct naming of the documents**. Many times, people save files with names like "Document1", "New", "Test", or "Final". Over time, these names no longer indicate the contents of the files, making it difficult to know what each document contains.

To avoid this problem, it is best to use **simple, clear names**. For example, instead of "Document1", we can save the file as "Energy bills". Thus, when we see the document's name, we immediately know what it is about.

It's helpful to include **the date or year** in the file name. For example, a file could be named "Energy_bills_2025." This makes it easier to identify different versions of the same document.

To keep order, it is good to check the saved files from time to time. Sometimes we keep documents that we no longer need or save the same file multiple times. If we delete unnecessary files and keep only what is important, the computer will be better organized.

Also, for very important documents, it is good to make **backups**. For example, we can save the files to a USB stick, an external hard drive, or an online storage service. In this way, if a problem occurs with the computer, the information is not lost.

Conclusion

Storing and managing digital information are important skills for anyone who uses a computer or phone. Saving files on our device, using USB sticks, external hard drives, or cloud services are ways we can keep data safe.

At the same time, organizing files into folders and using clear document names helps us quickly find the information we need. With a little attention to detail and organization, using technology becomes much simpler and more efficient.

Important ideas about storing information

To keep the information safe, it is good to:

- We save the files in organized places
- We use clear folders and names for documents
- We keep backups of important files
- We use cloud services for easy access from multiple devices.

Activity

Check how files are organized on your phone or computer.

Answer the following questions:

- Do you have folders for different types of files?
- Do the files have clear names that indicate their contents?
- Do you have backups for important documents?

If you notice that the files are hard to find, try creating a few simple folders to organize them better.

4. Utility Apps – Digital Tools for Everyday Life

Nowadays, smartphones, tablets and computers are part of our daily lives. We use them to talk to family, search for information, pay bills, or organize our activities.

To make all these things easier, we use different digital apps. Among the most useful are **utility apps**. These are simple programs that help us solve different daily tasks faster and more efficiently. They are not created for entertainment, but to help us better manage our daily activities.

In recent years, we have been using such apps more and more often for common activities, such as checking the weather, orienting on the map, paying bills or organizing our daily schedule. Most of them can be downloaded from app stores and can be used on our phone, tablet, or computer.

Utility apps have a few general characteristics that set them apart from other types of apps:

- they are designed to solve concrete problems or facilitate certain activities;
- they offer clear and user-friendly functions;
- they allow quick access to information or tools;
- they are frequently used in everyday life.

Depending on their purpose, these apps may have different functions. Some are intended for organizing activities and time management, others for orientation and navigation, and others for making payments or accessing online services.

Also, many applications are integrated with other digital services. For example, a calendar app can sync with our email account, and a navigation app can utilize traffic data to recommend faster routes.

Many of us use such apps without realizing it:

- In the morning, we check the weather on our phone;
- We use the alarm to wake us up;
- We use the map to get to an address.
- We do quick calculations when we pay for something.

In this chapter, we will see what utility applications are, what they are used for, and how they can help us in our daily lives.

4.1. Categories of Frequently Used Utility Applications

There are many types of utility apps, each created to meet different needs. Among the most used categories are apps for organization and productivity, apps for navigation and transportation, and apps for utilities and payments.

Apps for organization and productivity

Apps for organization and productivity are used for task planning and effective time management. They allow us to create to-do lists, schedule meetings, or organize important information.

An example of an app used to schedule tasks is Google Calendar. This allows us to add events to our calendar, set times for meetings, and receive notifications before they take place.

Applications such as Todoist are commonly used to manage daily tasks, which help us create to-do lists and set priorities for each task.

Another type of useful app is a note-taking app. For example, Microsoft OneNote lets us save and organize information in digital format, similar to a notebook. We can add text, images, or lists, making it easy to organize ideas and work materials.

By using these apps, we can get a clearer picture of the activities we need to perform and avoid forgetting or postponing tasks.

Navigation & Transport Apps

Navigation and transport apps are designed to help us find our way around and plan our journeys. These apps use technologies such as GPS and digital maps to determine our location and calculate routes to various destinations.

A very well-known example is Google Maps. This app provides detailed maps, traffic information, and directions for various modes of transportation, including driving, public transportation, and walking.

Another popular app is Waze, which relies on user-reported information to signal real-time traffic conditions such as accidents, traffic jams, or roadworks.

Navigation apps can suggest alternate routes when traffic is congested and provide voice instructions that guide us throughout the journey.

These tools are useful for both daily commutes and trips to unfamiliar areas, as they provide accurate information about routes and traffic conditions.

Apps for utilities and payments

Another important category of utility apps is utility and payment apps. They allow us to access administrative services or make payments without visiting institutions or counters.

Taxes owed to public institutions can be paid online through national e-government platforms — in Romania, through [Ghișeul.ro](https://ghișeul.ro); in Italy, through [PagoPA/App IO](https://pago.pa.it); in Slovenia, through [eUprava/eDavki](https://euprava.gov.si); in Belgium, through [MyMinfin/MyGov.be](https://myminfin.fgov.be); and in Poland, through obywatel.gov.pl. Citizens can check the amounts owed and make payments directly from their personal account, without visiting a physical office.

For online payments and money transfers, the PayPal application is frequently used to facilitate transactions in the digital environment.

Also, applications such as Google Pay allow contactless payments in stores using a mobile phone.

Through these apps, we can more easily manage payments and access various services quickly and conveniently.

4.2. Use of utility applications in daily activities

Utility applications can be integrated into many activities of daily life. They provide tools that make it easier to organize time, access information, and perform administrative tasks.

A common example is **the organization of daily activities**. We can use calendar apps to schedule meetings, events, or important tasks. To-do lists can also help track progress in completing various tasks.

Navigation apps are useful for **planning trips**. By entering a destination, we can find the optimal route and the estimated trip duration.

At the same time, digital applications can be used for **document and information management**. Notes, photos, or files can be saved and organized in an accessible way.

Another important area is **making payments and accessing online services**. Through dedicated apps, we can pay bills, check tax status, or transfer money.

By using these tools, many tasks can be carried out faster and more efficiently, without the need to travel or use paper documents.

4.3. Safe use of apps

The use of digital applications also entails responsibility for protecting personal data and financial information. For this reason, we should follow certain security rules.

A first step is to use secure passwords (at least 10–12 characters long, combining uppercase and lowercase letters, numbers, and symbols such as @, !, #) that include combinations of letters, numbers, and symbols. Passwords should be kept secure and not shared with others. Some apps and browsers offer to save and generate passwords automatically (password managers). These can be useful, but be aware that if someone gains access to your device or password manager account, they could access all your stored passwords. Always protect your device with a PIN or biometric lock.

Also, apps should only be downloaded from **official sources**, such as the operating system's app stores. This reduces the risk of installing unsafe programs.

Regularly updating apps is another important measure. Updates often include security improvements and fixes for technical issues.

We must also be careful about the information we enter into applications and avoid transmitting sensitive data over unsecured public networks. Also, avoid choosing "Remember my password" on shared or public computers, and do not store your username and password directly in website forms on devices that others may use..

Compliance with these rules helps to use apps safely and protect personal data.

Conclusions

Utility apps are important digital tools that help us carry out our daily tasks. They allow efficient time organization, travel planning, information management, and access to online services.

Using these apps, many tasks can be completed faster and more efficiently. At the same time, the development of digital skills contributes to the responsible and safe use of technology.

In the context of society's digitization, the ability to use utility applications becomes an essential skill. Those who acquire these skills can benefit from technology's advantages and participate more actively in social and professional life.

Activity

Think about the apps you use on your phone.

Note:

- An app that you use to organize activities.
- An app that you use for orientation or navigation.
- An app that you use for online payments or services.

Which of these apps help you the most in your daily life?

5. Use of videoconferencing services

Currently, many meetings, courses, or discussions can take place online. Instead of meeting in person, we can communicate online via **video conferencing** apps.

These apps let us talk to others, see their images, and join online meetings on our phones, tablets, or computers.

Videoconferencing services are used in many situations, for example:

- online meetings with teachers or school;
- courses and educational activities;
- work meetings;
- discussions with family or friends.

5.1 What is a video conference

A video conference is an online meeting where multiple people can communicate over the internet using a video camera and a microphone.

Participants can:

- to talk among themselves;
- see each other on the screen
- share documents or presentations.
- participate in group discussions.

This type of communication is especially useful when participants are in different places.

5.2 Video conferencing platforms

There are several apps that allow online meetings.

Among the best known are:

- Zoom
- Google Meet
- Microsoft Teams

These apps are relatively easy to use and work on both our phone and our computer.

5.3 How we participate in an online meeting

To participate in a video conference, we usually receive **an access link**.

The steps are generally as follows:

1. we open the link received;
2. access the videoconferencing application;
3. we activate the microphone and camera, if necessary;
4. We enter the meeting.

In some cases, we may need to enter an **access code** or write our name.

How to participate in an online meeting – step by step

If you're joining a video conference for the first time, you can follow these steps:

Step 1. We open the message or email containing the meeting link.

Step 2. We tap the link the organizer sent.

Step 3. The video conferencing app will automatically open or ask us to install it.

Step 4. We enter our name.

Step 5. We check that the microphone and camera are working.

Step 6. We press the "Join" or "Join Meeting" button.

💡 If we're nervous or unsure if everything is working properly, it's a good idea to get in a few minutes early.

💡 **Tip**

It is good to enter the meeting a few minutes before the scheduled time to check if the microphone and camera are working properly.

Activity

Think of an online meeting that a parent could attend (for example, a meeting with teachers).

Note:

- What device are you using (phone, tablet, or computer)
- If you need a camera or a microphone.
- What would you do if the meeting doesn't open?

5.4 Basic rules for participating in video conferences

In order for online meetings to take place in good conditions, it is useful to follow a few simple rules:

- Check your internet connection before the meeting.
- Keep the microphone off when you're not speaking.
- Listen carefully to the person speaking.
- Avoid background noise.

These rules help to communicate more clearly and effectively.

💡 **Tips for parents at online meetings with teachers**

When attending an online meeting with your child's teachers, a few simple things can help communication be clearer:

- Sign in a few minutes before the meeting starts.
- Find a quiet place;
- Keep the microphone off when you're not speaking.
- Write down the questions you want to ask.
- Listen carefully to the information provided by the teachers.

These simple things can make the meeting more efficient and enjoyable for all participants.

Example from everyday life

A parent is invited to an online meeting with their child's teachers. They receive a link to the meeting through a message. At the scheduled time, the parent opens the link on their phone, joins the videoconferencing app, and participates in the discussion alongside other parents and teachers.

Common problems during online meetings

Sometimes small technical difficulties may arise. Here are some of the most common situations:

You don't hear the sound

Check that the microphone is turned on and that the volume is on.

Camera not working

Check if the app has permission to use the camera.

The internet connection is weak

Try moving closer to your router or turning off other apps that use the internet.

You can't join the meeting

Check that the link is correct and that the meeting hasn't started yet.

Activity

Think about whether you've ever attended an online meeting.

1. What app did you use?
2. What was easy during the meeting?
3. What difficulties did you encounter?

6. Online shopping

Today, more and more people are buying products or services using the internet. Online shopping allows us to quickly find the products we need and order them directly from our phone or computer.

Through the internet, we can buy many types of products, for example:

digital apps, subscriptions, and online services (such as streaming platforms, educational apps, productivity tools, and games) – these are increasingly purchased online and are just as important as physical products.

- clothes and footwear;
- books and educational materials;
- children's toys;
- household appliances;
- tickets for events or transport.

Online shopping can be useful because it saves time and makes it easier to compare prices across different stores.

6.1 What is online shopping

Online shopping means purchasing products or services via the internet.

To make an online purchase, we usually follow a few simple steps:

1. we search for the desired product;
2. we choose the online store;
3. we add the product to the shopping cart;
4. we fill in the data for delivery;
5. we choose the payment method.

After the order is completed, the product is delivered to the indicated address.



How to make an online purchase – step by step

If we want to buy a product online, we can follow a few simple steps.

Step 1. We search for the desired product online.

Step 2. We open the online store page.

Step 3. We check the product information (description, price, delivery).

Step 4. We add the product to the shopping cart.

Step 5. We enter the delivery details.

Step 6. We choose the payment method and confirm the order.

After completing the order, the online store usually sends a confirmation message or email.



Activity

Find a product on an online store.

Check out:

- whether the site seems trustworthy;
- If there is information about the company;
- If there are reviews from other buyers.
- if the delivery conditions are clear.

Would you trust buying from this site? Why?

6.2 Online Shopping Platforms

There are many online stores where we can buy products.

Some of the most well-known international platforms are:

- Amazon
- eBay

In many countries, there are also local online stores that offer a wide range of products.

6.3 Advantages of online shopping

Online shopping has several advantages.

Among the most important are:

- we save time;
- we can compare several products;
- we can see the opinions of other buyers;
- We can buy products that are not available in local stores.

Also, many online stores offer detailed product information, including photos and descriptions.

✓ How to recognize a secure online store

Before placing an order, it is good to check a few simple things:

- The website has clear information about the company;
- There are contact details (address, telephone or email);
- The site uses a secure connection (the address starts with **https**).
- There are opinions or reviews from other buyers.

If a site does not provide this information, it is advisable to exercise caution before placing an order.

6.4 Safety of online shopping

When shopping online, it is important to pay attention to safety.

To avoid problems, it is good to:

- we buy from well-known and trusted sites;
- we check that the site is secure;
- we read the opinions of other buyers;
- we check the delivery and return conditions.

It is also recommended that we not share personal data on sites that do not appear secure.

Caution

If a price seems much too low or the offer seems too good to be true, it is good to check the information before placing an order.

How to avoid fraud when shopping online

To avoid problems, it is good to keep in mind a few simple rules:

- Avoid unknown or suspicious sites.
- Do not send personal data through unknown messages or emails;
- Don't pay upfront if the store doesn't seem trustworthy.
- Always check other buyers' reviews.

If an offer seems too good to be true, it is good to check the information before placing an order.

Example from everyday life

A parent wants to buy a book for their child. They search for the product online and find several online stores selling the same book.

To make a good choice, the parent compares prices, reads other buyers' opinions, and checks delivery times.

Activity

Think about whether you've ever made an online purchase.

1. What product did you buy?
2. How did you choose the online store?
3. What information did you check before placing your order?

✓ Checklist before an online purchase

Before you complete an order, check:

- ✓ the online store seems reliable,
- ✓ the product's price is reasonable,
- ✓ there are reviews from other buyers,
- ✓ delivery conditions are clear, and there is a possibility of returns.

If all of these things are okay, you can place your order with more confidence.

7. Online games, betting, and associated risks

7.1 Online games and child safety

What is important to know as parents

Online games are part of today's children's lives. Many children play on their phone, tablet or computer. Some games are fun, they help them socialize with friends and even learn new things.

For parents, a complete ban on games is not always the most effective solution. It is more useful to understand what types of games exist, what risks may arise, and how we can talk to children about these aspects. When parents better understand the digital environment in which children spend their time, it becomes easier to support and protect them.

Online games with dangerous challenges

Occasionally, challenges or "games" pop up online and spread mainly on social media. They motivate children to try different actions to show bravery or take part in a viral challenge.

Some of these challenges can become dangerous.

For example, many parents have probably heard of the **Blue Whale Challenge**, a game in which participants receive several challenges, each becoming increasingly risky. In some cases, challenges may include dangerous behaviors or self-harm. (Note: subsequent investigations found that the scale of this phenomenon was significantly exaggerated by media coverage; however, the type of psychological manipulation it illustrates remains a real concern.)

Another example is **the Momo Challenge**, where children received messages from a scary character urging them to do various risky things. (Note: the Momo Challenge was largely a media-driven moral panic with no verified evidence of direct harm; it remains useful as an example of how manipulative content can spread online.)

There was also a challenge called **the Fire Fairy Challenge**, in which children were urged to leave the gas on to "become a fairy". Obviously, this can cause fires or explosions and is extremely dangerous.

Such challenges can involve pressure from other people or even psychological manipulation. For this reason, it is important for parents to talk openly with their children about such situations and encourage them to say immediately if they come across such content online.

Multiplayer games where kids communicate with other people

Many popular games allow children to communicate with other players. Sometimes this is done through written messages (chat) or through the microphone.

Among the most well-known games are:

- Roblox
- Fortnite
- Minecraft

These games are not dangerous in themselves and are played by millions of children worldwide. However, sometimes children can come into contact with unknown people.

For this reason, it is important for parents to discuss with their children a few simple rules:

- not provide personal information;
- Not accept friend requests from strangers.
- tell an adult if someone is making them feel uncomfortable.

Games in which money can be spent

Some games include in-game shopping. For example, players can buy virtual items or "loot boxes (also called "surprise boxes" or "mystery boxes") that offer random rewards.

Well-known examples are:

- ***Counter-Strike 2 (CS2)***
- ***League of Legends***
- ***EA Sports FC (formerly FIFA Ultimate Team)***
- ***Genshin Impact***

The problem arises when children start spending money without understanding its exact value. Sometimes, gambling-like behaviors can also occur, as players try several times to get a rare item. For this reason, it is recommended that parents check the games' settings and talk to their children about how in-game shopping is used.

Very violent or scary games

There are also games created specifically for adults that can contain a lot of violence or scary scenes.

For example:

- ***Five Nights at Freddy's (FNAF)*** – *very popular among teenagers, despite its horror themes*
- ***Grand Theft Auto V***
- ***Outlast***

In younger children, such games can cause fear, anxiety, or nightmares. For this reason, it is recommended to check the age rating of games (PEGI).

Dangerous challenges that sometimes arise in gaming communities

Challenges sometimes appear online that seem fun but can become dangerous.

For example:

- ***Salt and Ice Challenge*** – *children put salt and ice on their skin, which can cause burns.*
- ***Skull Breaker Challenge*** – *a prank in which someone is pushed while jumping and can fall on their back.*

- **Blackout Challenge** – a challenge in which participants hold their breath until they almost lose consciousness.

Such challenges can cause serious injuries, and it is important to talk to children about them.

Signs that can show that a child has a problem with games

Sometimes, a child's behavior may change when a gaming problem arises.

For example, we would be careful if we notice that:

- *The child hides what they are doing on their phone or computer*
- *Quickly close the game when someone enters the room*
- *Stay online very late*
- *Becomes more withdrawn or irritated*
- *Scratches or bruises appear without explanation*

These things don't automatically mean there's a problem, but they can be a sign that a discussion is needed.

✓ Suggestion for parents

To reduce the risks, parents can:

- Check your games' parental control settings.
- Talk openly with children about their online experiences.
- Set limits on the time spent in games.

▣ Using Parental Controls and Screen Time Tools

Most devices and operating systems include built-in parental control tools: on iOS use "Screen Time" (Settings → Screen Time); on Android use "Digital Wellbeing & Parental Controls"; on Windows use "Family Safety" (Microsoft account settings). These tools allow us to set daily time limits for specific apps, block certain content categories, and monitor usage without invading our child's privacy.

Open communication and interest in children's digital activities can contribute to safer use of online games.

7.2. Risks of online betting for children and teenagers

1. Why are we discussing this topic?

Many children and teenagers spend time online every day: on their phones, in games, on social networks, or watching sports competitions. In this environment, advertisements for sports betting and online casinos appear more and more often.

Although these platforms are designed for adults, the reality is that many minors end up being exposed to them or even trying them.

To parents, the topic may seem distant or "adult-specific," but research shows that interest in betting often appears as early as adolescence.

The purpose of this material is not to create panic but to provide parents with information and simple prevention tools.

2. What attracts children to betting?

Teenagers are naturally curious and attracted to new experiences. In the online environment, bets are presented in a very attractive way.

What things can tempt children?

- The Promise of Quick Win
- Connection with sport (football, tennis, basketball)
- Influence of friends or group
- Frequent Internet and Social Media Ads
- Influencers promoting such platforms

To a teenager passionate about sports, betting might seem like an exciting game or a challenge rather than a risky activity.

3. How children come into contact with online betting

Often, contact with this phenomenon occurs gradually:

- Ads in apps or on sports websites
- Videos on social networks

Streamers and influencers on platforms like Twitch, YouTube, and Instagram who promote gambling sites and apps (often presenting it as entertainment)

TV advertising for betting companies and online casinos, which appears in many countries during sports broadcasts and evening programming

- Friends Talking About Betting
- Online games that include similar mechanisms (reward boxes, virtual gambling)

Sometimes, teens create accounts using fake data or use adult accounts.

4. What are the risks?

Addiction

The bets are designed to stimulate the desire to continue. Small or occasional gains can make young people think they can control the outcome.

Over time, the desire to bet again and again arises.

Financial problems

Teens can lose money from:

- allowance or pocket money
- money received for various activities
- sometimes even from parents' accounts

Often, the desire to recover losses leads to increasingly risky bets.

Emotional impact

Losing money or bets can cause:

- frustration
- irritation
- anxiety
- mood swings

For a teenager, these feelings can become very intense.

Impact on school and relationships

When betting becomes a constant concern, the following can occur:

- decreased interest in school

- lack of concentration
- conflicts with parents
- the tendency to hide online activities

5. Signs that parents can look out for

Sometimes small changes in behavior occur that are worth noticing:

- the child becomes very attentive to sports scores
- checks their phone often during matches
- ask for money more often than before
- gets nervous after watching sports results
- is very secretive about online activity

These signs do not automatically indicate a problem, but they can be a signal that the topic is worth discussing.

6. What can you do as parents?

Talk openly about this phenomenon

Children need to understand that betting is not a way to make money, but an activity in which the house almost always wins.

A calm and honest discussion is much more effective than rigid prohibitions.

Set clear rules

For example:

- Responsible use of the phone and the internet
- Using cards only with parental consent
- Limits for online payments

Pay attention to the digital environment

It is not about excessive control, but about real interest in the child's online world:

- What apps they use
- What they watch on the internet
- What to Discuss with Friends

Encourage real-life activities

Sports, hobbies and time spent with friends are important protective factors.

A teenager involved in various activities is much less likely to engage in risky behaviors.

7. If you find that the teenager is betting

A parent's first impulse may be anger or punishment. However, a calm reaction is more helpful.

Useful steps:

1. Talk openly about what's going on.
2. Try to understand the reasons behind the behavior.
3. Set new boundaries and rules together.
4. If the situation persists, the support of a school counselor or psychologist can be very helpful.

A final thought

Online betting is a part of a well-structured industry that uses marketing and psychological tactics to keep users engaged.

Children and adolescents do not yet have the maturity necessary to manage these pressures. That is why the parents' role is essential.

Information, dialogue, and interest in children's digital lives are the best forms of prevention.

8. Disinformation online

8.1. What is disinformation

Disinformation is the spread of **false or misleading** information to make people believe something that is not true.

Sometimes this information is created intentionally to:

- influencing people's opinion
- create fear or confusion
- manipulate the way people think

Today, disinformation spreads very quickly by:

- Social media
- News Sites
- Messages on the phone
- Videos on the Internet

What is "fake news"

Fake news is news presented as true.

They may look like normal news, but the information is:

- Invented
- exaggerated
- taken out of context

Often fake news has:

- Very shocking titles
- Claims without evidence
- Modified images or videos
- Information without a clear source

A simple example:

"The drug that cures all diseases has been discovered"

"A secret event was hidden by the authorities"

Such messages are created to attract attention and be shared quickly.

What is information manipulation?

Information manipulation occurs when someone presents information in a way that influences the way people think.

These are not always outright lies. Sometimes methods such as:

- Only part of the truth is being told
- Certain information is exaggerated
- An idea is repeated many times
- Strong emotions (fear, anger) are used

The goal is for people to believe a certain idea without analyzing all the information.

Why disinformation is dangerous

Disinformation can have negative effects:

- people can make wrong decisions
- conflicts and misunderstandings may arise
- people can lose trust in real information
- society can become more confused and divided

How to protect ourselves from false information

To avoid misinformation, it is good to:

1. **We verify the source of the information**
2. We look for the information on other sites as well
3. We don't immediately believe the very shocking headlines
4. We ask ourselves: is there evidence?
5. We do not share information if we are not sure it is true

Remember!

Not everything that appears on the internet is true. It is important to verify the information before we believe or share it.

8.2. How we recognize fake news

Source verification and content analysis

A lot of information circulates online daily. Some are correct, but others are inaccurate or false. That's why it's important to know how to verify information before believing or sharing it.

Recognizing fake news doesn't require complicated knowledge. Often, a few simple verification rules are enough.

Verification of the source of the information

The first step when reading a news item is to ask ourselves *where the information comes from*.

Useful questions

- Who published the news?
- Is it a well-known site or an unknown one?

- Is there any information about the author?
- Are sources or specialists cited?

Warning signs

A news story can be suspicious if:

- appears on an unknown site
- the author is not mentioned
- no sources or evidence are presented
- The information appears only on one site

Example

*If important information only appears on an obscure page and is not confirmed by other sources, it may be **fake news**.*

Checking information in multiple places

A simple method of verification is to look for the same information in other sources.

If the news is real, it usually appears in:

- More publications
- Well-known news sites
- Official pages of the institutions

If the information does not appear anywhere else, it should be viewed with caution.

Title Analysis

The title is the first thing we see. Some fake news uses headlines created specifically to attract attention.

Examples of suspicious headlines

- "You won't believe what happened!"
- "The authorities are hiding this secret!"
- "The doctors don't want you to know that!"

Such titles are often used to provoke curiosity, fear, or indignation.

Content analysis

After reading the headline, it is important to analyze the text of the news.

What to look out for

- Is there any evidence or studies cited?
- Are specialists or institutions mentioned?
- Is the information presented clearly and logically?

Signs of fake news

- Claims without evidence
- Exaggerated information
- confusing or contradictory text
- Many grammatical mistakes

Sometimes, fake news uses strong emotions to influence readers.

Check images and videos

Images can be manipulated or taken out of context.

⚠ Be aware of deepfakes

Artificial intelligence can now create highly realistic fake videos and audio recordings (called "deepfakes") that show real people saying or doing things they never actually did. These are increasingly used to spread disinformation. If a video seems surprisingly shocking or shows a public figure saying something extreme, check multiple trusted news sources before sharing it.

That's why it's good to check:

- If the image appears in other articles
- if the photo is old
- if the image is related to the news

Sometimes a real photo is used to illustrate a completely different event.

Critical thinking

An important element in recognizing fake news is critical thinking.

Before believing or sharing information, it is useful to ask ourselves:

- Does this information seem realistic?

- Is there any evidence?
- Who would have an interest in spreading this information?

Conclusion

Recognizing fake news is an important skill in the digital society.

By:

- *Source verification*
- *Content Analysis*
- *Comparison of information*
- *Using critical thinking*

We can avoid the spread of false information and contribute to accurate information.

8.3. Strategies to counter disinformation

Fact-checking and use of fact-checking sites

In the online environment, information circulates very quickly. For this reason, fake news or misleading information can reach many people quickly. Combating disinformation is possible if people learn to verify information before believing or sharing it.

There are some simple strategies that can help us identify and avoid false information.

❖ Verify information before sharing

An important first step is not to share information immediately, especially if it seems surprising or shocking.

Before sharing, it is useful to ask ourselves:

- Who published this information?
- Are there any sources or evidence?
- Is it confirmed by other publications?

Often, fake news spreads because people distribute it quickly, without checking it.

❖ Searching for information in multiple sources

A simple verification method is to look for the same information in other places.

If the news is real, it usually appears in:

- More news sites
- Well-known publications
- Official pages of the institutions

If the information is only found on a single website or on an unfamiliar page, it might be false or incomplete.

❖ **Content and title analysis**

Some information is presented in an exaggerated way to attract attention.

Signs of suspicious news can be:

- Very dramatic titles
- Claims without evidence
- emotional or aggressive language
- lack of author or sources

Reading the entire article carefully is important, as sometimes the title can be misleading.

❖ **Use of fact-checking sites**

An effective method of fact-checking is using fact-checking sites. These platforms analyze claims or news and verify their truth.

Fact-checking organizations:

- check the sources of the information
- analyze data and documents
- consult experts
- publish the results of the verification

These sites help the public understand whether a piece of information is:

- true
- partially true
- fake
- taken out of context

❖ **Critical thinking**

Combating disinformation also depends on our own critical thinking.

It is important to ask ourselves:

- Why was this information published?
- Who could benefit from its spread?
- Is there clear evidence?

By carefully analyzing information, we can avoid contributing to the spread of misinformation.

Conclusion

Disinformation can have negative effects on society, but it can be combated through responsible online behaviour.

The most effective strategies are:

- *Verification of information*
- *Consultation of multiple sources*
- *Content and title analysis*
- *Use of fact-checking sites*
- *applying critical thinking*

Through these simple practices, we can all contribute to a safer, better-informed online environment.

Recap: the main ideas of the chapter

The table below summarizes the main things we have discussed in this chapter.

Theme	What is important to remember
Information literacy	The internet offers a lot of information, but we must verify that it is accurate and reliable.
Search for information	We can use search engines or AI-powered tools to find information.

Theme	What is important to remember
Storage and management of information	Important information can be saved and organized on our phone, computer or in online storage services.
Utility Applications	There are applications that can help us communicate, organize our activities or use different online services.
Video Conferencing	We can participate in online meetings using video conferencing applications.
Online shopping	Online shopping is useful, but we need to check if the store is safe.
Online Games & Betting	Some online games may involve risk or expense. It is important to pay attention to how they are used.
Disinformation	Not all information on the internet is true. It is important to verify the information before believing or sharing it.

Advice for parents

The Internet can be a very useful tool for information, learning and communication. Used with care and responsibility, it can help us make better decisions and support children in the learning process.

How can we use this knowledge in everyday life

How this chapter can help us

The information in this chapter can be useful in many everyday situations.

For example, we can use this knowledge to:

- Look for information about school or activities for children.

- Check the information found on the internet before believing or sharing it;
- Save and organize important information on our phone or computer;
- Use digital apps that can help us in our daily lives;
- Participate in online meetings with teachers or others;
- Shop online safely.
- Talk to our children about how they use the internet and online games.

Using digital information correctly can help us make better decisions and use technology to our advantage and that of our family.

Quick Self-Assessment Test

Check what you've learned

Read the statements below and check the options you consider correct.

- Not all information on the internet is accurate or reliable.

- It's a good idea to check information from multiple sources before using or sharing it.
- We can use search engines or AI-powered tools to find information.
- Important information can be saved and organized on our phone, computer or in online storage services.
- We can participate in online meetings using video conferencing applications.
- It is important to check if an online store is safe before making a purchase.
- Some online games or betting platforms may involve risks or expenses.
- Not all information shared on the internet or social media is true.

Once you've completed the exercise, discuss your answers with other participants or your trainer.

CHAPTER II

1. Effective communication in the online environment

1.1 What is online communication

Communication is a fundamental part of everyday life. We communicate with family, friends, colleagues, teachers, and institutions. In recent years, a significant part of this communication has moved online.

Online communication means exchanging information, ideas or messages through digital tools and platforms. It can take many forms: text messages, emails, voice calls, video calls or posts on social media.

For parents, understanding how online communication works is important for several reasons: it helps them stay connected with their children's school, communicate with other parents, access public services and guide their children in using digital communication responsibly.

Why is it important to understand online communication?

- It helps us stay in contact with family, friends and institutions more easily;
- It allows us to access important information quickly;
- It helps us understand how our children communicate online;
- It enables us to recognize situations where online communication can be risky.

Online communication differs from face-to-face communication in several ways. When we talk to someone in person, we use **body language, facial expressions and tone of voice** to express our meaning. In online communication, many of these signals are absent, which can sometimes lead to misunderstandings.

Example from everyday life

A parent receives a short message from another parent in the class group chat: “Your child was involved in a situation today.” Without additional context, tone or facial expression, this message

can cause unnecessary worry. In a face-to-face conversation, the same information might be delivered with a reassuring tone.

Activity

Think about the last time you communicated with someone online (e.g., via WhatsApp, email or a school platform).

1. What tool did you use?
2. Was the communication clear or did any misunderstanding occur?
3. How could the communication have been improved?

1.2 Forms of online communication

Online communication can be divided into different categories depending on how and when messages are exchanged.

Synchronous communication (real-time)

This type of communication happens in real time, meaning both people are online at the same time. Examples include:

- Phone calls and video calls (e.g., WhatsApp, FaceTime, Zoom)
- Live chat and instant messaging (e.g., Messenger, WhatsApp, Telegram)
- Live online meetings (e.g., Google Meet, Microsoft Teams)

Asynchronous communication (not in real time)

In this form, messages are sent and received at different times. The other person does not need to be online at the same moment. Examples include:

- Email
- Messages on school platforms
- Posts and comments on social media
- Forum discussions

Both forms of communication are useful. **Synchronous communication** is better when we need an immediate answer or want to have a more personal interaction. **Asynchronous communication** is convenient when we want to take time to think about our response or when the other person is not available at the same moment.

	Synchronous	Asynchronous
Speed	Immediate response	Delayed response
Example	Video call, live chat	Email, forum post
Best for	Urgent matters, personal talks	Non-urgent, detailed messages

1.3 Choosing the right communication tool

Different situations call for different communication tools. Choosing the right tool can make communication more effective and avoid confusion.

If we want to...	We can use...
Send a quick message to a friend	WhatsApp, Messenger, SMS
Communicate with a school or institution	Email, school platform
Have a face-to-face conversation remotely	Video call (Zoom, Meet, FaceTime)
Share photos or updates with family	WhatsApp group, private social media
Report a problem to a service provider	Email, contact form on website

Tips for effective online communication

- Be clear and specific in your messages: avoid vague or very short messages that can be misunderstood;
- Use a polite and respectful tone, even in informal conversations;

- Think before sending: once a message is sent, it cannot always be taken back;
- Be mindful of when you send messages: avoid sending non-urgent messages late at night;
- When in doubt about tone, consider using a video or voice call instead of text.

1.4 Communication etiquette in the digital world

Just as there are rules for polite behavior in face-to-face communication, there are also guidelines for respectful and effective communication online. These guidelines are sometimes called “netiquette” (a combination of “internet” and “etiquette”).

Some basic principles of online communication etiquette include:

- Write clearly and avoid using only capital letters (this is often perceived as SHOUTING);
- Respond to messages within a reasonable time;
- Respect other people’s opinions, even when you disagree;
- Avoid sharing other people’s private information without their permission;
- Be careful with humor and sarcasm: they can easily be misunderstood in text;
- Do not forward messages or photos without the sender’s consent;
- Proofread your messages: check for spelling and grammar, especially in formal communications;
- Keep group chats focused: only post messages relevant to the entire group;
- Use specific subject lines (for email): this helps the recipient quickly prioritize and find your message later.

Example from everyday life

A parent posts a lengthy, personal complaint about a school policy in the general class WhatsApp group, followed by several short, separate messages. A better approach would be to send a single, well-written email to the teacher or administrator or use a private message to discuss the issue one-on-one, keeping the group chat focused on shared, relevant information.

Activity

Read the following messages and decide which one follows better netiquette principles and why:

Message A: "URGENT! THE FIELD TRIP IS CANCELED. NEED A NEW PLAN. TELL ME NOW!!"

Message B: "Subject: Field Trip Update: Action Needed. Dear Parents, please note that tomorrow's field trip has been canceled due to weather. A survey with alternative options will be sent out within the hour. Thank you for your flexibility."

Discussion: Why is Message B better? (It uses a clear subject, avoids all caps and provides constructive next steps instead of demanding an immediate response.)

⚠ Attention

Messages, photos and videos shared online can be saved, forwarded or shared by others. Before sending anything, ask yourself: "Would I be comfortable if this message were seen by everyone?"

1.5 Managing conflict and disagreements online

Online discussions, especially in group chats, can quickly become heated because people cannot see facial expressions or hear tone of voice. Learning to manage disagreements respectfully is a vital part of netiquette.

💡 Tips for managing online conflict

- **Pause before responding:** If a message makes you angry, step away for a few minutes before typing a reply. An emotional response rarely improves the situation.
- **Focus on the issue, not the person:** Attack the argument or problem, not the individual. Avoid personal insults or assigning blame.
- **Choose the right channel:** If a disagreement is complex or highly emotional, suggest moving the conversation to a private phone call or a face-to-face meeting.
- **Use clarifying language:** Phrases like, "I understand you are saying X, is that correct?" can prevent misunderstandings from escalating.

- Know when to step away: If the conversation becomes toxic, it is okay to mute the chat, leave the group or simply stop responding.

Example from everyday life

A parent is upset by a comment made in the class WhatsApp group about a school event donation. Instead of immediately typing a heated reply in the group, they send a private message to the group administrator or the person who posted the comment, asking for clarification. This keeps the conflict contained and professional.

1.6 Communicating with schools and teachers digitally

Staying connected with your child's school and teachers is crucial for their success. The digital tools used (email, school platforms, specific apps) require a more formal and professional approach than communicating with friends.

Guidelines for professional digital communication

- Choose the appropriate tool: Use the school's official email or dedicated platform for important, formal or confidential matters. Instant messaging should be reserved for quick, non-urgent questions only if the teacher has explicitly allowed it.
- Be concise and clear: Teachers receive many messages daily. Use clear subject lines and get straight to the point.
- Respect response times: Allow a reasonable timeframe (e.g., 24-48 hours) before following up. Avoid sending messages late at night or on weekends.
- Check the rules: Understand the school's official communication policy.
- Maintain a positive tone: Even when addressing a problem, use polite and respectful language. Your goal is to collaborate on a solution.

1.7 Using emojis and media effectively

Online communication lacks the cues of body language and tone of voice. Emojis and visual media (GIFs, short videos) can help bridge this gap, but they must be used carefully to maintain clarity and professionalism.

Understanding the impact of visuals

- Clarifying tone: Emojis are most useful for ensuring your intended tone is understood. Adding a smiley can ensure a message is read as friendly, not aggressive.
- Professional contexts: In formal communications, such as emails to teachers or institutions, it is best to avoid emojis and highly informal media, as they can be perceived as unprofessional.
- Cultural differences: The meaning of emojis can vary significantly across cultures and age groups.
- Media file size: Be mindful of the size of photos and videos you share, especially in group chats, as large files can consume others' data and phone storage.

Attention

Never use emojis or media to replace clear, direct language, especially when discussing important or sensitive topics. Over-reliance on visuals can lead to misinterpretation.

1.8 The importance of digital accessibility

Digital accessibility ensures that all people, including those with disabilities, can easily perceive, understand, navigate and interact with information online. As a parent communicating with a diverse community, understanding accessibility promotes inclusion.

Steps for accessible communication

- Use simple, clear formatting: Avoid overly complex fonts or text effects. Use standard headings and bullet points to organize information.
- Provide alternative text for images: If you share a photo or graphic, briefly describe the image's content. This helps people using screen readers.
- Avoid writing long sections in ALL CAPS, which is difficult to read and perceived as shouting.
- Be cautious with color: Do not use color alone to convey essential information (e.g., “The important text is in red”), as people with color blindness may miss it.

- Write out acronyms: When using an acronym for the first time, write out the full phrase (e.g., “Parent-Teacher Association (PTA)”) to ensure everyone understands.

Activity

Think about the group chats you are a member of (e.g., school group, family group, neighborhood group).

1. What rules do you think are important for respectful communication in these groups?
2. Have you ever experienced a misunderstanding in an online conversation? What happened?
3. Write down three personal rules you would like to follow for your online communication.

2. Social networks: what they are, how they work and their usefulness

2.1 What are social networks

Social networks are online platforms that allow people to connect with each other, share content and communicate. They have become one of the most widely used tools for online communication in the world.

The most widely used social networks include:

- Facebook: used for connecting with friends and family, joining groups and sharing updates;
- Instagram: focused on sharing photos and short videos;
- WhatsApp: used for private messaging, group chats and voice/video calls;
- TikTok: a platform for short videos, very popular among young people;
- YouTube: a platform for watching and sharing videos on various topics;
- X (formerly Twitter): used for sharing short messages and following news;
- LinkedIn: a professional network used for career and business connections;
- Snapchat: used for sending photos and videos that disappear after being viewed.

Each social network has its own **purpose, audience and features**. Some are more suitable for personal communication, while others are designed for professional or educational purposes.

Activity

Look at the list of social networks above.

1. Which one do you use most often for connecting with close friends and family?
2. Which one do you use primarily for consuming news or entertainment?
3. What is the main purpose of the platform your child uses most often?

2.2 How social networks work

Most social networks work based on a few common principles:

1. **Creating an account:** To use a social network, you first need to create a personal account using an email address or phone number.
2. **Building a profile:** After creating an account, you set up a profile with information about yourself (name, photo, interests).
3. **Connecting with others:** You can add friends, follow other people or join groups.
4. **Sharing content:** You can post text, photos, videos, links or comments.
5. **Interacting:** You can like, comment on or share other people's posts.
6. **Receiving a personalized feed:** Social networks use algorithms to show you content based on your interests and activity.

What are algorithms on social media?

- Algorithms are sets of rules that social media platforms use to decide which content to show you.
- They track what you like, comment on and how much time you spend viewing certain posts.
- Based on this information, they show you more similar content.
- This means that two people using the same platform may see very different content in their feeds.

How to reset your feed preferences

1. **Identify unwanted content:** When you see a post you don't like, look for the options menu (usually three dots '...' on the post).
2. **Select "Hide" or "Not Interested":** Choose the option to hide the post or indicate that you are not interested in seeing similar content.
3. **"Unfollow" or "Mute":** If you want to see less of an account, use the Unfollow or Mute features (Muting allows you to remain friends without seeing their posts).

4. Engage with desired content: Actively like, comment on and spend time viewing posts you do want to see more of. This trains the algorithm.

2.3 Benefits of social networks

When used thoughtfully, social networks can offer several benefits:

- Staying connected with family and friends, especially those who live far away;
- Accessing information and news quickly;
- Joining communities with shared interests (e.g., parenting groups, hobby groups);
- Finding educational content and learning opportunities;
- Connecting with schools, teachers and other parents.

Maximize the “Connect” feature

- When using social media, be mindful of the difference between “passive scrolling” (just looking at other people’s lives) and “active connection” (directly engaging).
- To make the time you spend more beneficial, prioritize sending private messages, responding constructively to posts or joining a specific group with a genuine, shared interest.
- This shifts the experience from passive consumption to active participation.

2.4 Risks and challenges of social networks

While social networks have many benefits, they also come with risks and challenges that are important to understand. In this section, we will explore each major risk in depth, providing practical advice, real-life examples and activities to help you recognize and address these challenges in your own life and in your family.

2.4.1 Privacy risks

Personal information can be seen by people we do not know. When we share our location, phone numbers or family photos, we may be exposing ourselves to identity theft or unwanted contact.

What personal information is at risk?

When we use social networks, we often share more information than we realize. Some of this information is shared directly by us, while other data is collected automatically by the platform.

Directly shared information includes things we actively post or enter into our profiles: our full name, date of birth, location, photos, workplace, school, family relationships and phone number.

Automatically collected information includes data the platform gathers without us actively posting it: our IP address, the device we use, our browsing habits, location data from our phone and the times we are active on the platform.

Together, these pieces of information can create a very detailed picture of who we are, where we go and what we do; a picture that can be exploited if it falls into the wrong hands.

Common privacy risks on social media

- Identity theft: Criminals can use personal information to impersonate you, open accounts in your name or carry out financial fraud.
- Location tracking: Sharing your location or posting photos with geotags can reveal where you live, work or where your children go to school.
- Data harvesting: Many apps and platforms collect and sell user data to third-party advertisers without users fully understanding the extent.
- Social engineering: Scammers use information from your social media profile (such as your pet's name, birthday or hometown) to guess passwords or security questions.
- Unwanted contact: A public profile can attract messages from strangers, including spam, phishing attempts or harassment.

Privacy risks specific to families

For parents, the privacy risks extend beyond their own data:

- Photos of children in school uniforms can reveal which school they attend;
- Birthday posts can confirm a child's exact date of birth;
- Check-in posts at locations like parks or after-school activities can establish predictable routines;

- Group photos shared publicly may include other people's children without their parents' consent.

Attention

Before posting a photo that includes other people's children, always ask their parents for permission. In many countries, sharing images of minors without parental consent can have legal implications.

Practical tips for protecting your privacy on social media

- Review your privacy settings on each platform at least once every three months;
- Avoid sharing your real-time location: if you want to share, post about a location after you have left;
- Do not accept friend requests from people you do not know;
- Be careful with quizzes and games on social media that ask for personal information: they are often designed to collect your data;
- Use different passwords for each social media account;
- Disable location services for social media apps on your phone unless absolutely necessary;
- Review the apps connected to your social media accounts and remove those you no longer use.

How to review your privacy settings on Facebook

1. Open Facebook and click on your profile picture in the top right corner.
2. Go to "Settings & Privacy" and then click "Settings."
3. Click "Privacy" in the left-hand menu.
4. Under "Your Activity," set "Who can see your future posts?" to "Friends" instead of "Public."
5. Under "How People Find and Contact You," review who can send you friend requests and who can look you up by email or phone number.

6. Go back to “Settings” and click “Profile and Tagging” to control who can post on your timeline and who can see posts you are tagged in.
7. Review “Apps and Websites” to see which third-party apps have access to your Facebook data and remove any you do not recognize.

Activity: Privacy audit

Take 15 minutes to do a privacy audit of your most-used social media account.

1. Open the app and go to your privacy settings.
2. Check: who can see your posts? (Public, Friends or Only Me?)
3. Check: who can send you friend or follow requests?
4. Check: is your phone number or email address visible to others?
5. Check: which third-party apps are connected to your account?
6. Write down at least two changes you made to improve your privacy.

2.4.2 Misinformation

Not everything shared on social media is true. False news, rumors and manipulated images can spread quickly, leading to confusion or poor decision-making. Developing critical thinking skills is necessary to verify information before believing or sharing it.

Understanding misinformation and disinformation

It is important to distinguish between two related concepts: **misinformation** and **disinformation**.

Misinformation is false or inaccurate information that is spread without the intention to deceive. A person sharing misinformation may genuinely believe it is true.

Disinformation is false information that is deliberately created and spread with the intention to mislead, cause harm or manipulate people’s opinions and behavior.

Both are dangerous, but disinformation is particularly concerning because it is often designed to look credible and to exploit people’s emotions, fears and biases.

Why does misinformation spread so easily on social media?

- Algorithms prioritize engagement: Content that generates strong emotional reactions gets more visibility, regardless of whether it is true.
- Speed over accuracy: On social media, information travels instantly. By the time a fact-check is published, the false story may have already reached millions.
- Echo chambers: Social media algorithms tend to show us content that aligns with our existing beliefs, creating “bubbles” where we rarely encounter corrections.
- Trust in personal networks: When a friend or family member shares something, we are more likely to believe it without verifying.
- Visual manipulation: Photos and videos can be easily edited or taken out of context. AI-generated images and deepfake videos make it increasingly difficult to distinguish real content from fabricated content.

Common forms of misinformation on social media

- Fake news articles: Articles designed to look like real journalism, often with sensational headlines;
- Misleading statistics: Real numbers presented without context to create a false impression;
- Out-of-context photos and videos: Real images from one event used to misrepresent a different event;
- Health misinformation: False claims about treatments, diets or medical conditions;
- Emotional manipulation posts: Stories designed to trigger outrage, pity or fear, often with a “Share this before it gets deleted!” message;
- Impersonation accounts: Fake accounts pretending to be public figures organizations or news sources.

The impact of misinformation on families

- Parents may make health decisions based on false medical advice found online;
- Family arguments can arise from sharing or believing politically charged false content;
- Children may adopt incorrect beliefs based on content they see on social media;

- Financial scams disguised as investment advice can lead to monetary losses.

⚠ Attention

If a piece of content triggers a strong emotional reaction (anger, fear, disbelief), take a moment before sharing it. Emotionally charged content is more likely to be misinformation. Strong emotions are exactly what misinformation is designed to exploit.

💡 How to spot misinformation

- Check the source: Is the article from a known, reputable news outlet?
- Look beyond the headline: Many misleading articles have sensational headlines that do not match the actual content;
- Check the date: Old articles are sometimes reshared as if they are current news;
- Verify with other sources: If a story is true and important, multiple reputable news outlets will be covering it;
- Use fact-checking websites: Platforms like Snopes, FactCheck.org and the EU's EUvsDisinfo can help you verify claims;
- Reverse image search: If a photo seems suspicious, use Google Images reverse search to check if it has been used in a different context;
- Be skeptical of “urgent” sharing requests: If a post tells you to “Share immediately!”, it is likely misinformation.

📌 How to fact-check a social media post

1. Read the entire post or article, not just the headline.
2. Look at who shared it: is this a credible source? Is it a verified account?
3. Search for the same story on established news websites (e.g., BBC, Reuters, your national public broadcaster).
4. If the post includes a photo, do a reverse image search: right-click the image and select “Search image with Google” or use Google Lens on your phone.
5. Check a fact-checking website (such as Snopes.com or FactCheck.org) to see if the claim has already been debunked.

6. If you cannot verify the information, do not share it. It is better to share nothing than to spread false information.

Example from everyday life

A parent sees a post in a WhatsApp group claiming that a popular children's toy has been recalled due to a dangerous chemical. The post includes an alarming photo and urges parents to share the warning immediately.

Before sharing, the parent searches for the toy's name and "recall" on Google. No reputable news source or official consumer safety website mentions the recall. The parent checks Snopes.com and finds that the claim has been debunked as a recurring hoax.

By taking two minutes to verify the information, the parent avoided spreading unnecessary panic in their community.

Activity: Fact-checking practice

Find a post on your social media feed that shares a surprising or alarming claim.

1. What is the claim being made?
2. Who shared it? Is it from a verified or reputable source?
3. Can you find the same information on at least two reputable news websites?
4. Did you check a fact-checking website? What did you find?
5. Based on your research, do you think the claim is true, false or unverified?

2.4.3 Cyberbullying

People can be harassed, insulted or excluded online. This behavior can have serious emotional and psychological impacts on victims. Unlike traditional bullying, cyberbullying can happen 24/7 and reach a very wide audience instantly.

What is cyberbullying?

Cyberbullying is the use of digital devices, platforms and technologies to harass, threaten, embarrass or target another person. Key characteristics that make cyberbullying different from traditional bullying:

- It can happen anytime, anywhere: The victim cannot escape by going home;
- It can reach a large audience instantly: A hurtful message can be shared with thousands within minutes;
- It can be anonymous: Bullies can hide behind fake accounts or anonymous profiles;
- It leaves a permanent record: Messages can be saved, screenshotted and reshared;
- It can be hard to detect: Parents and teachers may not see what is happening in private messages.

Forms of cyberbullying

- Harassment: Sending repeated offensive, threatening or hurtful messages;
- Public humiliation: Posting embarrassing photos or information without consent;
- Exclusion: Deliberately leaving someone out of online groups, chats or activities;
- Impersonation: Creating fake accounts pretending to be someone else;
- Outing: Sharing someone's private information or secrets publicly;
- Trolling: Posting deliberately provocative or offensive content to upset someone;
- Doxxing: Publishing someone's personal details online without their consent;
- Cyberstalking: Persistent, unwanted online monitoring and contact that causes fear.

The psychological impact of cyberbullying

- Anxiety and depression: Victims often experience persistent worry, sadness and helplessness;
- Low self-esteem: Repeated negative messages can make victims internalize the criticism;
- Social withdrawal: Victims may isolate themselves from friends and activities;
- Academic difficulties: Children who are cyberbullied often experience a decline in school performance;
- Physical symptoms: Stress can lead to headaches, sleep problems and stomach issues;

- In severe cases, cyberbullying has been linked to self-harm and suicidal thoughts, particularly in adolescents.

How to recognize if your child is being cyberbullied

Children often do not tell their parents about cyberbullying because they fear losing their devices or that the situation will get worse. Signs to watch for include:

- Sudden reluctance to use their phone or computer;
- Becoming visibly upset, anxious or withdrawn after using their device;
- Avoiding school or social activities;
- Unexpected changes in friendships;
- Declining grades;
- Secretive behavior about their online activities;
- Difficulty sleeping or changes in appetite.

⚠ Attention

If your child tells you they are being cyberbullied, the most important first step is to listen without judgment and reassure them that it is not their fault. Avoid reacting with anger or immediately taking away their devices, as this may discourage them from coming to you in the future.

💡 What to do if your child is being cyberbullied

- Listen calmly and take the situation seriously;
- Do not blame the child or suggest they caused it;
- Save evidence: take screenshots of messages, posts and interactions;
- Help the child block the person doing the bullying;
- Report the behavior to the social media platform;
- Contact the school if the bullying involves classmates;
- If the bullying involves threats of violence or illegal activity, contact the local authorities;
- Consider seeking support from a professional (counselor or psychologist) if the child shows signs of significant emotional distress.

When to contact authorities for cyberbullying

1. Document everything: Before blocking or deleting anything, take screenshots of all offensive posts, messages and comments, noting the dates, times and usernames involved.
2. Assess the threat: Determine if the cyberbullying involves illegal activity (e.g., explicit threats of physical harm, hate speech, sharing non-consensual images).
3. Contact local authorities: If the cyberbullying involves threats, illegal actions or if the safety of your child is compromised, immediately contact your local police department or cybercrime unit.
4. Provide evidence: Submit all collected screenshots and documentation to the authorities.
5. Seek professional support: Prioritize your child's emotional well-being by seeking support from a school counselor or psychologist.
6. Follow school protocol: If the bully is known to be a classmate, inform the school administration with the necessary documentation.

Example from everyday life

A 13-year-old child comes home from school upset. When the parent gently asks what happened, the child eventually shows a group chat where several classmates have been making fun of a photo the child posted. The comments are hurtful and other children have been adding laughing emojis.

The parent stays calm, thanks the child for sharing and reassures them that the behavior is not acceptable and is not their fault. Together, they take screenshots of the messages. The parent then helps the child block the accounts involved and reports the conversation to the platform. The next day, the parent contacts the school to discuss the situation.

Activity: Preparing for cyberbullying situations

Even if your child has not experienced cyberbullying, it is useful to be prepared. Discuss the following questions with your child:

1. What would you do if someone sent you a hurtful message online?
2. Do you know how to block someone on the apps you use?

3. Would you feel comfortable telling a parent or trusted adult if you were being bullied online? Why or why not?
4. Can you think of a situation where something that started as a joke online went too far?
5. Together, practice blocking and reporting on one of the apps your child uses.

2.4.4 Comparison and self-esteem issues

Seeing curated content can create unrealistic expectations. Users often compare their behind-the-scenes lives to everyone else's "highlight reel," which can lead to feelings of inadequacy, anxiety and lower self-esteem, especially among younger users.

The "highlight reel" effect

Social media gives us a window into other people's lives. However, what we see is almost never the full picture. People tend to share their best moments: the perfect family vacation, the well-behaved children, the beautifully decorated home, the career success.

What we rarely see are the struggles behind those posts: the argument before the vacation photo was taken, the tantrum that happened five minutes later, the financial stress or the lonely evenings.

This creates what psychologists call the **"highlight reel" effect**; we compare our unfiltered, everyday reality to other people's carefully curated best moments. This comparison is unfair and inevitably makes us feel that our own lives are somehow lacking.

How social comparison affects parents

- Parenting comparison: Seeing posts from "perfect" parents can make other parents feel inadequate;
- Achievement comparison: Posts about children's achievements can create pressure to "keep up";
- Lifestyle comparison: Vacation photos and material purchases can trigger feelings of financial stress;

- Body image: Filtered and edited photos set unrealistic standards for physical appearance.

How social comparison affects children and teenagers

- Body image issues: Exposure to edited and filtered images can lead to dissatisfaction with their own appearance;
- Social status anxiety: The number of likes, followers and comments can become a measure of social acceptance;
- Fear of missing out (FOMO): Seeing peers at events they were not invited to can cause feelings of exclusion;
- Academic and extracurricular pressure: Comparing achievements with peers can increase stress and anxiety.

Research published by the **Royal Society for Public Health** found that Instagram was rated as the worst social media platform for young people's mental health, particularly in relation to body image, anxiety and depression.

⚠ Attention

Beware of the “Highlight Reel”: Remember that the content people share on social media is usually their best moments, carefully selected and often filtered. Do not compare your everyday life to the seemingly perfect lives presented online. This curated content can be a major source of self-esteem issues if you forget it is not a complete or accurate reality.

💡 Strategies for dealing with social comparison

- Remind yourself that social media shows a curated version of reality, not the full picture;
- Unfollow or mute accounts that consistently make you feel inadequate or unhappy;
- Follow accounts that inspire you in a healthy way or share realistic, honest content about parenting and everyday life;
- Limit the time you spend scrolling through feeds: set a timer if needed;
- Practice gratitude: at the end of each day, write down three things you are grateful for in your own life;
- Talk to your children about the difference between real life and social media;

- Encourage children to focus on their own growth and interests rather than comparing themselves to others.

Example from everyday life

A mother finds herself feeling stressed and inadequate after scrolling through a parenting influencer's Instagram. The influencer seems to have a perfectly organized home, always-smiling children and creative activities every day.

The mother realizes she has been spending 30 minutes every morning comparing herself to this account and feeling bad about her own parenting. She decides to unfollow the account and instead follows a page where parents share honest, unfiltered moments; including the messy, difficult ones.

Within a week, she notices that her mornings feel lighter and she is more present with her own children.

Activity: Social media and your emotions

For the next three days, pay attention to how you feel after using social media.

1. After each session, write down: Which platform did I use? How long did I spend? How do I feel now (energized, neutral, anxious, inadequate, inspired)?
2. At the end of three days, look at your notes. Do you notice any patterns?
3. Are there specific accounts or types of content that make you feel worse about yourself?
4. Are there accounts that make you feel good or inspired?
5. Based on your observations, make one change to your social media habits.

2.4.5 Time consumption

Social media can be very engaging and take up a lot of time. Features like infinite scrolling and constant notifications are designed to keep users on the platform, which can lead to neglecting real-life responsibilities, sleep and physical activity.

How social media is designed to capture your attention

Social media platforms are not neutral tools; they are carefully engineered to maximize the time you spend on them. Understanding the design techniques used can help you make more conscious choices:

- Infinite scrolling: There is no natural stopping point when browsing a social media feed. The content keeps loading endlessly;
- Pull-to-refresh: This mechanism mimics the action of a slot machine, creating anticipation about what new content will appear;
- Notifications: Each notification is designed to pull you back to the app, even when you were not planning to use it;
- Autoplay: Videos that start playing automatically make it easy to keep watching one after another;
- Variable reward schedules: Sometimes you find very interesting content, sometimes you do not; this unpredictability is the same mechanism that makes gambling addictive;
- Social obligation: Notifications about friends' activities, birthdays and messages create a sense of obligation to respond.

The real cost of excessive screen time

- Sleep disruption: Using screens before bed reduces melatonin production, making it harder to fall asleep;
- Reduced physical activity: Time spent scrolling replaces time that could be spent moving or exercising;
- Neglected relationships: Being on the phone during family time reduces the quality of interactions;
- Lower productivity: Constant switching between tasks and checking social media interrupts focus;
- Missed experiences: Focusing on capturing and posting moments rather than experiencing them fully.

Most people underestimate how much time they spend on social media. Studies show that the average adult spends approximately 2-3 hours per day on social media platforms. For teenagers, this number can be significantly higher.

⚠ Attention

The World Health Organization recommends that children under 5 should have no more than 1 hour of sedentary screen time per day and children under 1 should have no screen time at all. For older children and adolescents, screen time should not replace sleep, physical activity or face-to-face social interaction.

■ How to check and limit your screen time

1. On iPhone: Go to Settings → Screen Time. You will see a summary of your daily and weekly usage, broken down by app.
2. On Android: Go to Settings → Digital Wellbeing & Parental Controls. You will see your usage statistics.
3. Review which apps you spend the most time on.
4. Set daily time limits for specific apps: on iPhone, tap the app in Screen Time and select “Add Limit.” On Android, tap the app in Digital Wellbeing and set a timer.
5. Enable “Downtime” (iPhone) or “Focus Mode” (Android) to automatically block distracting apps during certain hours.
6. Review your results after one week and adjust if needed.

💡 Practical strategies for reducing screen time

- Move social media apps off your home screen and into a folder; the extra step reduces mindless opening;
- Turn off non-essential notifications for social media apps;
- Set specific “social media times” during the day instead of checking throughout the day;
- Use a physical alarm clock instead of your phone, so you do not start the day by checking social media;

- Create phone-free zones in your home (e.g., the dining table, bedrooms);
- When you feel the urge to check social media, try the “5-minute rule”: wait 5 minutes. Often the urge will pass.

Example from everyday life

A father decides to check his screen time statistics for the first time. He discovers that he spends an average of 2 hours and 40 minutes per day on his phone, with most of that time on Facebook and YouTube.

Surprised by the numbers, he decides to make changes. He moves both apps to a second screen on his phone, turns off notifications and sets a daily limit of 30 minutes for each app. He also commits to not using his phone during dinner time.

After two weeks, his average screen time has dropped to 1 hour and 20 minutes. He notices that he has more time for reading, playing with his children and sleeping better.

Activity: Screen time challenge

This activity involves the whole family.

1. Each family member checks their screen time statistics for the past week (use the built-in feature on your phone).
2. Discuss the results together: are you surprised by the numbers?
3. Together, set a family goal for the coming week (e.g., reduce total screen time by 30 minutes per day or create one screen-free hour each evening).
4. At the end of the week, check the results again. Did you meet your goal?
5. Celebrate your progress, no matter how small.

2.4.6 Exposure to inappropriate content

This is a significant risk, especially for children who use these platforms. Users may accidentally encounter violent, hateful or sexually explicit content that is not age-appropriate, making active parental guidance and the use of filters vital.

Types of inappropriate content children may encounter

- Violent content: Videos or images depicting real or simulated violence;
- Sexually explicit content: Pornographic material or sexually suggestive content;
- Hate speech: Content that promotes hatred, discrimination or violence against specific groups;
- Self-harm content: Content that promotes or provides instructions for self-harm or suicide;
- Dangerous challenges: Viral social media “challenges” that encourage risky or harmful behavior;
- Predatory content: Content or interactions designed by adults to groom, manipulate or exploit children.

How children encounter inappropriate content

- Through algorithmic recommendations: A child watching innocent videos may be recommended increasingly extreme content;
- Through search results: Innocent search queries can sometimes return inappropriate results;
- Through peer sharing: Friends or classmates may share inappropriate content in group chats;
- Through pop-up ads: Advertisements on websites or within apps may contain inappropriate material;
- Through direct messages from strangers: On platforms where messaging is open, strangers can send unsolicited content.

What to do if your child encounters inappropriate content

- Stay calm: Reacting with shock or anger may make the child reluctant to come to you in the future;
- Listen and validate: Ask the child how they feel about what they saw. Acknowledge that it is normal to feel confused, scared or uncomfortable;
- Explain in an age-appropriate way: Help the child understand what they saw and why it is not appropriate;
- Reassure them: Let them know they are not in trouble for seeing something inappropriate;

- Report the content: Use the platform's reporting tools to flag inappropriate content;
- Adjust settings: Review and strengthen parental controls and privacy settings after an incident.

Attention

No filter or parental control tool is 100% effective. Technology-based protections should always be combined with open, ongoing conversations with your child about what to do when they encounter something upsetting or confusing online.

Setting up parental controls on YouTube

1. Open the YouTube app on your child's device.
2. If your child is under 13, consider using YouTube Kids instead, as it has stronger content filters.
3. For the main YouTube app: go to Settings → General → Restricted Mode and turn it ON.
4. If using Google Family Link, you can manage YouTube settings remotely, including setting daily time limits.
5. Check the Watch History regularly to see what your child has been viewing.
6. Discuss with your child that filters are not perfect and encourage them to tell you if they see something uncomfortable.

Proactive steps to protect children from inappropriate content

- Keep devices in shared family spaces rather than in bedrooms, especially for younger children;
- Use parental controls and safe search filters on all devices and browsers;
- Regularly have conversations about what your child does online and what they see;
- Teach your child what to do if they see something upsetting: close the screen, tell a trusted adult and do not share the content with others;

- Review the apps your child uses: some apps that seem harmless may have hidden chat features;
- Stay informed about the latest apps and platforms popular among children.

Example from everyday life

A 10-year-old is watching animal videos on YouTube when the algorithm recommends a video that contains violent content. The child is upset and tells their parent.

The parent stays calm, thanks the child for telling them and asks how the child feels. They explain that sometimes the internet shows content that is not meant for children and that it is not the child's fault.

Together, they report the video. The parent then activates Restricted Mode on YouTube and decides to install YouTube Kids as a safer alternative. They also agree on a new rule: the child will only watch YouTube in the living room.

Activity: Family safety review

Sit down with your child and review the apps and platforms they use.

1. List all the apps on your child's device. Do you know what each one is for?
2. Are there any apps with messaging or chat features that you were not aware of?
3. Together, check the privacy and safety settings on each app.
4. Ask your child: "Have you ever seen something online that made you feel uncomfortable?"
5. Agree on a simple rule together: "If I see something that makes me feel weird or uncomfortable, I will tell a trusted adult right away."

2.4.7 Summary: Risks at a glance

The table below provides a quick overview of the risks discussed in this section and the key actions parents can take.

Risk	What to watch for	Key actions
------	-------------------	-------------

Privacy risks	Personal data visible to strangers; location sharing; data harvesting	Review privacy settings regularly; limit what you share; be careful with third-party apps
Misinformation	False news; emotional manipulation; health hoaxes	Verify before sharing; check multiple sources; use fact-checking websites
Cyberbullying	Harassment; exclusion; humiliation online	Listen to your child; save evidence; report and block; contact school if needed
Comparison & self-esteem	Feeling inadequate; parenting guilt; body image issues	Remember the “highlight reel”; unfollow toxic accounts; practice gratitude
Time consumption	Excessive scrolling; sleep disruption; neglected responsibilities	Track screen time; set daily limits; create phone-free zones
Inappropriate content	Violent, explicit or harmful content; dangerous challenges	Use parental controls; keep devices in shared spaces; talk openly with children

Final advice for section 2.4

- You do not need to be an expert in technology to protect your family. The most powerful tool you have is open, honest communication with your children about their online experiences. Technology changes, but the trust between a parent and child is the foundation of safety in any environment; online or offline.

3. Social media profiles

3.1 What is a social media profile

A social media profile is a personal page that represents you on a social network. It usually includes information such as your name, profile picture, personal details and the content you share.

Your profile is the first thing other people see when they find you on a social network. It creates a first impression and determines how others perceive you online.

3.2 What information is included in a profile

Depending on the platform, a social media profile may include:

- Name and surname (or a username);
- Profile photo and cover photo;
- Date of birth;
- Location (city, country);
- Work and education information;
- Personal interests and hobbies;
- Posts, photos and videos you have shared;
- Friends or followers list.

⚠ Attention

Not all information needs to be shared on your profile. The more personal information you share publicly, the more vulnerable you may be to privacy risks. It is a good practice to share only what you are comfortable with everyone seeing.

3.3 Public vs. private profiles

Most social networks allow you to choose between a public and a private profile.

Public profile	Private profile
----------------	-----------------

Anyone can see your posts and information	Only people you approve can see your content
Search engines may index your profile	Your profile is not visible in search engines
Useful for professional purposes or public figures	Better for personal use and protecting family privacy

Tip for parents

- Consider setting your personal social media profiles to private, especially if you share content related to your children or family;
- Regularly review your privacy settings, as social networks sometimes change their policies;
- Check what information is visible to people who are not your friends or followers.

3.4 Managing and updating your profile

It is important to regularly review and update your social media profile to ensure that the information is accurate and that your privacy settings are appropriate.

Steps to review your social media profile

1. Open the social network and go to your profile page.
2. Check what information is visible (name, location, photos, posts).
3. Go to the privacy settings and review who can see your profile and posts.
4. Remove or hide any information you no longer want to be public.
5. Update your profile photo and cover photo if needed.
6. Check your friend or follower list and remove people you do not know.

Activity

Open one of your social media profiles (e.g., Facebook or Instagram).

1. Check your profile: what information is visible to everyone?
2. Is there any information you would like to remove or hide?
3. Are your privacy settings set to public or private?
4. When was the last time you reviewed your privacy settings?

3.5 Guiding your child's first profile

When a child reaches the minimum age requirement (usually 13) for social media platforms, parents have a crucial opportunity to guide the creation of their first profile safely and responsibly.

Key considerations before profile creation

- Age check and consent: Most major platforms require users to be at least 13 years old. Ensure your child understands this requirement.
- The “why”: Discuss why your child wants a profile and establish clear expectations about its purpose.
- The monitoring agreement: For younger teens, it is reasonable for a parent to have access to the account, especially during the initial months. This must be a transparent agreement based on trust.

Creating a safe first profile together

1. Choose a strong username: Select a username that does not contain the child's full name, date of birth or school name.
2. Set the profile to private: This is the most crucial step. A private profile ensures that only people the child approves can see their posts.
3. Use a safe profile photo: Choose a photo that does not reveal identifying background details (like a school logo or house number).

4. Review the bio/about section: Ensure the bio does not contain any personal information (age, location, phone number).
5. Review friends/followers: Teach your child the rule: Only accept requests from people you know in real life.
6. Activate parental controls: On certain platforms, enable the built-in parental settings to help manage time limits and monitor activity.

Essential safety rules for a new user

- Rule of Three: Teach your child to never post content that reveals their location, their phone number or their home/school address.
- Think Before You Post: Everything posted online is permanent. Ask: “Would I be comfortable if my teacher or future employer saw this?”
- Block and Report: Empower your child to block and report unwanted or mean messages immediately.

3.5.1 5 finger tools for strong standing for CyberHealth

The digital world often presents challenges in social interaction, where conflicts and unkindness can quickly escalate into cyberbullying. Beyond setting up technical controls, teaching children proactive, self-managed problem-solving strategies is essential for building digital resilience. One highly effective framework for empowering students to manage peer conflict, both online and offline, is the '5 Finger Tools' for strong standing in CyberHealth.

This method provides a structured, five-step problem-solving strategy that is easy for children and adolescents to remember and apply in a variety of challenging social situations. These situations can range from minor classroom disagreements to perceived bullying incidents in the playground or within online group chats. Implementing this as a whole-school approach can not only equip students with conflict resolution skills but can also contribute to eradicating bullying by providing a consistent, known response mechanism. The strategy emphasizes graduated responses, moving from the least confrontational actions to the most formal reporting mechanisms. Teaching these steps helps students avoid emotional, impulsive reactions, fostering a sense of control and competence when faced with peer pressure or hostility.

The Hi 5 Steps for Conflict Resolution:

1. Ignore: The first and simplest step. This tool is crucial for managing low-level annoyance or attention-seeking behavior. If an unwanted message or comment is not dangerous and is simply aimed at provoking a reaction, ignoring it takes away the power from the sender. This is particularly useful online, where responding to trolls or minor mean comments often fuels the behavior.

2. Talk Friendly: If the behavior is confusing or unintentional, the next step is to address it gently. A friendly response can clarify a misunderstanding or politely request the person to stop without escalating the conflict. For example, a child might say: "I think you misunderstood my post, it was just a joke," or "Could you please stop sending me those messages?"

3. Walk Away: If ignoring and talking friendly do not work, the physical or digital distance is necessary. In an online environment, this means closing the app, leaving the group chat, muting a user or blocking the profile. Walking away signals that the interaction is unacceptable and protects the child from further harm.

4. Talk Firmly: This step requires the child to use assertive communication. If the unwanted behavior continues, the child should clearly and firmly tell the person: "Stop that now. I don't like it," or "Do not tag me in posts like that again." This is an important lesson in setting and maintaining personal boundaries.

5. Report: If the firm talk does not stop the behavior, or if the incident is severe, immediate reporting is mandatory. The child should know to report the incident to a trusted adult (parent, teacher, school administrator). Online, this also involves using the platform's specific reporting tools (blocking, reporting the post/account). This ensures that adults are aware and can step in to handle the situation, especially when dealing with persistent harassment or serious cyberbullying.

By teaching the '5 Finger Tools' framework, parents can transition from being constant monitors to coaches, empowering their children to build the necessary social-emotional skills for healthy interactions in all areas of their lives, both digital and physical.

3.6 Fake accounts, bots and impersonation

The online environment is not always populated by genuine users. Fake accounts, automated bots and malicious impersonators pose a direct threat to privacy, safety and reliable communication.

Understanding non-genuine accounts

- Fake accounts: Profiles created using false identities, often to engage in scams, harassment or spread disinformation.
- Bots: Automated software programs that perform repetitive tasks, such as posting comments or sending mass messages.
- Impersonation: Creating a profile that deliberately copies a known person or organization to trick users into sharing private information.

Risks associated with fake profiles

- Phishing and scams: Fake accounts often use personalized information to craft convincing messages aimed at stealing passwords or money.
- Data harvesting: Bots are programmed to rapidly scrape public profile information and photos.
- Erosion of trust: Constant exposure to fake interactions makes it difficult for children to trust genuine connections.

How to spot a fake or bot account

- Profile picture: Often a stock image, a very attractive photo that seems too professional or no photo at all.
- Activity: They post excessively and rapidly, usually irrelevant or generic comments.
- Followers/Following: Very few followers or they follow thousands of accounts while having only a handful of posts.
- Username: Often consists of a real-sounding name followed by a long string of random numbers (e.g., jane_smith89457).

Verifying a suspicious friend request

1. Stop and check: Before accepting, examine the profile for red flags (generic photos, low activity, suspicious username).
2. Cross-reference: If the profile claims to be someone you know, search for the person's original, established account.
3. Use an alternative channel: Contact the real person directly via text message or phone call and ask: "Did you just send me a new friend request?"
4. Block and report: If the account cannot be verified or is clearly malicious, immediately block and report it.

Example from everyday life

A teenager receives a message from a new account claiming to be a friend who "lost their phone and is locked out." The account asks for the teenager's password to retrieve a shared photo. The parent, having discussed fake accounts, prompts the child to verify the request through a different channel (like a quick phone call to the real friend's parent) before sharing any sensitive information.

Attention

Teach your child to treat unsolicited messages from strangers, especially those asking for urgent help or personal information, with extreme skepticism. The core rule is: Never share passwords, financial details or identifying information with an unverified account.

3.7 Online image and reputation management

In the digital age, a social media profile is more than just a personal diary; it is often a public portfolio that impacts how others perceive a person. Managing one's online image and reputation is crucial for long-term success and well-being.

The long-term impact of online content

- Professional screening: A high percentage of employers and university admissions officers review applicants' social media profiles.

- Context loss: Content posted in a specific context can be easily taken out of context years later.
- Future opportunities: An image or post deemed inappropriate today can prevent a teenager from getting an internship, a scholarship or a job years later.

Guiding your child on online image

- Consistency: Encourage your child to maintain a consistent and authentic image that reflects their true values.
- The “Grandma Rule”: Teach your child to pause before posting and ask: “Would I be comfortable if my strictest teacher, my future boss or my grandmother saw this?”
- Focus on positive contribution: Encourage them to share content that reflects their interests, achievements and positive contributions.

Activity

Imagine your child is applying for their dream job in five years.

1. What are three positive things they are passionate about that their profile should highlight?
2. What kind of content would you want them to remove now to avoid embarrassment in the future?
3. Discuss the distinction between a personal journal (which should be kept private) and a social media profile (which is a form of public communication).

3.8 Advanced profile security

While simply setting a profile to private is a necessary first step, strong digital security requires technical measures to protect accounts from unauthorized access, hacking and data theft.

Moving beyond basic passwords

- Strong, unique passwords: A strong password should be long (12+ characters), use a mix of uppercase and lowercase letters, numbers and symbols. Every account must have a unique password.

- Password managers: Encourage the use of a reputable password manager (e.g., Google Password Manager, LastPass, 1Password) to safely generate and store complex, unique passwords.

Two-Factor Authentication (2FA)

Two-Factor Authentication is the single most effective way to prevent unauthorized access.

- How 2FA works: Even if a hacker knows the username and password, they cannot log in without the second factor; a unique, temporary code sent to the user's phone or authenticator app.
- Why it matters: If your child's password is stolen in a data breach, 2FA ensures their account remains locked to the thief.
- The best method: Authenticator apps (like Google Authenticator or Authy) are generally considered safer than codes sent via text message.

Setting up 2-Step Verification

1. Go to Settings: On the social media platform, navigate to "Settings" or "Security and Login."
2. Find 2FA: Locate the "Two-Factor Authentication" or "2-Step Verification" option.
3. Choose a method: Select your preferred security method (e.g., Authenticator App, Text Message or Security Key).
4. Follow prompts: The system will generate backup codes (which you must save offline) and guide you through the setup.
5. Test it: Log out and log back in to ensure the process works correctly.

Attention

Never share your 2FA code with anyone, even if they claim to be from the platform's support team. Customer support will never ask for your one-time login code.

Activity

1. On your primary social media account, check if Two-Factor Authentication is enabled.

2. If it is not enabled, use the step-by-step guide above to activate it.
3. Discuss with your child the concept of 2FA. Why is it safer than just a password?

3.9 Platform-specific profile differences

The same person may have different social media profiles and each one should be structured and managed differently, reflecting the distinct purpose of the platform.

Platform Type	Primary Purpose	Key Profile Info	Recommended Privacy
Professional (e.g., LinkedIn)	Networking, career development	Work history, skills, education	Public; needs to be discoverable
Visual (e.g., Instagram, TikTok)	Entertainment, peer communication	Hobbies, personal updates, creativity	Private, especially for teens
Communication (e.g., WhatsApp)	Private, immediate messaging	Phone number, last seen status	Strictly private, minimal info

The importance of audience and tone

Encourage children and teenagers to consider their audience before posting on any platform. A common mistake is treating all profiles the same. Posting casual content on a professional profile can damage credibility, just as sharing personal details on a public entertainment profile can compromise safety.

Example from everyday life

A college-bound teenager is using three platforms: LinkedIn for a scholarship application, Instagram for friends and TikTok for funny videos. The parent helps the teen understand that the photo used on LinkedIn must be professional, the Instagram profile should be private and the TikTok profile should never feature their full name or college details, keeping the professional and private lives separate.

Reviewing Platform Terms of Service

- When your child creates a new profile, make it a family habit to spend 10 minutes reviewing the platform's Terms of Service and Privacy Policy together. Focus on two questions: 1) What is the minimum age? 2) What content is the platform explicitly prohibited?

Activity

Choose three different social media platforms you or your child use.

1. For each, define the ideal audience (e.g., family, colleagues, classmates).
2. What is the riskiest type of information to share on each of these three platforms?
3. Review the privacy settings for each platform to ensure they match the platform's purpose.

4. Digital footprint

4.1 What is a digital footprint

Every time we use the internet, we leave traces of our activity. These traces are called our digital footprint. It includes everything we do online: the websites we visit, the messages we send, the photos we post, the purchases we make and even the searches we perform.

A digital footprint can be **active** or **passive**.

Active digital footprint

This is the information we deliberately share online. Examples include:

- Posts, comments and photos on social media;
- Filling out online forms;
- Sending emails;
- Creating accounts on websites or apps.

Passive digital footprint

This is information collected about us without our direct action. Examples include:

- Websites tracking our browsing history through cookies;
- Location data collected by apps on our phone;
- Advertising companies tracking our online behavior to show targeted ads.

4.2 Why does your digital footprint matter

Your digital footprint can have real consequences in your life:

- Employers may search your name online before hiring you;
- Schools or organizations may check your social media activity;
- Information posted online can be difficult or impossible to completely remove;
- Personal data can be used by third parties for advertising, scams or identity theft.

⚠ Attention

Once something is posted on the internet, it can be very difficult to fully remove. Even if you delete a post, someone may have already saved or shared it. This is especially important to consider before posting photos of children.

4.3 Managing your digital footprint

While we cannot completely avoid leaving a digital footprint, we can take steps to manage it:

- Think before posting: Ask yourself: “Would I be comfortable if this were seen by everyone?”
- Regularly review your social media profiles and remove old or unwanted content;
- Use privacy settings to control who can see your information;
- Be careful about which apps and websites you give permission to access your data;
- Search your own name on a search engine to see what information about you is publicly available.

How to check your digital footprint

1. Open a search engine (e.g., Google).
2. Type your full name in the search bar.
3. Look at the results: what information about you is visible?
4. Check the images tab as well to see if any photos of you appear.
5. If you find information you want to remove, visit the relevant website and look for options to delete your account or request removal.

4.4 Your children’s digital footprint

Parents play a crucial role in shaping their children’s digital footprint, often even before the child starts using the internet themselves.

The practice of parents sharing information, photos and stories about their children on social media is sometimes called “**sharenting**” (a combination of “sharing” and “parenting”). While sharing proud moments about children is natural, it is important to consider the potential consequences.

Before sharing content about your children, ask yourself:

- Who can see these photos and posts?
- Could this content embarrass the child in the future?
- Does the photo include information that could reveal the child’s location (school uniform, address, etc.)?
- Has the child (if old enough) given their consent?

Tips for protecting your child’s digital footprint

- Avoid posting photos that reveal your child’s school, address or daily routine;
- Use privacy settings so that only trusted people can see photos of your children;
- Ask your child’s permission before posting their photos, especially as they get older;
- Talk to your children about the importance of thinking before sharing content online.

Activity

Search your name and your children’s names on Google.

1. What information appears in the results?
2. Are there any photos of you or your children that you did not expect to find?
3. Are there any steps you would like to take to reduce your digital footprint?

4.5 The persistence and permanence of the footprint

Many people believe that deleting a photo or post completely removes it from the internet. This is a dangerous misconception. The reality is that the internet has a long memory and true digital erasure is nearly impossible.

- Caching and indexing: Search engines frequently save temporary copies of content. Even after a user deletes the original post, the cached copy can persist for a significant time.
- Third-party data aggregation: Data brokers and various third-party apps may have already collected and stored the information.
- Screenshots and resharing: Once content is shared, it can be screenshotted, downloaded and distributed globally outside of the original platform's control.

The Right to Be Forgotten

While legislation like the GDPR provides citizens in some regions with a “Right to Be Forgotten,” this right is limited. It primarily compels search engines to de-list certain search results, but it does not remove the information from the original website or from archives.

⚠ Attention

Teach your children that the moment they hit “post,” they should consider that information permanent. The goal is not to delete, but to prevent the creation of damaging content in the first place.

4.6 The footprint and future opportunities

A positive digital footprint is increasingly seen as a necessary part of a competitive profile for education and career advancement. Conversely, a negative footprint can serve as an automatic gatekeeper.

Academic and professional screening

- University admissions committees often review a candidate's public online presence to assess character and judgment.
- Scholarship committees view social media as a quick way to vet candidates. Inappropriate posts can lead to the loss of funding.
- Studies consistently show that a large percentage of employers use social media screening as part of the hiring process.

Building a positive online portfolio

- Highlight achievements: Use platforms to share achievements, projects, volunteer work or positive contributions.
- Show passion: Engage in relevant online discussions related to desired fields of study or career.
- Professional communication: Always maintain respectful and articulate communication, even in casual posts.

Tip for families

- Encourage your child to think of their online presence as a long-term portfolio. Just as they would carefully prepare a CV, their social media should reflect their best qualities and interests.

4.7 Auditing and cleaning up old footprints

Parents and children should periodically engage in a comprehensive digital cleanup to minimize risk.

Steps for a comprehensive digital audit

1. Search engine deep dive: Use multiple search terms (full name, old usernames, email addresses) across different search engines (Google, Bing) and check all tabs (Web, Images, Video).
2. Social media review: Review old posts, comments and photos on every social media account. Use the “View As” feature (if available) to see what a stranger sees. Delete or archive anything potentially embarrassing.
3. Third-party connections: Review the settings on major accounts (e.g., Google or Facebook) to see a list of every third-party app with access to your data. Revoke access to any unused or suspicious apps.
4. Old account deactivation: Identify any old accounts (from forgotten games, forums or old projects) and follow the specific steps to deactivate or permanently delete them.

4.8 Digital shadows: the footprint left by others

An individual's digital footprint is often a mix of their own actions and the actions of others. Managing this “digital shadow” is vital, especially for teenagers who are frequently tagged by friends or mentioned by family.

Managing tagged content

- Review and approval: Most platforms offer a setting that requires the user to review and manually approve any photo or post they are tagged in before it becomes visible. This is a critical setting for teens to enable.
- Untagging: Teach children how to untag themselves from inappropriate or unwanted photos. If the content remains public, they should ask the person who posted it to remove it.
- Public mentions: Be aware of content that mentions your child's name without a tag (e.g., a news article, a blog post). This requires regular search engine monitoring.

The sharenting legacy

Parents' historical sharenting (photos posted from childhood) forms a significant part of their child's early digital shadow. As children become teenagers, parents should involve them in the decision-making process for this legacy content.

- Consent: Honor the teen's request to remove or archive content from their childhood that they find embarrassing. This respects their developing autonomy and builds trust.
- Privacy settings: Ensure all older posts featuring the child are restricted to “Friends Only” or an even narrower list of trusted family members.

Activity: The digital shadow check

1. Ask your child to look at their profile. How many people are allowed to tag them in photos without their approval?
2. Review the last five photos they were tagged in by friends. Do these photos accurately represent the image they want to project?

3. Discuss a piece of content you (the parent) posted about them when they were younger. Ask them directly: “Do you want this content to remain online?”

5. Social media addiction

5.1 What is social media addiction

Social media platforms are designed to be engaging. They use features like notifications, likes, comments and personalized content feeds to keep users coming back and spending more time on the platform.

For some people, this engagement can become excessive. When a person feels unable to stop using social media, experiences anxiety when not online or allows social media to interfere with their daily responsibilities, this may be a sign of social media addiction.

Social media addiction is not yet officially classified as a clinical disorder in most medical systems, but research increasingly shows that **excessive social media use can have significant effects on mental health, relationships and daily functioning.**

5.2 Signs of excessive social media use

It is important to recognize when social media use becomes problematic. Some common signs include:

- Checking your phone or social media first thing in the morning and last thing at night;
- Feeling anxious or restless when you cannot access social media;
- Spending more time on social media than intended;
- Neglecting responsibilities, hobbies or face-to-face relationships because of social media;
- Comparing yourself to others on social media and feeling inadequate;
- Using social media to cope with negative emotions (boredom, loneliness, stress).

5.3 The psychology behind social media engagement

Social media platforms are designed by teams of engineers and psychologists to maximize user engagement. Understanding the mechanisms involved can help us be more aware:

- Dopamine loops: Every like, comment or notification triggers a small release of dopamine, which makes us want to check back for more;
- Fear of Missing Out (FOMO): Seeing others' posts about activities can create a feeling that we are missing out;
- Variable rewards: Social media feeds are unpredictable, which keeps us scrolling, similar to slot machines;
- Social validation: The number of likes, comments and followers can become a measure of self-worth.

5.4 Effects on parents and family life

Excessive social media use by parents can affect family dynamics:

- Reduced quality time with children: Being on the phone during family moments sends a message that the screen is more important;
- Modeling behavior: If parents are constantly on their phones, children are likely to develop similar habits;
- Emotional impact: Comparing oneself to “perfect” families can lead to feelings of inadequacy or guilt;
- Sleep disruption: Using social media before bed can affect sleep quality.



Example from everyday life

A parent realizes that every evening, instead of spending time with their children, they spend over an hour scrolling through Instagram and Facebook. The children start asking for their own phones, saying: “You’re always on your phone too.” This moment becomes a wake-up call for the parent to reconsider their own habits.

5.5 Children and social media addiction

Children and teenagers are especially vulnerable to social media addiction because:

- Their brains are still developing, particularly the areas responsible for impulse control and decision-making;

- Social media plays a significant role in their social life and identity formation;
- They may not yet have the skills to self-regulate their screen time;
- Peer pressure and the desire to fit in can drive excessive use.

Signs that a child may be struggling with excessive social media use include:

- Becoming irritable or upset when asked to stop using their phone;
- Declining interest in activities they used to enjoy;
- Changes in sleep patterns;
- Withdrawal from family interactions;
- Secretive behavior about their online activities.

5.6 Strategies for healthier social media habits

Both parents and children can benefit from developing healthier habits around social media use.

For parents

- Set specific times for checking social media and stick to them;
- Use “screen time” features on your phone to track and limit your social media use;
- Create “phone-free zones” at home (e.g., during meals, in bedrooms);
- Turn off non-essential notifications to reduce the urge to check your phone;
- Before opening a social media app, ask yourself: “What am I looking for?” If there is no specific purpose, consider doing something else.

For families

- Establish a “family media agreement” that sets rules for screen time for everyone, including parents;
- Plan regular activities that do not involve screens (board games, outdoor activities, cooking together);
- Talk openly about social media experiences: what is enjoyable, what is stressful and what is concerning;

- Use social media together sometimes: watch a video, explore an interesting page or discuss a post.

The “3 Questions” approach before using social media

- Before picking up your phone, ask yourself:
 1. Why am I opening this app? (Purpose)
 2. How long will I spend on it? (Time limit)
 3. How will I feel after using it? (Emotional impact)

Activity

For one week, track your daily social media usage using your phone’s built-in screen time tracker.

1. How many hours per day do you spend on social media?
2. Which app do you use the most?
3. Are you surprised by the results?
4. What is one change you could make to reduce your screen time?

5.7 Social media, blue light and sleep deprivation

The direct link between screen time, particularly in the evening and poor sleep quality is a major concern for both children and adults.

The role of blue light and notifications

- Blue light suppression: Digital screens emit blue light, which suppresses melatonin production, delaying sleep onset and reducing rest quality.
- Cognitive arousal: Engaging with stimulating content activates the brain, making it difficult to transition into a restful state.
- The urge to check: The constant stream of notifications keeps users in a state of hypervigilance, preventing deep relaxation.

Strategies for protecting sleep

- The one-hour rule: Implement a strict rule: no screens for at least one hour before bedtime.
- Charging station: Charge all family devices in a central location outside of bedrooms overnight.
- Use blue light filters: Activate “Night Shift” (Apple) or “Blue Light Filter” (Android) settings in the evenings.

⚠ Attention

A lack of quality sleep has severe consequences for young people, including reduced attention span, increased irritability, impaired learning and a higher risk of anxiety and depression. Protecting sleep is one of the most critical aspects of digital well-being.

5.8 Assessing dependency: the difference between habit and addiction

A strong habit, such as checking a phone often, is not the same as a dependency or addiction.

Parents need objective criteria to determine when social media use crosses the line into a problematic pattern.

The criteria for problematic use

- Tolerance: The need to spend increasing amounts of time online to achieve the same level of satisfaction.
- Withdrawal: Experiencing negative mood states (anxiety, irritability, restlessness) when unable to access social media.
- Loss of control: Repeated unsuccessful attempts to cut down or stop social media use.
- Neglect of responsibilities: Prioritizing social media over significant life activities such as homework, personal hygiene or family time.
- Deception: Lying to parents or others about the amount of time spent online.
- Continued use despite problems: Continuing to use social media even after realizing it is causing significant problems.

■ Professional screening approach

1. Consider using this adapted screening: Does your child use social media to Calm down, Relax, Avoid problems, Forget feelings, Feel better or get Thrills? (C-R-A-F-F-T)
2. If the answer is consistently yes to multiple items, the use may be serving an unhealthy coping function.
3. Consult a school counselor or mental health professional for a proper assessment.

5.9 Implementing a family digital detox

A planned digital detox is a structured, temporary break from screens or social media. It serves as a necessary reset, helping both parents and children break compulsive habits and rediscover alternative activities.

Goals of a digital detox

- Habit disruption: To break the automatic reflex of checking the phone during every moment of boredom.
- Rediscover analog life: To shift attention back to physical activities, reading, hobbies and family interactions.
- Identify triggers: To become aware of the emotional states that trigger the urge to check social media.

Planning a family digital fast (24-72 hours)

1. Set clear boundaries: Define exactly what is out (all social media, non-essential apps, gaming) and what is in (essential communication like phone calls for emergencies, school work).
2. Plan alternative activities: Before the fast begins, plan several screen-free, engaging activities (e.g., cooking a new recipe, hiking, board game tournament, family art project).
3. Manage expectations: Discuss that withdrawal symptoms (boredom, irritability, “phantom vibrations”) are normal and temporary.
4. Hold a review session: After the fast, discuss the experience: What was the hardest part? What did you enjoy doing instead? What permanent changes will you make?

5.10 When and how to seek professional help

While most excessive use issues can be managed with healthy boundaries and family rules, some cases of dependency are severe enough to require intervention from a qualified mental health professional.

Recognizing the need for professional help

Seek professional support if the child's social media use is consistently associated with:

- Severe functional impairment: The child is failing school, has completely withdrawn from peers and family or has significant sleep/eating disorders.
- Co-occurring issues: The dependency is clearly linked to or worsening underlying mental health issues (e.g., severe depression, anxiety disorders).
- Failure of intervention: Previous, consistent attempts to implement family boundaries have failed or symptoms rapidly return after a break.
- Self-harm or suicidal ideation: The child is using social media to engage in self-harm communities or shows any signs of suicidal ideation. In this case, seek immediate crisis intervention.

Who to contact

- School counselor or psychologist: A good first point of contact for assessment and early intervention.
- Pediatrician: Can rule out physical causes and provide referrals to specialists.
- Clinical psychologist or specialized therapist: Look for professionals with expertise in behavioral addictions or cognitive-behavioral therapy (CBT).

Seeking help is a sign of strength, not failure. Specialized professionals can provide personalized strategies, help the child develop coping mechanisms and support the family in creating a sustainable, healthier environment.

6. Digital parenting: guiding your child's online communication

6.1 Why digital parenting matters

Children today grow up in a digital world. They start using smartphones, tablets and the internet at increasingly younger ages. While technology offers many learning and entertainment opportunities, it also exposes children to risks that they may not yet understand.

Digital parenting means being actively involved in your child's digital life; not to control every action, but to guide, support and educate them so they can use technology safely and responsibly.

6.2 Talking to your children about online communication

Open and ongoing conversations about online communication are one of the most important tools parents have. Topics to discuss with your children:

- Who do they communicate with online? Do they know all the people they interact with?
- What information do they share in messages and posts?
- Have they ever felt uncomfortable because of something someone said to them online?
- Do they understand that messages and photos sent online can be permanent?
- Do they know how to block or report someone who is being hurtful?

Tips for having productive conversations about digital life

- Be curious, not judgmental: ask questions to understand, not to lecture;
- Share your own experiences with technology, including your own challenges;
- Make it a regular conversation, not just a one-time talk;
- Focus on situations, not on punishment: children are more likely to come to you with problems if they do not fear being punished;
- Acknowledge that the online world is an important part of their social life.

6.3 Setting boundaries together

Rather than imposing strict rules without explanation, research shows that collaboratively setting boundaries with children is more effective. This approach helps children understand the reasons behind the rules, builds their ability to self-regulate and strengthens the parent-child relationship.

A **family media agreement** can be a useful tool. This is a simple document that the whole family creates together, outlining the rules and expectations for using technology at home.

A family media agreement might include:

- Agreed screen time limits for each family member;
- Phone-free times (e.g., during meals, after a certain hour at night);
- Rules about downloading apps or creating new accounts;
- What to do if something upsetting happens online;
- The understanding that parents may occasionally check in on younger children's online activity.

6.4 Parental control tools

Parental control tools can help parents manage their children's online activities:

- Limit screen time and app usage;
- Filter inappropriate content;
- Location tracking;
- Monitor online activity;
- Set age-appropriate restrictions.

Common parental control options include:

- Google Family Link (for Android devices);
- Apple Screen Time (for Apple devices);
- Built-in parental controls on game consoles and streaming services;
- Router-level controls that apply to the entire home network.

⚠ Attention

Parental controls are a useful tool, but they should not replace open communication with your child. Children who understand why certain limits exist are more likely to follow them even when they are not being monitored.

Activity

Sit down with your child and discuss the idea of creating a family media agreement.

1. What rules do both of you think are important?
2. What screen time limits seem fair for everyone?
3. What should happen if someone in the family breaks the agreement?
4. Write the agreement together and place it somewhere visible at home.

6.5 Creating a safe zone for disclosure

The primary goal of digital parenting is to ensure the child feels safe enough to come to the parent immediately when something goes wrong online. This requires creating a “safe zone” in the relationship where fear of punishment does not override the need for safety.

Key to openness: focusing on support, not consequences

- The “Tell Me First” rule: Establish a family rule that if anything scary, confusing or upsetting happens online, the child’s only immediate responsibility is to close the screen and tell a trusted adult. Reassure them that the consequence for telling will always be support, not punishment.
- Validate, don’t judge: If a child comes to you, start by thanking them for their bravery and focusing on their feelings, not the mistake they might have made.
- Model calmness: When a child discloses a danger, the parent’s immediate reaction teaches the child how safe it is to share next time.
- Collaborative problem solving: Instead of dictating a solution, involve the child in deciding the next steps. This empowers them and avoids generating fear.

Example from everyday life

A 14-year-old receives a suspicious message from a stranger asking for photos. The child hesitates for an hour, afraid of losing their phone. Remembering their family's "Tell Me First" rule, they show the parent. The parent's first response is, "I am so proud of you for showing me this. This is serious and we will handle it together." The parent thanks them, blocks the user, reports the account and discusses the risk without mentioning punishment.

Attention

The immediate fear of a child is often the loss of the device, which is their social lifeline. If you must remove the device for security reasons, be clear that this is a temporary safety measure, not a punishment for coming forward.

6.6 The “monitoring vs. trust” dilemma

Parenting in the digital age presents the ethical challenge of deciding how much to monitor a child's online activities. The goal is to balance essential security concerns with respecting a child's growing need for privacy.

The spectrum of parental involvement

Parental involvement ranges from full, transparent monitoring (necessary for young children) to relying on mutual trust and check-ins (appropriate for older teens).

- Age appropriateness: For young children (under 13), monitoring is a necessary safety tool. Explain why it is used (safety, not spying).
- Teenagers and privacy: For teenagers, routine, secret monitoring can break trust. Shift from reading their messages to reviewing app usage trends and having open conversations.
- Before a child reaches their country's legally mandated age (mostly 13; 14 in Spain, 15 in France, 16 in Germany), they cannot independently agree to data collection. It is entirely up to the parent or guardian to grant explicit consent, meaning the parent assumes full legal and practical responsibility for the child's presence on that platform.

Finding the balance

- Focus on trust-building monitoring: Instead of monitoring content, focus on monitoring behavior. Monitor screen time limits, app downloads and privacy settings, which are technical boundaries agreed upon in the family media agreement. This shows that you trust them but still uphold the rules.

Attention

Trust is a vital part of digital resilience. If a child feels constantly spied upon, they lose the opportunity to develop independent judgment and problem-solving skills.

Activity: Family privacy talk

Discuss with your teen: “What information on your phone do you consider private and what information do you feel comfortable sharing with me for your safety?”

Use this as a starting point to agree on a monitoring strategy that respects their boundaries while ensuring essential safety checks.

6.7 Handling online stranger danger

This section addresses the critical safety risks of interacting with unknown people online and establishes strict rules for meeting online contacts in person.

The online stranger paradox

In the digital world, the line between “friend” and “stranger” is blurred. A child may interact with an online acquaintance daily for months, leading them to feel they “know” this person, even though they have never met them in person.

Key risks of online strangers

- Grooming: Adults may pose as children or teens to build trust, often leading to inappropriate requests and sharing inappropriate content.
- Identity deception: People online can easily lie about their age, gender and intentions.

- Scams and phishing: Strangers often initiate contact as part of a financial scam or to steal personal information.

Safety rules for online contacts

1. Rule 1: Never share personal data: Never give an online contact your full name, home address, school, phone number or a photo of your house.
2. Rule 2: Never accept money or gifts: Refuse any offer of money, gifts or favors, as this is a common tactic to create obligation.
3. Rule 3: Report and block: Immediately report and block any contact who asks for private photos, seems sexually suggestive or asks to meet up. It is okay to block or report anyone who makes you feel uncomfortable in any way.

The Safest Approach: Avoiding Real-Life Meetings

The absolute safest and most risk-free policy is for children to **never** meet **online-only** contacts in real life. Avoiding physical meetings altogether is the best way to eliminate real-world risks. However, if a meeting is deemed completely unavoidable, simply bringing a friend is never sufficient protection. The following strict, non-negotiable rules must apply:

- **Mandatory Parental Presence:** A parent or guardian must be fully informed and physically present at the meeting.
- **Public Place Only:** The meeting must take place in a highly visible, crowded, and public location.

Attention

Teach your child that a friend who is truly safe and genuine will respect these boundaries. Any online friend who pressures them to break these rules or keep the meeting secret is an immediate red flag.

Activity: What-if scenario

Ask your child: “If your online gaming friend said they were coming to your city and wanted to meet you at the park tomorrow, what would you say?”

Use their answer to practice the official family procedure for meeting online contacts.

6.8 Teaching digital empathy and kindness

This moves beyond basic netiquette to emphasize emotional intelligence online, focusing on how parents must model kind, respectful and measured communication and actively teach children about the impact of their words on others.

The disinhibition effect

Online communication often leads to a “disinhibition effect,” where people say things they would never say in person. This is due to anonymity, lack of face-to-face cues and the feeling that the online world is less “real.”

Modeling digital kindness

- Emotional pause: Model pausing before reacting to an angry message. Say out loud, “That comment made me angry, so I am going to wait ten minutes before I reply.”
- Focus on the human: Teach children that there is always a real person with real feelings behind every profile.
- Apologizing online: If a child makes a mistake, guide them on how to apologize genuinely, teaching them accountability.

Empathy and critical thinking

- Encourage your child to practice perspective-taking: “If you posted that comment, how might the person receiving it feel?” Discuss the permanent damage of cyberbullying and how even seemingly harmless comments can contribute to a toxic environment.

Attention

The greatest risk to a child's online reputation is often poor communication skills driven by impulsive emotional reactions. Teaching them to pause, take a breath and choose empathy is an essential life skill.

Activity: The “Re-read” rule

When your child is drafting a response to a disagreement or a critical post, introduce the “Re-read” rule: Before hitting send, read the message out loud in the meanest voice possible. If it sounds too harsh, rewrite it.

6.9 Building digital resilience and critical thinking

This section shifts the focus from relying on parental controls to equipping the child with the mental tools to handle risks independently. Digital resilience is the ability to navigate online challenges, recover quickly from negative experiences and make safe choices independently.

Core components of digital resilience

- Critical information consumption: Teach children to be skeptics; questioning the source, identifying emotional manipulation and recognizing that not everything they see is real or true.
- Scam recognition: Teach them how to identify common digital traps: urgent messages requiring a password, free offers that seem too good to be true and links sent by unfamiliar sources.
- Emotional regulation: Equip them with techniques to manage strong feelings triggered by negative content or cyberbullying.
- Know how to report: Ensure the child knows the specific steps to block, mute and report abusive content on all their platforms.

The goal is to move the child from thinking, “What should Mom or Dad do?” to “What is the safest action I can take right now?” This shift in ownership builds self-efficacy and confidence.

The “Stop, Think, Act” method

- Teach your child this simple process when facing a risky or upsetting situation online:

- Stop: Pause, close the screen and take a deep breath. Do not react immediately.
- Think: Is this real? Is this safe? Does this make me feel scared? Who should I tell?
- Act: Block, report and tell a trusted adult.

⚠ Attention

The digital environment will continue to evolve, introducing new threats. The most future-proof skill a child can possess is critical thinking; the ability to evaluate new information and risks independently.

Activity: App review

Go through a new app your child wants to download. Instead of saying “yes” or “no,” ask them to lead the review: “What are three rules we should set for this app and what is the biggest danger you think it has?”

Recap: the main ideas of the chapter

The table below summarizes the main things we have discussed in this chapter.

Theme	What is important to remember
Online communication	Online communication can be synchronous or asynchronous. Choosing the right tool and being respectful helps avoid misunderstandings.
Social networks	Social networks are useful for connecting with others, but they also carry risks related to privacy, misinformation and excessive use.
Social media profiles	Your profile is your online identity. Control what information is visible, keep profiles private when possible, be aware of your digital footprints, use strong passwords and 2FA and be aware of fake accounts.
Digital footprint	Everything we do online leaves a trace. Managing our digital footprint helps protect our privacy and reputation. Content is effectively permanent once posted.
Social media addiction	Social media is designed to be engaging. Recognizing signs of excessive use, understanding the psychology behind it, protecting sleep and setting healthy boundaries is important for both parents and children.
Digital parenting	Open communication, collaborative rule-setting, creating a safe zone for disclosure, teaching empathy and resilience and understanding your child's digital world are key to effective digital parenting.

Advice for parents

- The internet and social media are a significant part of modern life. Rather than avoiding them, learning to use them wisely; and teaching our children to do the same; is the most effective approach.

Quick Self-Assessment Test

Check what you've learned

Read the statements below and check the options you consider correct.

- ☐ Online communication can be synchronous (real-time) or asynchronous (not in real time).
- ☐ It is important to think about tone and clarity when communicating online, as body language is absent.
- ☐ Social networks use algorithms to decide what content to show us.
- ☐ Setting your social media profile to private helps protect your personal information.
- ☐ A digital footprint includes everything we do online, both active and passive traces.
- ☐ Sharing photos of children online (“sharenting”) should be done carefully, considering privacy.
- ☐ Social media is designed to be engaging and excessive use can affect mental health and family life.
- ☐ Open communication with children about their digital life is more effective than strict control alone.
- ☐ Two-Factor Authentication (2FA) is one of the most effective ways to protect online accounts.
- ☐ Teaching children digital empathy and resilience is as important as using parental control tools.

Once you've completed the exercise, discuss your answers with other participants or your trainer.

How can we use this knowledge in everyday life

How this chapter can help us

- The information in this chapter can be useful in many everyday situations.

For example, we can use this knowledge to:

- Communicate more effectively and respectfully with others online;
- Understand how social networks work and use them more consciously;
- Review and improve our social media profiles and privacy settings;
- Be aware of the digital footprint we leave online and manage it actively;
- Recognize signs of excessive social media use in ourselves and our children;
- Have open and productive conversations with our children about their online activities;
- Set healthy boundaries around technology use for the whole family;
- Recognize fake accounts, misinformation and online scams;
- Build digital resilience and empathy in our children.

Using digital communication wisely and understanding the impact of social media on our lives can help us build healthier relationships with technology; and help our children do the same.

CHAPTER III

1. Antivirus software – necessity or fad

To establish a clear foundation for digital safety, it is essential to first define its core tool: an antivirus is a software program that acts like a digital immune system, quietly running in the background to detect, block, and remove harmful threats before they can damage your devices, prevent catastrophic data loss and safeguard your digital identity from unauthorized access. In the early days of the personal computer, an antivirus was often seen as a luxury or a specialized tool for those who spent their lives on the "darker" corners of the web. Many people believed that as long as they didn't visit suspicious websites, they were perfectly safe. In 2026, the reality is vastly different. The internet is now a fundamental utility, like electricity or water, and just as we wouldn't want a leak in our pipes, we cannot afford a leak in our digital security.

When we talk about digital security, the essential starting point typically introduced to users for safeguarding personal data and devices is antivirus software. For many years, antivirus programs have been presented as essential tools to protect computers from viruses and cyberattacks. However, today many people wonder whether they are still necessary or if they are simply an outdated solution.

This question is particularly relevant for families, where multiple devices are used daily by both adults and children. Understanding whether antivirus software is truly needed helps families make informed decisions about how to protect their digital environment. To answer this question, it is important to understand how digital threats work and how antivirus software contributes to protecting devices and personal data.

The truth lies somewhere in between: antivirus software is not a magical solution that guarantees complete safety, but it is also far from being useless. It is one of several tools that, when combined with proactive digital habits, including regular system updates, avoiding suspicious links, downloading software exclusively from verified official sources and exercising caution with email attachments, can significantly reduce online risks such as the stealthy theft of online credentials,

financial fraud, and the catastrophic loss of irreplaceable family files or photos to ransomware encryption.

The debate over whether antivirus software is a "necessity or a fad" often stems from a misunderstanding of how modern cyber-attacks work. Today's threats are silent and invisible. They don't always wait for you to make a mistake; they actively seek out vulnerabilities in the devices that have become extensions of our personalities. This section will help you understand that while your behaviour is the first line of defence, a reliable antivirus is the safety net that catches the dangers the human eye simply cannot see.

1.1 What is an antivirus and how it works

Today, antivirus software is often part of a larger security system that may include firewalls, web protection, and tools to block dangerous websites.

An antivirus is a specialized program that monitors your device's "health" in real-time. It acts as a digital bodyguard, constantly vetting every file and program that tries to run on your system. It primarily uses two methods to keep you safe:

- **Signature Matching:** The software maintains a massive library of "digital fingerprints" of every known virus. Every time you download a file, the software checks it against this library.
- **Behavioural Monitoring (Heuristics):** This is the "smart" part of the software. It watches for programs that act suspiciously—such as a simple calculator app suddenly trying to access your microphone or a document trying to change your system settings. In modern cybersecurity, this has evolved into **AI-assisted Behavioural Monitoring**. Thanks to the integration of Artificial Intelligence and machine learning, the antivirus does not limit itself to searching for threats already catalogued in its database. The software observes the computer's behaviour in real time, learns to recognize operational anomalies, and instantly blocks any suspicious activity, neutralizing even viruses created just moments prior and never seen before.

To choose the right tool to block, detect and remove malware, which includes viruses, Trojans (malicious programs disguised as legitimate software, games, documents, or updates in order to

trick users into installing them voluntarily), spyware, ransomware, and other harmful programs that can damage devices and/or steal personal information, it is important to understand the different typologies available which primarily include built-in operating system defences and independent third-party software such as Avast, Norton, Malwarebytes etc. Among the most common threats families may encounter are Trojans, spyware, and ransomware. While Trojans disguise themselves as legitimate software in order to trick users into installing them, spyware is designed to remain hidden and silently collect information about user activity. Some forms of spyware, known as keyloggers, can even record everything typed on a keyboard, including passwords, PIN codes, and payment information. Ransomware operates differently: rather than remaining hidden, it typically reveals its presence by locking files or devices and demanding payment in exchange for restoring access. Whether a family chooses to utilize a baseline free tool or invest in a paid subscription depends heavily on their specific digital habits and risk exposure. For basic users whose online activity is limited to reading news, watching official streaming services, the probability of encountering sophisticated cyberattacks is generally lower, meaning they might have less immediate need for advanced premium add-ons. However, robust protection remains essential for every user, as even basic activities carry some risk. If household members frequently engage in online banking, remote work, online shopping, or intensive downloading of files and games, upgrading to a paid premium subscription becomes a critical priority. These subscriptions unlock essential advanced features like ransomware protection, secure VPNs (Virtual Private Network), identity theft monitoring, and integrated parental controls for multiple devices, offering a vital shield for households exposed to higher digital risks. When it comes to acquiring these programs, knowing how and from where to download them is a critical safety step, as cybercriminals often disguise malware as security software. Users must exclusively download third-party antivirus programs from the official, verified websites of the respective vendors or through legitimate marketplaces such as the Microsoft Store and the Apple App Store. It is crucial to completely avoid unauthorized third-party download portals, peer-to-peer file-sharing networks, or links found on forums, as these unverified sources are frequently compromised and used to distribute malicious code under the guise of free protection.

Beyond the initial acquisition, keeping the security software constantly updated is vital, as an outdated database cannot recognize or defend against newly engineered cyber threats.

Furthermore, if a user is unfamiliar with the subject or feels insecure about navigating technical settings, having a competent person or a trusted professional handle the installation and initial configuration for them is a crucial step to ensure the family defence system is set up correctly and operating at peak efficiency.

Antivirus software works by scanning files and monitoring activities on a device. It compares files to a database of known threats and also looks for suspicious behaviour, such as programs trying to access sensitive data without permission. Many antiviruses' tools work in real time, meaning they can stop threats before they cause damage. However, being a responsible user means understanding that these tools are not completely passive, nor are they always neutral. While the software can update itself, you always retain full control and can actively initiate a manual check whenever you suspect a threat or want a deeper system inspection. Furthermore, it is crucial to stay vigilant about the types of notifications these programs send. Many antivirus tools—particularly basic versions—frequently spam users with non-essential alerts or aggressive, alarming messages claiming the device is "at risk." In most cases, these are not actual virus infections, but commercial marketing tactics engineered to create artificial urgency and trick you into buying a premium upgrade. True digital safety requires learning to distinguish a real security alert from a simple, fear-based sales pitch.

Why is it important to understand how antivirus software works?

Understanding how antivirus software works helps families become more aware of digital risks. It enhances proactive security behaviour because knowing that antivirus software can be bypassed by complex attacks reinforces the need for manual caution, such as avoiding suspicious links and not opening unexpected email attachments. It also prevents a false sense of security: some people believe that having antivirus software means they are completely safe, while others believe they do not need it at all.

In reality, as seen, digital security depends on a combination of tools and behaviours. Knowing what antivirus software can and cannot do allows families to use it effectively as part of their overall protection strategy.

✓ Signs that you are using antivirus protection correctly

You are managing your basic security well when:

- You have a trusted antivirus program installed and active on your main computer ensuring it is regularly updated to the latest version.
- You notice that the software performs "background scans" without interrupting your work while remembering that you can always actively initiate a manual check yourself whenever you want a deeper inspection.
- You do not disable the antivirus even if a website asks you to do so to download a "free" file
- You feel confident that the software is vetting the attachments in your emails.
- A competent person, technician, or trusted professional has installed and verified the software for you if you did not know how to set it up yourself and its update.

Example from everyday life

A teenager downloads a free game from an unknown website. The game looks harmless, but it contains a Trojan disguised as the game. Without antivirus protection, the Trojan installs itself on the device and starts collecting personal data. With antivirus software, the download may be blocked or flagged as dangerous before it is opened, preventing the problem.

You can tell the phone or computer got infected if the battery drains very fast, the device gets hot for no reason, it becomes extremely slow, or strange apps and pop-up ads appear out of nowhere. If you notice these signs, you must immediately turn off the internet, run a security scan to find the threat, delete the infected app right away, and change your passwords using a different, clean device.

Activity

Think about the devices used in your family (computer, smartphone, tablet).

1. Do you know if they have antivirus protection?

2. Do you know the name of the antivirus software installed on it?
3. Have you ever seen a warning message from antivirus software?

Discuss together how you would react if a device showed a security alert. Open your "Security" or "Settings" menu of your antivirus software and look for the status of your protection. Is the "Real-time protection" or "Resident shield" turned on?

1.2 Common myths: "I don't need it if I'm careful"

Many people believe that digital security is only a concern for those who visit "dangerous" websites. While safe browsing habits and common sense are crucial, they are not sufficient protection against modern cyber threats, as sophisticated malware can infect a computer without any user action. This belief, being nothing more than a myth, maybe the most common in the digital world and risks becoming a truly dangerous force. In reality, cyber-attacks have become so sophisticated that even a cautious user can be targeted while doing something as simple as reading the morning news or checking a weather app. Relying solely on "common sense" is like driving a car without a seatbelt because you consider yourself a good driver. While your behaviour is the most important factor, technical protection serves as the safety net for the moments when human error or sophisticated technical tricks take over.

Today's online threats are often designed to look trustworthy. Cybercriminals use techniques that imitate real websites, official emails, and well-known platforms. These are not obvious "dangerous" situations, but carefully constructed traps that can deceive even attentive users.

In this context, it is crucial to recognize a specific category of threats that does not operate in the shadows but relies entirely on psychological manipulation: scareware. These are deceptive software programs or pop-up notifications designed to generate immediate anxiety and a sense of urgency, often displaying fake alerts about virus infections or critical system vulnerabilities. The goal of scareware is not to technically breach the device's defences, but to trick a panicked user into clicking a malicious link, downloading fraudulent tools, or voluntarily surrendering personal credentials. Ultimately, this psychological manipulation aims to steal money and deeply sensitive personal information and gain unauthorized access to real-time location tracking or device

microphone inputs to invade the family's privacy. While it often begins with immediate financial extortion, it can also have devastating long-term consequences leading to unauthorized loans, total financial ruin, or even the loss of major personal assets, including the family home.

Children and teenagers are particularly exposed to these risks, not only because of their age but also because of how they use digital devices. They tend to spend more time online, especially on smartphones, social media, games, and video platforms. This increases the likelihood of encountering harmful content or malicious links.

For example, risks may be hidden in:

- online games that offer “free rewards” or extra lives
- pop-up ads that promise tempting discounts on popular items, such as clothing, or exclusive access to educational content, including online courses and books that appear useful or appealing to young people
- links shared through messaging apps or social media
- unofficial app downloads or modified (“cracked”) versions of games, music streaming platforms and other types of software.

In these situations, children may click quickly out of curiosity or excitement, without fully understanding the consequences.

However, adults are not less at risk—just in a different way. While parents may be more cautious, they are often less familiar with how digital threats appear today. Many adults did not grow up in a fully digital environment and may find it harder to recognize fake messages, fraudulent websites, or misleading advertisements. It is important to note that even adults who consider themselves tech-savvy are not immune to these traps, as contemporary fraud is engineered to exploit psychological vulnerabilities that can catch anyone off guard, regardless of their technical expertise.

For example, adults may:

- confuse a fake email with a real one from a bank or delivery service

- fail to closely inspect the technical details of an email, such as opening unexpected attachments, clicking unverified links, or neglecting to check the sender's actual email address, domain name, and extension.
- click on sponsored ads without realizing they are not official sources
- trust messages that create urgency (e.g., “Your account will be blocked”)
- plug USB flash drives or external devices into their computers, unaware that physical hardware carries significant security risks and can automatically inject malware into the system the moment it is connected.
- falling victim to sophisticated scams widespread on platforms like WhatsApp (such as impersonation fraud or fake family emergencies) or Booking (such as urgent, fraudulent requests to re-enter payment details to prevent a room cancellation)

For this reason, digital security must be a shared responsibility within the family. Parents need to develop their own digital skills, not only for their own safety but also to guide and protect their children effectively.

Antivirus software, together with awareness and education, helps reduce these risks. It is crucial to recognize that these digital threats cause severe consequences that go far beyond psychological distress; they can inflict direct, functional damage on our physical devices, leading to the permanent loss of important documents and files such as critical work projects, essential study materials, university theses, financial records, or irreplaceable family photo archives, and compromise highly critical data also through the loss of passwords.

Why is it important to debunk this myth?

Understanding that both children and adults are vulnerable—although in different ways—helps families adopt a more balanced and realistic approach to digital safety. Recognizing and understanding the differences of both generations significantly facilitates communication between both parties, creating a supportive space for dialogue. This shared awareness actively encourages family members to openly discuss their daily online experiences, including the specific digital

risks they have actually faced or successfully avoided and that they may face in the future in order to prevent them.

By moving past these misconceptions, we can:

- realize that every device connected to the internet is a target for a potential threat, regardless of the user's habits
- understand that "Malvertising" (fake ads on real sites) can infect a computer even on trusted platforms
- build a more realistic and effective defence strategy for the whole family.

✓ Signs that you have a realistic view of digital risks

You are showing a safe digital mindset when:

- you do not assume a website is safe just because it looks professional or famous
- you understand that a "free" offer that seems too good to be true is usually a trap
- you treat your smartphone with the same security caution as your laptop
- you explain to your children that even "safe" games can sometimes have security holes.

Example from everyday life

A child sees a message inside an online game offering free coins if they click on a link. Excited, they click without thinking, and the link leads to a fake page asking for account details.

At the same time, a parent receives an email that looks like it comes from a delivery company. The message asks them to confirm personal information to receive a package. The parent clicks on the link, believing it is legitimate.

In both cases, the risk comes from trusting something that appears real.

Activity

Discuss together as a family:

- Have you ever clicked on something online that later seemed suspicious?
- Do you think children or adults in your family are more exposed to online risks? Why?

Try to identify at least one situation where being “careful” might not be enough, and think about what additional protection could help.

1.3 Built-in security vs. third-party software

When you buy a new computer or smartphone, it usually comes with some form of built-in security, such as Windows Defender or Apple's internal protections. For many years, there has been a debate about whether these free, built-in tools are enough or if parents should invest in professional, third-party antivirus suites. This built-in protection often includes:

- basic antivirus functions firewalls that control incoming and outgoing connections
- warnings about unsafe websites or downloads

For many families, these tools provide a good starting level of protection, especially if devices are updated regularly and used responsibly.

Built-in security has improved significantly and provides a great "baseline" for the average user. However, third-party software often offers specific features designed for families, such as advanced filters for children's browsing, identity theft monitoring, and more powerful tools to stop "Ransomware" (viruses that lock your files for money).

Choosing between them depends on how much time your family spends online and what kind of data you need to protect.

Third-party antivirus software, on the other hand, offers additional features that can strengthen digital protection. These may include:

- more advanced threat detection systems
- parental control tools
- protection against phishing and online scams
- detailed reports about device activity and risks

For example, some third-party solutions allow parents to monitor how devices are used, block unsafe websites, or set time limits for children's online activities.

A family where devices are mainly used by adults for work and basic activities may find built-in protection sufficient. On the other hand, a family with younger children, multiple devices, and frequent online activity may benefit from additional security tools.

Why is it important to choose the right level of protection?

Understanding the difference between built-in and additional security tools helps families avoid two common mistakes: under-protecting, so relying too much on default protection while handling sensitive work data or visiting high-risk sites or on the contrary, over-protecting and installing unnecessary tools without knowing how to use them.

Choosing the right software allows you to:

- match the level of security to your family's actual digital habits
- access "Parental Control" features that are often more advanced in paid versions
- protect multiple devices (phones, tablets, PCs) under a single-family subscription
- get professional support if something goes wrong and your data is compromised.

Example from everyday life

A family uses a shared computer with built-in security. The parents mainly use it for emails and online banking, while their children use it for schoolwork and games.

At first, everything seems safe. However, one day a child accidentally downloads a file from an unsafe website. The built-in protection does not recognize it as a threat, and the file installs unwanted software on the device.

After this experience, the family decides to install additional security software because the new software allows them to see which websites their young son was visiting and automatically blocks any "in-app" purchase attempts on his tablet, saving them from both security risks and unexpected bills.

Activity

Check your current security software. Think about the devices used in your family.

- Do you rely only on built-in security, or do you use additional software?
- Who uses each device, and for what purposes?

Discuss whether your current level of protection is enough or if additional tools could improve your family's digital safety.

⚠ Attention

There is no need to install multiple antivirus programs on the same device. In fact, having more than one can create conflicts and reduce performance. It is better to choose one reliable solution and keep it updated.

1.4 Mobile security: protecting smartphones and tablets

For most of us, our smartphones are the most personal devices we own. We use them to wake up in the morning, to navigate our cities, to manage our bank accounts, and to stay in constant contact with our family and friends. Because these devices are so small and convenient, we often forget that they are actually powerful computers—often more powerful than the laptops we used a decade ago. This convenience, however, comes with a trade-off. Because our phones are always connected to the internet and always with us, they represent a goldmine of information for cybercriminals, from our real-time physical location to our private photos and messages. The "mobile-first" world we live in means that hackers have shifted their focus. They no longer just target desktop computers; they create sophisticated mobile malware designed to hide inside seemingly harmless applications. Protecting a smartphone requires a different mindset than protecting a PC, as the risks often come from the very apps we choose to download and the permissions we grant them without a second thought. Understanding mobile security means recognizing that your phone is not just a phone—it is a digital extension of your home. Consequently, it holds constant access to exactly where you are and who you are, making the security stakes incredibly high. By casually approving access requests, users risk installing intrusive tracking applications that monitor their daily geographical movements, or malicious software that directly plunders their private photo archives, effectively exposing their physical routines, core identity, and intimate family life to external exploitation.

Mobile devices can be exposed to several threats, including:

- downloading unsafe or fake applications that secretly bundle commercial tracking software or spyware, software designed to secretly monitor user activity
- clicking on malicious links received through messages or social media
- connecting to unsecured public Wi-Fi networks
- granting excessive permissions to apps giving unknown developers unauthorized access to the device's camera, microphone, and private photos

Children are particularly exposed because they use mobile devices more frequently and often in a more spontaneous way. For example, they may download games, follow links shared by friends, or interact with online content without fully understanding potential risks.

At the same time, adults may underestimate these dangers. A parent might assume that a smartphone is “safe by default” and therefore pay less attention to what is installed or accessed on the device.

Smartphones often contain a large amount of personal information, including photos, contacts, messages, and even access to banking or payment apps. This makes them a valuable target for cybercriminals especially now that the landscape of mobile security has grown significantly more complex with the rise of offensive Artificial Intelligence. Cybercriminals no longer rely on generic scams; they now deploy generative AI to orchestrate hyper-personalized social engineering tactics on platforms like WhatsApp, Instagram, or TikTok. By analysing public trends, AI tools can effortlessly mimic the exact communication style of a child's peer group or favourite content creators, tricking them into downloading malicious, modified clones of popular games or granting invasive device permissions. Protecting the modern mobile ecosystem requires defence mechanisms equipped with predictive AI, capable of identifying these automated, highly targeted manipulation patterns before they compromise the household network.

Why is it important to understand mobile security?

Mobile devices are not just tools for communication—they are personal spaces where a large part of daily life takes place. For children, they are often the main gateway to the online world.

Understanding the risks associated with mobile devices helps families take proactive steps to protect personal data and prevent unwanted situations. It also encourages responsible use of technology from an early age. By treating our mobile devices with the same security respect as our computers, we can:

- prevent "spyware" from tracking our family's movements through GPS data or covertly activating the device's microphone to record private surroundings
- protect our mobile banking apps and digital wallets from being accessed by unauthorized users
- ensure that the "free" games our children play are not secretly collecting their personal data or recording their surroundings

✓ **Signs that your mobile devices are secure**

You are practicing good mobile security when:

- you only download applications from the official Google Play or Apple App Store
- you regularly review the "App Permissions" (e.g., access to camera, location, contacts) in your settings and turn off access to the camera or microphone or location for apps that don't need them
- you have the in-built "Find My Device" (or similar) app activated so you can remotely wipe your data if the phone is lost or stolen
- you avoid using public, unprotected Wi-Fi for sensitive tasks like checking your bank balance
- you delete old apps that you no longer use, as they can become security risks over time.
- keep the device updated with the latest software version

Example from everyday life

A child receives a message on a social media platform from a friend, containing a link to a “funny video.” Without thinking too much, they click on it. The link opens a page that asks them to log in again, but it is actually a fake page designed to steal their account credentials.

At the same time, a parent connects to a free public Wi-Fi network in a café to check emails and access online banking. Without realizing it, the connection is not secure, and sensitive information may be exposed.

Activity

Take your smartphone right now and open the "Settings" menu.

1. Go to the "Apps" or "Privacy" section and select "Permission Manager."
2. Look at which apps have access to your Camera and Microphone.
3. If you see an app that you haven't used in months or that shouldn't need that access, turn the permission off or delete the app entirely.

How many apps did you find that had more access than they needed?

Tip

Activating remote-tracking features is a fundamental defence for wiping your data if a device is physically lost or stolen. However, because your smartphone is a literal digital extension of your daily life, these features require permanent, non-stop access to your real-time location. To balance safety and privacy, you must rely **exclusively** on the official anti-theft tools built directly into the operating system by Apple or Google. Avoid downloading third-party "phone finder" or "device locator" apps from the store: many of these applications use the excuse of security simply to harvest your location data and track your movements under a legitimate guise. Similarly, you must strictly avoid activating or authorizing background location tracking for social media platforms and networks, as these applications do not contribute to your device's security infrastructure and continuously exploit your real-time coordinates to monitor your daily habits and feed invasive advertising algorithms.

1.5 Keeping system software updated: the first line of defence

We have all seen the notification: *"A software update is available. Install now or remind me later?"* For many busy parents, the temptation to click "Remind me later" is very strong. However, keeping

software updated is one of the simplest and most effective ways to protect digital devices, and it plays a crucial role in digital security. We worry that the update will take too long, change the look of our favourite apps, or slow down our devices but updates are not only introduced to add new features or improve performance, but also to fix vulnerabilities—weak points in the system that cybercriminals can exploit, holes that hackers can use to sneak into your device without you ever clicking a link.

When a vulnerability is discovered, software developers usually release an update to correct it. When a company like Apple, Google, or Microsoft discovers one of these holes, they quickly write a "patch" to fix it and send it to you in the form of an update. If you do not install it, the hole remains open, and eventually, a cybercriminal will find it and can be used to gain unauthorized access, install malware, or steal personal data. In the world of digital security, an update is the equivalent of a professional repairman coming to fix a broken lock on your front door.

This means that an outdated device can become an easy target, even if the user behaves carefully online. In a family context, this is particularly important because multiple devices are often used at the same time, and not all of them are checked regularly. A forgotten tablet, an old smartphone, or a rarely used computer can quickly become the weakest point in the household's digital security.

However, it is also true that updates do not always work perfectly. Sometimes, after an update, a device may become slower, certain applications may stop working correctly, or new bugs may appear. In some cases, users may experience a "chain effect", where one update creates a problem that is later fixed by another update. These situations can be frustrating, especially for families who rely on their devices for daily activities. As a result, some people choose to delay updates or ignore them completely, believing that they might create more problems than they solve.

While these concerns are understandable, it is important to remember that most updates are released specifically to fix security issues. Even if an update introduces temporary inconveniences, leaving a device unpatched for a long time usually represents a greater risk.

For this reason, it is recommended to install updates regularly, while adopting a balanced approach. For example, users may choose to wait a short time before installing major updates, allowing developers to fix initial issues, but should avoid postponing them indefinitely.

Why is it important to keep software updated?

It reduces the risk of being exposed to known and unknown threats. Many cyberattacks do not rely on complex techniques, but simply target outdated systems that have not been properly maintained. By staying current with updates and security patches, we can

- close the "digital doors" that hackers use to enter our systems without our knowledge
- ensure our devices run more efficiently and experience fewer software crashes
- protect our children from new types of malwares that didn't exist when the device was first purchased
- gain access to the latest privacy features that companies develop to give users more control over their data
- extend the life of our devices by keeping the software optimized and secure.

Understanding this balance helps families avoid both extremes: installing updates without awareness or avoiding them completely due to fear of temporary issues.

Example from everyday life

A family has an old tablet that is mainly used by their child to watch videos and use simple apps. Since the device still “works fine”, update notifications are often ignored.

After some time, the tablet starts showing unusual pop-ups and becomes slower. The problem is linked to a known security vulnerability that had already been fixed by a software update—but the update was never installed.

Activity

Think about the devices used in your family.

- Do you usually install updates immediately, or do you postpone them?
- Are there devices that have not been updated for a long time?

Make a list of all your devices and check if updates are available.

Choose one device and update it today.

If an update is available, plug the device into its charger and start the update now. Make it a habit to perform a "family update check" at least once a month to ensure everyone is protected.

⚠ Attention

If possible, enable automatic updates on your devices not only for your device's operating system but also for all installed applications. This simple action ensures that important security fixes across all your software are installed without delay, reducing the risk of forgetting them and leaving potential vulnerabilities exposed that cybercriminals can exploit to silently breach your device. In the digital world, an unpatched app or an outdated operating system is the equivalent of leaving a back window unlatched; hackers use automated tools to constantly scan for these exact software flaws, allowing them to install spyware, access your camera, or steal family data without you ever clicking a malicious link or realizing anything is wrong.

2. The importance of passwords in securing accounts

If the internet is a vast city where we store our most precious memories, family finances, and private conversations, then passwords are the physical keys to our front doors. Every day, we lock and unlock dozens of digital doors—from our email and social media to our children's school portals and our banking apps. However, because we have so many accounts to manage, many parents fall into the trap of "password fatigue." This exhaustion often leads us to take dangerous shortcuts, such as using simple, easy-to-guess words or reusing the same password across every website we visit.

However, as we move through 2026, the nature of these "keys" is changing. We are moving away from simple codes toward more advanced, biological, and automated ways of proving who we are. In the modern digital landscape, hackers do not usually "break" into accounts by guessing; they use powerful computers that can test millions of combinations every second. Understanding the mechanics of a strong password and the tools available to manage them is not just a technical chore; it is a fundamental act of protection for your family's digital home. By shifting our

perspective from seeing passwords as a nuisance to seeing them as our primary line of defence, we can significantly reduce the risk of identity theft and privacy breaches.

2.1 Anatomy of a strong password

A strong password is one of the simplest and most effective ways to protect personal accounts. Every day, we use passwords to access important services such as email, social media, online banking, and school platforms. For this reason, choosing a secure password is essential.

For years, we were told that a good password needed to be complex, like P@ssw0rd123!. While this looks difficult to a human, modern hacking software can crack such patterns almost instantly because they follow predictable rules. Today, security experts recommend a different approach: the **Passphrase**. A passphrase is a shorthand term for a "password phrase"—a long string of words or a sentence that are easy for you to visualize but incredibly difficult for a computer to guess. While a machine can guess a 10-character password in seconds, a 15-to-20 character passphrase is much harder to crack. These are memorable phrases that hold some kind of meaning for their user, which makes them significantly easier to recall than a string of random characters, even though they are much longer.

The clear problem with all of these passphrases is that they are constructed using words from the dictionary and can be, therefore, cracked and decoded easily by cybercriminals using various techniques. In particular, a type of brute force attack called a “dictionary” attack.

A dictionary attack involves a hacker using a list (consisting of multiple words in a dictionary or a list of popular phrases) in conjunction with specialist software, including artificial intelligence to repeatedly try and guess the passphrase to a user’s account. These systems are capable of inputting the guesses in a variety of different forms (including capitalizing letters and substituting combinations of numbers and symbols into each guess) and can equally be used to guess some keys used in certain encryption processes.

However, with the added variation of numbers, uppercase and lowercase characters, computation can take so long that it is unfeasible or too risky for the hacker to continue their work. This is the reason that passphrases need to be “strong” and unique (which will be covered later in this article).

The strength of a password today comes from its “entropy”, which is essentially its unpredictability. A password that is long and contains a mix of characters is exponentially harder to crack than a short one with complex symbols. This technical strength is best achieved through the “human touch”. While a machine hacking algorithm is incredibly fast at calculating mathematical probabilities, it struggles to solve the logic of a personal, unique human memory. For a parent, the goal is to create 'keys'—memorable phrases that hold some kind of meaning for their user—that are easy to remember but impossible for a cold, calculating machine to replicate, even if that machine knows your children’s names or your pet’s birthday. Consequently, completely avoiding the use of these easily accessible personal details as actual passwords is the absolute baseline for keeping your family's accounts secure since it would be too easy to guess for both a cybercriminal and especially for a powerful machine.

Why is it important to create strong passwords?

Strong passwords are the first barrier protecting personal information. Today, with the help of advanced technologies, weak passwords can be compromised very quickly. By upgrading to high-security passphrases, we can counter the speed of modern AI cracking tools that exploit human predictability.

Signs that your password is truly strong

A professional-grade passphrase should be around 15 to 20 characters long and include a mix of uppercase and lowercase letters, numbers, and punctuation. It is most effective when it avoids common dictionary phrases like "my dog is black" which are easily caught by hacking software. Instead, a strong passphrase should be unique, perhaps combining words from different languages or adding spaces and symbols in random, non-grammatical places. If you have a different, long, and imaginative passphrase for every major account, your digital armour is functioning correctly.

Example from everyday life

Stefano used to use Rex1985! for his accounts. It was short, predictable, and based on his dog and his birth year—exactly what an AI tool looks for. After learning about the "human element," Stefano created a new passphrase: "i-PlaYeD-bAll-on-SundaY-26-vito!". By using a 28-character

sentence that combines a memory, a random number, and a specific name, he created a wall that would take a computer centuries to crack. Even if a hacker knew Stefano liked sports, they could never guess the irregular capitalization and the specific way he structured his memory.

Activity

Let's create a "Hybrid Passphrase" that is easy for you to remember but impossible for an AI to guess.

1. Think of a simple sentence about your morning, like "I drank a hot coffee."
2. Now, "break" the grammar and add a number and a symbol in a random place: **"i-Drank1-Hot-Caffè-!"**.
3. Notice how replacing "coffee" with the Italian "caffè" and adding a number in the middle makes it much stronger.
4. Practice typing this new phrase a few times. By adding a word from another language or a random symbol, you have just created a professional-grade secret key that no machine can easily replicate.

2.2 The risks of password reuse across multiple sites

One of the most common habits when managing passwords is reusing the same one across multiple accounts. Many people do this because it is easier to remember a single password rather than creating a different one for each service not realizing that is also the most dangerous habits in digital security. Even the strongest passphrase loses its power if it is used for every account you own.

When the same password is used for multiple accounts, or across different platforms, a single data breach can compromise all of them. If one website is hacked and login details are exposed, cybercriminals can try the same email and password combination on other platforms. This technique is known as “credential stuffing” and is widely used. In practice it means that you are essentially providing a master key to every door in your digital life. A single mistake by a third-

party company can lead to a total compromise of your identity, your finances, and your family's privacy.

For example, a password used for a simple online service, such as a forum or a shopping website, may not seem important as these platforms are often perceived as “low risk” because they do not contain highly sensitive information. However, if the same password is also used for email or banking accounts, the consequences can be much more serious: this creates what is often called a “chain effect” or a “domino effect” meaning that once one account is compromised, others can quickly follow. At this point, automated tools can be used to test these credentials on other platforms in a matter of seconds and what started as a minor issue, a single security breach on a less important website can quickly turn into a widespread violation affecting multiple aspects of a person’s digital life.

When even a small retail shop website is hacked, attackers gain access to databases containing user information, including email addresses and passwords. These stolen credentials are then frequently shared or sold on the dark web, where they can be accessed by other cybercriminals.

In a family context, the risk can be even greater. Shared devices, similar habits, or the tendency to reuse passwords across family members can increase exposure.

Why is it important to avoid password reuse?

Avoiding password reuse helps contain the damage in case of a security breach. If each account has a unique password, a problem affecting one service will not automatically spread to others.

This simple habit can significantly reduce the impact of cyberattacks and protect personal and family data more effectively. By ensuring every account has its own unique key, you contain any potential security breach to just one room, preventing it from spreading to your entire life. This strategy protects your most sensitive data—like your primary email—even if a minor site you rarely use is compromised. It also saves you from the massive stress of having to change every single password you own at the same time if a breach occurs.

Example from everyday life

Consider a family. Their teenage son, uses a very clever passphrase for his favourite online game, but because it's easy to remember, he also uses it for the family's "Smart Fridge" app and his dad's old tablet. One day, that small game company is compromised. The hackers don't care about his game progress; they use an AI script to try that passphrase on thousands of other apps.

They hit a match with the **Smart Fridge app**. By logging in there, the hackers see the family's grocery list, but more importantly, they gain access to the home Wi-Fi credentials stored in the app's settings. Suddenly, the hacker isn't just in a game—they are "inside" the house, watching the family's network traffic from the kitchen. If he had used a unique, "disposable" password for the game, the hacker would have hit a dead end at the digital front door.

Activity

Think about your own habits.

- Do you use the same password for more than one account?
- Which accounts are the most important for you (e.g., email, banking, social media)?

Make a plan to change at least one important account today by creating a unique password.

Attention

As we have seen it is fundamental not to underestimate any account on any website but some are obviously more important than others and should **always** have strong and unique passwords. These include:

- your email account (often used to reset other passwords)
- online banking or payment services
- school or work portals
- social media accounts

If you are not sure where to start, begin by securing these accounts first. —and above all, your password manager if you use one, as it holds the keys to your entire digital life.

2.3 2FA and MFA: The essential layers of security

Imagine you are at the entrance of a high-security facility. The guard doesn't just ask for a password; they check your ID badge, scan your fingerprint, and perhaps even verify that you are scheduled to be there at that specific time. In the digital world, this is the difference between a simple login and **Multi-Factor Authentication (MFA)**. While we traditionally relied on **Two-Factor Authentication (2FA)**—usually a password followed by a text message code—the landscape of 2026 has proven that two layers are the absolute minimum and sometimes simply not enough. Even the best passphrase can be stolen through a clever phishing site or a database leak. Adding that second layer is what transforms a vulnerable account into a digital fortress. Hackers have become adept at "SIM swapping," a technique where they hijack your phone number to intercept your SMS codes. This has pushed the gold standard of family security toward MFA, advocated as the ultimate safety net, which utilizes three distinct pillars of identity: something you **know** (your passphrase), something you **have** (your physical smartphone or a security key), and something you **are** (your biometrics like FaceID or a fingerprint). In practice, families can deploy these layers using specific tools: Authenticator Apps (like Google or Microsoft Authenticator) which generate temporary, offline verification codes; physical hardware tokens (such as YubiKeys) plugged directly into a device; dedicated app push notifications that require a single secure tap; or secure QR code scanning, which utilizes a trusted mobile app to instantly authorize a login on a secondary screen. For instance, public digital identity systems like the Italian SPID (Public Digital Identity System) and CIE (Electronic Identity Card) perfectly illustrate this multi-layered approach. When accessing official services, parents are required to combine something they know—such as a password or a PIN—with something they possess, like a smartphone receiving a push notification or a physical smart card, ensuring that even if a password is leaked, the account remains secure.

The true innovation of MFA in recent years is "Contextual Security." Modern systems no longer just ask for a second code every single time; they look at the context of your login. If you are at home using your usual Wi-Fi, the system might stay quiet. But if a login attempt occurs at 3:00 AM from a device in a different country, the MFA "wall" rises instantly.

At first glance, this might seem contradictory. If we are advising you to limit location tracking and app permissions, why would we want our devices to know where we are and what time it is? It is important to distinguish between GPS tracking and security metadata.

- **Marketing Tracking** (which you should limit) uses high-precision GPS to follow your physical movements for advertising.
- **Security Metadata** (which powers MFA) simply looks at your "Digital Letterhead"—your IP address and device ID.

This data is used as a "silent handshake" to prove it's you, and in most modern systems, this check happens via encrypted tokens that don't share your private life with the wider web. Some of these tokens also function as session tokens, which are temporary digital credentials that allow you to remain signed in to a website or application without repeatedly entering your password. If stolen by a cybercriminal, a session token may sometimes provide access to an account even without knowing the password, which is why logging out of unused devices and terminating old active sessions remains an important security practice.

For a parent, this means you are not just setting up a lock; you are hiring a digital sentry that understands the patterns of your family's life and only interrupts you when something looks suspicious. By moving from the "hassle" of 2FA to the "intelligence" of MFA, requiring these multiple, different types of proof, you turn an easy target into a digital fortress that a hacker in another country simply cannot enter and you ensure that even a stolen passphrase is a useless piece of data to a criminal.

Why is it important to use these authentication factors?

The most critical reason to enable 2FA or MFA is that it provides a **safety net for human error**. We all get tired or distracted, and we might accidentally enter a passphrase into a fake site. In that moment, the second factor becomes a metaphorical brick wall. It changes the math for a hacker: instead of just needing to "guess" a code, they would need to physically hold your smartphone or replicate your fingerprint. By making the attack "too expensive" and too difficult, hackers will almost always move on to an easier target, leaving your family's data untouched.

✓ Signs that your security layers are working

You are protecting your family like a pro when your primary "Master" accounts require a second step to log in. You have moved away from SMS codes and instead use **Push Proving**, where your phone simply asks you to tap "Approve." Most importantly, you have practiced the most important rule of 2026: **If you didn't start the login, never provide the second factor.** No matter who asks or what the location says, an unsolicited MFA prompt is a hacker hitting your wall and failing to get through.

Example from everyday life

Consider Giulia, who is enjoying a quiet afternoon at the park when her phone suddenly buzzes. A notification from her primary email account appears: *"Are you trying to log in? Tap to approve."* Giulia isn't using her phone; she's pushing her daughter on the swings. She doesn't even look at the location indicated—it might say "Rome" or "London"—what matters is that **she** didn't initiate the login. Because she has 2FA/MFA enabled, the hacker who found her password is stuck at a screen they cannot bypass. Giulia simply taps "No, it's not me." Her digital home stays safe because the "key" required a physical action that only she could perform.

 **Activity: The "Master Account" Upgrade** Your primary email is the "key to the kingdom" because it can reset passwords for almost every other service.

1. Log into your primary Email account and go to **Security Settings**.
2. Find the **Two-Step Verification** or **MFA** menu.
3. If you are using SMS, try to switch to an **Authenticator App** or **Passkey**.

Attention

It is common to receive a security alert saying someone is trying to log in from a city hundreds of kilometres away. Don't panic: this usually happens because internet providers route traffic through distant servers. An alert might say "Prague" even if you are in Rome. The only thing that matters is this: **if you are not actively trying to log in at that exact moment, deny the request.** Your focus should always be on the "timing," not the "place."

Furthermore, be highly aware of the physical trap of these pop-ups. Cybercriminals often use a tactic called "MFA Fatigue," flooding your phone with sudden, repeated alerts via system-level push notifications that appear on top of any app, even while you are actively scrolling through social media, typing, or using your phone normally. Cybercriminals hope that you will reflexively or accidentally tap "Approve" just to clear your screen. If a verification prompt catches you by surprise while you are using your phone, freeze instantly to prevent your fingers from making an accidental reflex click due to muscle memory. It is crucial to remain calm and realize that this notification does not mean your phone has been hacked or that someone has gained access to your device; it simply means an outsider is actively trying to break into your account and is currently blocked at the security gate. To handle this safely, first close or minimize the application or browser you were actively using to clear your workspace and eliminate any risk of accidental tapping. Once you have isolated the notification and regained control, do not ignore it indefinitely; instead, safely tap "Deny" or "Report Fraud" directly through the prompt or the authenticator app to actively block the ongoing attack. Additionally, remember that receiving an unsolicited prompt means someone has already compromised your password. In this scenario, denying the request is only the first step; you must immediately change your passphrases first, and only after that, select the option to sign out of all devices and active sessions globally. This precise order is vital, because changing the password first revokes the attacker's access keys, ensuring they cannot simply log back in with your old credentials after the global sign-out kicks them out.

2.4 Digital Vaults and Passkeys: Management without the memory load

By now, you might be thinking: *"How am I supposed to remember twenty different 20-character passphrases and manage MFA for all of them?"* The answer is that you shouldn't. In today's world, trying to memorize your passwords is not only stressful but actually less secure, as it leads to the dangerous habit of password reuse. This is where Digital Vaults (or "Password Managers") and Passkeys come in. These tools act as a professional-grade assistant that stores, generates, and protects your credentials, allowing you to focus on your family instead of your settings.

A good way to picture this is a real-world “safe”: your Digital Vault is that safe, and your Master Password is the only key you carry. Digital Vaults work by encrypting all your passwords and other sensitive data (like credit-card numbers or secure notes) using strong cryptographic algorithms, so even if attackers somehow access the vault’s server, they cannot read your data without your key. However, this absolute security comes with a critical warning: personal Digital Vaults operate on a "zero-knowledge" architecture. Unlike the password managers you might use at work—where an IT administrator can easily reset your account—personal family vaults have no master reset button. If you lose your Master Password, the provider cannot recover it for you, and you risk being permanently locked out of your digital life. To prevent this disaster without adding any daily mental stress, modern vaults do not ask you to memorize another backup code. Instead, during setup, they generate a one-time cryptographic "Recovery Key." Think of this not as a memory chore, but as an emergency physical seatbelt: you simply print it out or write it down once on a piece of paper and store it away safely at home. It demands zero daily memory load because you never have to look at it unless an emergency happens. Alternatively, most modern vaults allow you to enable your phone's biometric data as a form of authentication, like Face ID, to act as a secure everyday back door, allowing you to reset your master phrase seamlessly without ever needing that paper backup unless your biometric system fails completely. For those who prefer a more advanced, hardware-based solution, you can also pair your vault with a physical hardware token, such as a USB security key. This small physical device acts as a tangible master key; during an emergency login or recovery process, you simply plug it into your computer or tap it against your phone using wireless technology to instantly verify your identity, completely removing the need for paper codes or biometric fallback.

Most modern vaults (such as Bitwarden, 1Password, or similar) are end-to-end encrypted (meaning your data is scrambled directly on your device so not even the provider can see your passwords), device-bound, and support multi-device sync across your phone, tablet, and computer so the whole family can stay protected without sharing passwords in plain text. Many also check whether your passwords are weak, reused, or already leaked in known data breaches, and can automatically suggest or generate stronger replacements for each account.

The newest and most powerful shift is toward Passkeys: a revolutionary tool that allows you to log into websites using your face or fingerprint, just like you unlock your phone. Since there is no

actual "word" to steal, a hacker cannot trick you into giving it away through a fake email or a phone call making it mathematically impossible for a hacker to "phish" or steal your passkey. Passkeys are built on public-key cryptography: each site stores only a public key that can't be reused anywhere else, while your private key stays securely on your own device. A prime example of this technology in daily life is Face ID. When using a Passkey backed by facial recognition, your biometric data never leaves your device. The system relies on public-key cryptography, meaning your actual facial map is stored securely in the device's local hardware and is never transmitted to external servers or websites, completely neutralizing traditional phishing attacks.

However, while combining these authentication factors dramatically increases credential security, the rise of offensive artificial intelligence introduces a dangerous paradox. Precisely because our local credentials become unhackable, cybercriminals are shifting their focus away from cracking passwords and toward stealing public images and video clips to craft hyper-personalized scams. A clear distinction must be made between local biometric authentication and public visual data: while Face ID protects your device hardware, the images and videos we share freely online or during video calls are highly vulnerable to visual cloning. Malicious actors can harvest this public media to feed generative AI tools, creating deepfakes or impersonating family members in video format to bypass human trust, making the strict protection of our visual identity just as critical as protecting a text password and creating a crucial bridge between our access keys and the protection of our family's digital footprint, which extends far beyond mere social media presence to safeguard your core personal identity and highly sensitive online banking credentials from catastrophic theft.

Despite these emerging AI threats to our public identity, securing our foundational access keys remains the essential first step. This is where the practical synergy of these tools comes together: by using a Digital Vault, you only need to remember one "Master Password". The vault handles the rest, creating 20-character codes for every site and syncing your Passkeys across your phone, tablet, and computer. This removes the "mental load" of security, making it easier to be safe than it is to be lazy. It turns a chaotic list of forgotten codes into a streamlined, professional security system for your entire family.

Why is it important to use these management tools?

The primary benefit is **"Security without Friction."** When security is difficult, we tend to skip it. Password Managers and Passkeys make being secure faster than being insecure. They automatically fill in your details in forms and/or in websites when required, for example during shopping online, subscriptions and they can also protect you if a website is fake by refusing to autofill, and can even identify which of your old passwords are weak or have been leaked. Research shows that about 30% of people report that their passwords have been stolen at least in part because of password reuse, and around 35% of hacking victims directly blame weak or reused credentials as the main cause of the breach.

This means that for many families, the biggest single risk to their online accounts is not clever hacking tools, but simply using the same or easy passwords across multiple sites. For a busy parent, this means you can maintain a "military-grade" defence for your family's data with less effort than it takes to find a pair of lost socks.

✓ Signs that you are managing your vault like a pro

You have mastered digital management when

- You no longer know what your individual passwords are (because they are all unique)
- You have enabled a "Legacy Contact" or "Emergency Access" within your manager ensuring that your partner or a trusted family member can access the vault if something happens to you.
- You have started replacing traditional passwords with **Passkeys** on every site that offers them (like Google, Amazon, or Apple)

Enjoy a login experience that is both faster and unhackable.

Example from everyday life

Maura used to feel overwhelmed by the dozens of accounts for her children's sports, school, and healthcare. After setting up a Digital Vault, she saved her old passwords and created new Passkeys for her main accounts. Now, when she visits the school portal, her Vault recognizes the site and asks for her fingerprint. Maura doesn't type a single letter. Even if a hacker targets the school's database, they won't find a password to steal from her, because a Passkey doesn't exist as a word—it's a secure, private link that only Maura's vault can activate.

Activity: Start your Digital Vault

1. Choose a reputable Password Manager (like Bitwarden, 1Password, or your device's built-in keychain).
2. Set a **Master Passphrase** using the "human touch" method.
3. Save your 5 most used accounts into the vault.
4. If a site offers to "Create a Passkey," say yes and save it directly into your vault.

2.5 Teaching children how to create and hide their “secret keys”

Helping children build safe habits around passwords and “secret keys” is one of the best long-term investments in their digital security. The goal is not to make them experts in cryptography, or cyber security, but to give them simple, clear rules they can remember and follow.

A good starting point is to explain that every online account (games, school, video platforms, social media) needs its own “secret key”. You can call it a **password** or a **secret code**, depending on what feels more natural for your child. The key ideas are that passwords need to be:

- hard to guess, but still possible to remember
- used only for that account, and never shared with others.

You can help them turn a simple phrase like “I like pizza on Tuesday” into Ilk3p!zza0nTuesd@y, this helps them understand that mixing letters, numbers, and symbols makes the password stronger, without having to memorise random characters. It is important to explain that writing passwords on paper near the device, texting them to friends, or saving them in a plain note on the phone are all risky ways to “hide” their secret keys. Instead, you can introduce them to the idea that adults often use a **Digital Vault** or **passkeys** to store and protect codes, so they only need to remember one main password or use their fingerprint/face. When discussing these biometric shortcuts, it is crucial to address a modern shift in identity theft. It is essential to instil a fundamental rule in teenagers a fundamental rule: while using their face or fingerprint to unlock a device or a passkey is completely safe and private, the visual data they share publicly is not. A key distinction to explain is that because traditional passwords are becoming obsolete, scammers now

actively target the videos, selfies, voice notes, and live streams teenagers broadcast on social media. It is essential to clarify the method behind this threat: while biometrics function as an unhackable method of authentication (like FaceID) when kept locally on a device, publicly exposing your face changes the game entirely. When explaining this to your teens, shifting the focus from abstract data safety to the emotional reality of their social circle help them realize that cybercriminals don't just want to steal their profiles; they want to harvest their public video and audio to weaponize their voice and face for an endless array of malicious schemes and harmful actions that completely escape their control: from creating fake identities to run commercial scams, to framing them for controversial statements they never made, or even generating abusive deepfakes that can permanently destroy their school and professional reputation. On top of these widespread risks, it is worth illustrating how a cloned voice can be used in urgent, fake phone calls to trick their grandparents or friends into sending money during a staged emergency. By framing their visual identity not just as data, but as a protective shield for the people they care about, online caution transforms from an annoying parental rule into an act of loyalty and mature digital stewardship. Helping them understand that their visual identity is a precious 'key' prevents them from oversharing and builds a deep respect for their own digital footprint.

For older children (teens), the concepts of **two-factor authentication (2FA)** and **passkeys** can be gently introduced. A helpful approach is to explain that that MFA is like a second lock: first you use your password, then you confirm with your phone, fingerprint, or a code. This makes it much harder for strangers to get in, even if they somehow learn the password.

The ultimate goal is to turn password creation into a creative game rather than a chore. For a child, a passphrase shouldn't be a random string of numbers, but a "Magic Spell" or a "Secret Code" that protects their digital toys and schoolwork. By teaching them to keep these keys private—even from their best friends—we are building the foundation of digital boundaries that will protect them for the rest of their lives.

Maintaining regular dialogue with children, rather than just an initial conversation, is paramount. Initiating casual checks about how they feel regarding their accounts, what they would do if a friend asked for their password, or whether they have ever felt pressured to share it, keeps the communication channel open. This approach fosters trust, making young people far more likely to

seek parental guidance if something goes wrong. Ultimately, by instilling the habit of creating and responsibly safeguarding these secret keys, children not only protect their online presence but also develop a deep-seated understanding of privacy, respect for others' data, and their own digital independence.

Why is it important to involve children early?

Children are often the primary targets for "Social Engineering"—hackers who pretend to be friends or game moderators to steal account access. If a child understands that their passphrase is a physical "Secret Key" that must never be shared, they are much less likely to fall for these tricks. Teaching them early also prevents the habit of using easily guessable info (like the dog's name or their birth year), making their accounts—and by extension, your home network—significantly safer.

Signs that your child is becoming a "Security Pro"

You know the lesson is sinking in when the child understands that a password is a secret between them and their parents, and never their friends. They start using "Secret Stories" for their games instead of simple words, and they recognize that "biometrics" (like their thumbprint) are a special way to prove they are the rightful owner of their tablet. Most importantly, they feel comfortable coming to you if someone online asks them for their "key," knowing that a secret key is meant to stay hidden.

Example from everyday life

8-year-old Leo wanted to create a password for his new tablet. Instead of letting him use "Leo2018," his mom played a game with him: *"Tell me something funny that happened at the park that only we saw."* Leo remembered a squirrel eating a blue popsicle. Their secret code became: BlueSquirrelAteIt! Leo finds it easy to remember because it's a funny picture in his head, but a hacker's computer would take years to guess a "Blue Squirrel." Leo feels like a spy with a secret code, and his mom feels safe knowing his "key" is strong.

Activity: The "Secret Story" Game

Instead of setting a password for your child, help them find their first "Secret Story." Ask them to think of a funny or strange memory that only your family knows (e.g., a cat wearing a hat). Help them turn that image into a simple passphrase for their favourite game or tablet. This small step shifts their mindset from "remembering a code" to "protecting a secret story," preparing them for the more structured family rules you will establish later.

3. Protecting your family's online data

If the previous chapter was about the "keys" to our home, this chapter is about the **walls and windows**. In the digital world, our family's data—our photos, our location, our children's identities, and our private habits—is the most valuable asset we own. In 2026, we are no longer just fighting against "viruses"; we are navigating a landscape where information is a currency. Every time we click "Accept" on a website's cookie banner, a terms-of-service update, or an app permission pop-up or share a family moment, we are making a choice about how much of our private world we want to expose to the outside. Also casually clicking through unexpected pages or intrusive pop-ups just to make them disappear is a major privacy and security slip. In many cases, these notices concern cookies and other tracking technologies that can collect information about how your family uses websites and online services. While some cookies are necessary for websites to function properly, others may be used for analytics, advertising, or behavioural profiling. Understanding how these technologies work and how to manage them is an important part of protecting your family's digital privacy.

Protecting your family's online data is not about hiding from the internet; it is about **controlled transparency**. At its core, privacy is no longer just about keeping secrets; it is about establishing digital boundaries and exercising your fundamental right to govern your own identity. To protect this right from being corporate property, modern legal frameworks like the General Data Protection Regulation (GDPR) were established as a powerful digital armour for citizens. The GDPR fundamentally changes the rules of the game by legally declaring that your data belongs entirely to you, forcing companies to grant you transparency and the explicit right to view, limit,

or completely erase your personal information from their databases. In the modern digital and marketing ecosystem, "controlled transparency" means having the ultimate agency over what, when, and how your information is communicated. By actively exercising these GDPR privacy rights, you maintain the authority to decide exactly what third-party platforms can harvest from your household. However, big tech frequently challenges this through tactical "forced consent"—such as when platforms like Instagram or other major social networks block your access completely unless you click "Accept" to their extensive tracking terms. Navigating this reality requires us to be the "Digital Guardians" of our children's privacy. As we move forward, we must stay informed about new protective technologies and regulations designed to keep families safe. By shifting our perspective from seeing data as "abstract information" to seeing it as our family's "digital DNA," we can ensure that our online presence remains a source of joy rather than a source of risk.

3.1 Personal Data: What it is, How it is Collected and Why it Matters

Think of personal data as your family's **Digital DNA**: fragments of information that, when combined, create a detailed map of your family's daily life. It includes for example legal name, phone number, birthdate, home addresses, parents' names, and also, a child's school schedule, shopping preferences, location history, photos and device identifiers — and it can be gathered not only in large breaches but quietly by apps, websites, smart toys and social platforms used every day by families.

One of the most common ways personal data is collected today is through website cookies. When visiting a website, one of the first things families often see is a cookie banner asking them to "Accept All", "Reject All", or "Manage Preferences". Although many people click the quickest option simply to access the page, these choices can have important privacy implications. Cookies are small text files stored on a device that allow websites to remember actions, preferences, and information about a user's visit. Some cookies are strictly necessary for a website to function correctly, such as remembering language preferences, keeping a user logged in, or storing items in an online shopping cart. Other cookies may be used for analytics, advertising, personalisation, or behavioural profiling, allowing companies to better understand browsing habits and online

interests. For this reason, families should develop the habit of reviewing cookie choices before proceeding. Whenever possible, select "Manage Preferences", "Customize", or "Learn More" and enable only the cookies that are necessary for the service being used (if required since generally are already activated by default). So if you are not interested in any optional cookie, better simply deny them all. For example, if you are visiting an online newspaper, checking school information, or browsing a public website, you can often access the content while declining many optional tracking features. In these situations, the website generally only needs the cookies required to display the page correctly and remember basic settings, such as your language preferences. Advertising, marketing, and profiling cookies are often not essential for the service itself and can frequently be declined without affecting the core functionality of the site. However, families will sometimes encounter websites or platforms that make this choice more difficult. Some services limit certain features, repeatedly ask for consent, or even block access unless tracking cookies are accepted. This practice is often referred to as "forced consent" because users are pressured into sharing more data than they might otherwise choose. When this happens, it is important to understand that accepting cookies is not a security requirement but a privacy choice. If the service is essential—such as a school platform, government portal, banking service, or other trusted resource—you may decide to proceed while limiting data sharing wherever possible through the available privacy settings. If the service is not essential, consider whether the convenience offered is worth the additional collection of personal information. In fact, most parents mistakenly believe personal data is limited to sensitive records like credit card numbers, but the digital ecosystem silently harvests invisible elements like tracking cookies that shadow your family's browsing habits across different websites to build behavioural profiles, your device's unique IP address and metadata—the hidden tracking information embedded inside every smartphone photo that reveals the exact GPS coordinates and time the picture was taken.

This data is valuable because of its predictive power. Social media platforms like Instagram, TikTok, and YouTube have turned this into a hyper-sophisticated science by tracking "dwell time", the exact millisecond a child pauses while scrolling through their feed because a specific post or video catches their eye or sparks their curiosity. The algorithm interprets this brief, silent hesitation as an unspoken sign of interest, using it to construct psychological profiles that exploit emotional vulnerabilities and trap young users in addictive feedback loops.

While social networks leverage this data for engagement, a child's digital footprint can also attract far more dangerous actors. For a criminal, knowing a child's birthdate and middle name can be the first step toward identity theft. The primary reason perpetrators target minors, is because children represent a financial "clean slate" in fact they have entirely pristine records that are completely unmonitored by parents, banks, or credit bureaus precisely because as minors they cannot open bank accounts. To exploit this, criminals use a highly strategic method known as "Synthetic Identity Theft": they take the child's legitimate core identifiers—such as their birthdate and government identification numbers—and blend them with a completely fabricated name or a different address to create a hybrid, "ghost" identity, automatically forcing the system to generate a brand-new credit file under that hybrid persona at the criminal's first fraudulent application. The criminal then carefully nurtures this fake profile over several years creating an unmonitored baseline of fraudulent activity that often can go undetected for over a decade.

Moreover, for a scammer, knowing that you just booked a flight or your regular habits is the perfect “hook” for a fraudulent message. When a phishing text arrives pretending to be a courier or an airline support agent at the exact moment the family is actually expecting that specific service, it is no longer a random coincidence, but a highly calculated manipulation designed to lower a parent's guard. Crucially, these highly targeted messages rarely require your personal account to be compromised; cybercriminals frequently exploit vulnerabilities or steal credentials directly within major third-party platforms, like Booking.com. This allows them to do far more than just harvest your reservation details; they can actually hijack the official communication channel and chat with you directly inside the platform's legitimate interface, making the fraudulent message appear entirely authentic because it comes from the hotel's verified account. If an urgent notification inside your app demands immediate credit card verification for an upcoming stay, parents should never click the provided links. The safest defence is to step completely away from the interface and independently call the hotel directly or contact the platform's verified, official support line to confirm the request. For companies, the same information allows targeted advertising, behavioural profiling and personalised offers that can follow a child as they grow. This continuous tracking feeds a multi-billion-dollar shadow economy run by data brokers, who buy and aggregate data from free mobile games, school platforms, and online quizzes to build extensive digital dossiers on entire households. Your data is the currency that pays for many “free”

services — but the cost of giving too much away can be high. When an app costs nothing to download, your children are not the customers; they are the product, and these digital choices can follow them well into adulthood. Recognising that your family's information is a high-value asset is the first step toward building a safer digital environment.

Why is it important to understand data value?

Informed consent is the practical core of data value: when an app or website is “free,” you are usually paying with data. True consent means understanding what is collected, why it is needed, who will see it, how long it will be stored, and whether it is shared with third parties. With that awareness, parents can choose to share only the minimal data necessary and refuse requests that are not justified by the service.

Signs that you are managing your data value correctly?

- choosing the “minimal data” option (provide an email instead of a phone number when possible)
- routinely checking app permissions (camera, microphone, location, contacts) and removing anything unnecessary
- hesitating before filling forms or surveys that ask for more information than seems relevant
- treating your financial details as high-value data during online shopping by using temporary virtual cards, refusing to save payment information permanently inside retail databases, and shielding your purchase history
- teaching children not to post location, school, or full birthdates in public places.
- resisting the urge to blindly click "Accept All" on website banners, taking a brief moment to choose "Manage Preferences" or "Reject All" to block unnecessary tracking and marketing cookies

When assessing an app, check both the store's privacy label and the developer's reputation and reviews; store labels are helpful but not always complete.

Example from everyday life

The Smith family wanted to download a simple "Flashlight" app on their son's tablet. The app requested access to their contacts, location, and microphone. Instead of clicking "Allow," they realized that a flashlight doesn't need to know who their friends are or where they live. They recognized the app was just a "data harvester" and chose a different one that requested zero permissions. They protected their data value by simply saying "No" to an unnecessary request.

However, the Smiths also encountered a much harder challenge when setting up their daughter's mandatory school communication platform and her social media accounts. In those cases, there was no alternative app to choose; they faced a strict take-it-or-leave-it wall where clicking "Accept" to aggressive data terms was the only way to access the service. Instead of feeling completely powerless under this forced consent, the family applied the principle of controlled transparency. Since they couldn't say "No" to the initial download, they immediately went into the app's internal privacy settings after installation, manually turning off precise location tracking, revoking ad-personalization permissions, and using a dedicated, secondary email address—a separate account kept isolated from important matters like online banking, work, or official communications, and/or used only for casual app registrations and online profiles—to isolate their household's primary digital identity.

Activity: The "Invisible Audit"

Take 5 minutes to look at the "Free" apps on your phone. Pick one and look it up in the App Store or Play Store under "Data Privacy." Notice how much data it collects (Location, Contacts, Browsing History).

Ask yourself: "Is the service this app provides worth the amount of data I am giving it?"

If the answer is no, delete the app. This is the simplest way to immediately increase your family's digital security

⚠ Attention: Your Child's "Data Cleanliness"

Children are prime targets for identity theft because their credit records are clean and often unmonitored for years. Avoid publishing full birthdates or national ID numbers online when not strictly required for an official process. Where local law allows, consider placing protections (fraud

alerts or credit freezes) on a child's record and keep their personal identifiers as private as you would keep a physical valuable.

3.2 Phishing and Social Engineering: how hackers "trick" families

In the world of cybersecurity, the weakest link is rarely the software; it is the human element.

Both phishing and social engineering are techniques that rely on tricking people rather than breaking into systems.

Social engineering is the art of manipulating people into giving confidential information. While a hacker might spend weeks trying to break a password, a social engineer can achieve the same result in seconds – it can happen on the phone, in person, or inside games or social media apps – by simply asking the right question and the right time and creating a sense of urgency so that you act without thinking. This often takes the form of **Phishing**: fraudulent emails, text messages (Smishing), or phone calls (Vishing) designed to look real and from a trusted source – such as your bank, your child's school or even a popular site like Netflix or Amazon. This constant financial targeting is exactly why modern families must change how they pay online. When scammers trick you into entering card details on a fake website, a traditional credit card leaves your entire bank account exposed. This is where secure tools like PayPal, prepaid cards, and virtual cards act as a financial shield. PayPal acts as a trusted middleman, ensuring the merchant—and any hacker watching them—never sees your actual bank details. For direct purchases, virtual cards generated inside your banking app offer the ultimate protection: they create a temporary, digital-only card number for a specific amount or a single transaction. Once used, that number expires automatically. This means that even if a highly sophisticated phishing attack manages to lower your guard and trick you into typing those card details, the cybercriminal walks away with a dead, useless number, completely neutralizing the financial trap before it can hurt your family. However, even if your financial shields successfully block the threat and prevent money from being stolen, it is absolutely vital never to let these attempts slide. Families must always report the incident to their bank, block the credit card and file a formal report with local cybercrime authorities and block whoever contacted you; sharing these digital footprints is the only way law enforcement can track down scammers, shut down malicious servers, and protect the wider community.

In 2026, these attacks have become incredibly sophisticated. Scammers no longer rely on poorly written emails with obvious spelling mistakes; using advanced generative AI tools, cybercriminals can now instantly generate flawless highly persuasive messages and they often use familiar logos, names or specific language to appear trustworthy while the sender is pretending to be someone else.

They use the personal data we discussed to create "spear-phishing" attacks—highly targeted messages that include your real name, your recent purchases, or mentions of events happening in your local community.

For a parent, the danger is doubled: you aren't just protecting your own data, but also teaching your children not to fall for the digital "stranger danger" that often arrives disguised as a friendly notification or a gift card offer.

💡 **Why is it important to recognize manipulation?**

The primary reason is "**Emotional Defence.**" Phishing and social engineering works by triggering an emotional response—usually curiosity or fear (e.g., "Your account will be deleted!") or greed (e.g., "You've won a €500 voucher!").

For families this is especially risky because:

- children often respond to messages from “friends” or gifts in games
- parents may act quickly when a message appears to come from a school, bank or the family calendar

By understanding these psychological triggers, and realizing that a threat that begins on the internet can crawl directly into your physical reality where scammers pick up enough digital crumbs to map your daily routine, meaning a virtual compromise can escalate until you literally find the threat right outside your house or at your very doorstep, you can train your brain to pause when a message feels too urgent or too good to be true. This "digital intuition" is your family's best shield against scams that no antivirus can stop.

✓ **Signs of a Phishing attempt**

You can spot a "trick" by looking for a few red flags: an unusual sender address (e.g., *support@netflix.security.com* or even a completely generic public domain not associated with the platform like

netflix@gmail.com instead of *netflix.com*), a generic greeting like "Dear Customer," or a link that doesn't match the destination when you hover over it. Most importantly, any message that asks you to "verify" your password or provide a one-time code via a link is almost certainly a scam. Legitimate companies will never ask for your credentials in this way.

Example from everyday life

A parent receives a text that looks like it's from the school: "Immediate: view your child's report here [link]." The message looks urgent and uses the school's logo. Instead of clicking, the parent opens the school's official website directly (not the link), finds no such notice, and calls the school office to confirm. The school confirms it didn't send any message.

Activity: The "Spot the Fake" Game

Next time you receive a marketing email or a notification from a service you use, sit down with your children and play detective.

1. Look at the sender's email address. Is it completely accurate?
2. If there is a link do not click on it, do the same for email attachments.
3. Check the tone. Is it trying to make you feel panicked or rushed?

Teaching your kids to be "sceptical by default" is the most valuable digital life skill you can give them.

⚠️Attention: The "Go to the Source" Rule

If you receive an alarming message from a bank, a school, or a government agency, **never** use the links or phone numbers provided in that message. Always open a new browser tab and go directly to the official website you know, or use the official app. If the problem is real, you will see a notification there. If it's not, you've just avoided a trap.

3.3 Public Wi-Fi risks and the use of VPNs

When we are away from home—at a cafe, an airport, or a hotel—we often look for a public Wi-Fi network and we reach for our phones as soon as we see that familiar symbol appears: "Available

Wi-Fi networks” because the promise of a free connection is hard to resist. For parents, it can feel like a small relief: let the children watch a video, play a game, or check homework without using up mobile data. However, from a security perspective, a public Wi-Fi network is like a room with glass walls: anyone with the right tools can potentially see what you are doing. Public Wi-Fi is an open ecosystem where the rules of trust break down entirely and understanding the specific attack vectors that flourish on these networks is the first and most essential step toward meaningful protection. When you connect to a public Wi-Fi network, your device joins a shared space with everyone else in that location. If the network is not properly secured, it becomes easier for someone else on the same network to see what you are doing online. In 2026, hackers use "Man-in-the-Middle" (MitM) attacks which is arguably the most dangerous and pervasive threat on public Wi-Fi networks. The concept is deceptively simple: an attacker positions themselves — technically speaking — between your device and the network's access point to intercept the data flowing between your device and the router and every packet of data you send or receive passes through the attacker's system first.

Without encryption they can capture login credentials, private messages, or credit card info, often by setting up a fake network with a name like "Free_Airport_WiFi" that looks legitimate but is actually a trap. These are often called “evil twin” hotspots, and they can be used to capture your login details, redirect you to fake websites, or distribute malware onto your device. In some cases, attackers use these fake networks to distribute spyware or a specific kind of keylogger called DarkHotel that reports keystrokes to the hackers who particularly target unsecured Wi-Fi at hotels. Once downloaded, this spyware tracks every keystroke entered and saves the data in a file so that malicious users can identify and exploit your personal information such as credit card information, log in credentials from all the personal platforms or even the company’s network in order to steal confidential information. After a certain number of recorded keystrokes, DarkHotel deletes itself from the device to avoid detection. The best protection against keylogging, or any other type of attack, is education about how the attacks occur: it is fundamental to check that emails and websites are from a legitimate source and to never use public Wi-Fi for any activity involving sensitive personal, financial, or confidential information.

Recent reports from consumer-security organizations and financial institutions explain that a large share of people still use public Wi-Fi for sensitive tasks such as online banking, shopping, or account logins, even though these networks are often unencrypted and easy to spy on. Studies show that Wi-Fi is one of the most frequent attack surfaces for data theft, especially when people reuse passwords or do not check whether a website uses a secure HTTPS connection. In a family context, this is particularly risky because children tend to use devices in public places, and their accounts are sometimes less protected than adults': a game profile, a school portal, or a social media account can become a doorway for someone who wants to steal information or gain access to more. Public Wi-Fi networks are not all the same: some are genuinely secure and managed by the venue, while others are open, unencrypted, or even fake.

To protect your family's privacy in these situations, there are two main defences. The first is to avoid sensitive tasks (like banking) on public networks. The second, and more modern solution, is using a **VPN (Virtual Private Network)**. For everyday users, a VPN is simply a software application that you download and install directly onto your smartphone, tablet, or laptop from an official app store or a trusted provider's website. Once installed and activated, it offers a simple way to reduce some of these risks by establishing a secure tunnel between your device and internet so that even if someone intercepts your connection, all they will see is scrambled, unreadable code. When you turn on a VPN, your data travels through an encrypted channel to a server operated by the VPN provider, and then to the internet; this makes it much harder for someone in the same café or hotel to see which sites you visit or what information.

Modern VPN services are designed to be easy to use, often with a single button you can turn it on your phone or tablet. They are especially useful when travelling, studying in a library, or using Wi-Fi in a hotel or train, where you cannot be sure about the network's security. However, a VPN is not a magic button that makes everything safe. It cannot protect you from phishing, social engineering, or from clicking on suspicious links. It also cannot compensate for an outdated device or software: if your phone or apps or computer software is not updated, you are still exposed to other vulnerabilities, even if the connection is encrypted. In practice, a VPN should be used as one layer of protection, alongside habits like using strong, unique passwords, avoiding sensitive logins

on public Wi-Fi, and checking that the networks you use are truly official. Furthermore, it is vital to know how to react in real-time: if you ever suspect that your connection has been compromised or that you are actively under attack—which usually manifests as sudden slowdown of your device, unexpected security warnings, or strange page redirects—your very first reflex must be to immediately disconnect from the Wi-Fi network or switch off your device's wireless connection entirely, instantly cutting off the hacker's visibility.

Nowadays, a VPN is no longer just a tool for tech experts; it is a fundamental travel essential for any family that wants to stay connected safely while on the move.

Why is it important to understand public Wi-Fi and VPNs?

Understanding public Wi-Fi and VPNs helps families move from “I connected to the Wi-Fi here without thinking” to “I know when it is risky and when it is safer.”

One of the most important reasons to understand the usage of VPNs and public Wi-Fi is **"Anonymity and Integrity."** A VPN hides your IP address and encrypts your traffic, making it nearly impossible for hackers or even the Wi-Fi provider to track your online behaviour. For a family, this means you can check your emails or browse the web at a train station with the same level of security you have in your own living room.

Signs that you are using Wi-Fi safely

You are practicing good digital hygiene if your devices are set to "Ask to Join Networks" rather than connecting automatically. You know you are protected when your VPN app shows a "Connected" status with a lock icon before you open your browser. Most importantly, you recognize that "Free" Wi-Fi often comes with a hidden privacy cost and you choose to use your mobile data hotspot for sensitive transactions instead.

Note: Since a modern household uses a mix of different devices, you actively check these steps across your family's ecosystem: toggling "Ask to Join Networks" under the Wi-Fi settings on iOS, disabling "Connect to public networks automatically" within Android's network preferences, and ensuring the "Connect automatically" box is completely unchecked on Windows and macOS laptops for any unfamiliar hotspot.

Example from everyday life

During a family holiday, Marco needed to check the balance on his travel card while waiting at a crowded bus station. Instead of joining the "City_Guest_WiFi," which required no password and felt suspicious, he turned on the family VPN on his phone first. This ensured that his bank login details were wrapped in encryption, protecting his money from anyone else lurking on that same public connection.

Activity: The "Hotspot Check"

Open the Wi-Fi settings on your phone right now while you are in a public place. Count how many "Open" networks (those without a padlock icon) you can see. Remind your children that an open network is like a public conversation—anyone can listen in. Practice turning on your VPN or using your "Mobile Hotspot" as a safer alternative together.

Before turning that hotspot on, take a moment to open its settings together and check the password. It is important to know that when your hotspot is turned off, it is completely invisible and safe from outside attacks. Even when active, cracking its password does not grant a hacker access to your phone's internal photos, chats, or personal data. However, leaving the default factory password active creates an easy entry point for automated guessing tools. Once inside your hotspot, a stranger can quickly drain your monthly cellular data or, more dangerously, intercept the internet traffic of your children's tablets and laptops connected to that same network. Taking thirty seconds to change the default key to a unique, custom password completely neutralizes this boundary risk before you share your connection.

Attention: Forget the Network

Once you leave a public place, tell your device to "Forget this Network." You can find this option right inside your Wi-Fi settings: on an iPhone or iPad, tap the small "i" icon next to the network name to see the command; on Android devices, tap the gear icon or long-press the connection name to select "Forget" or "Remove"; and on Windows or Mac laptops, open your known networks list within the network settings to clear it. This prevents your phone from automatically

reconnecting to that same Wi-Fi (or a fake one with the same name) the next time you are nearby, closing a potential "backdoor" into your device.

3.4 Privacy on the Internet, in the Cloud and on Connected Home Devices

Our digital lives are no longer confined to a single computer screen; they flow seamlessly between the websites we browse, the **cloud** servers storing our digital data, documents and memories, which serve as remote, internet-based storage networks that hold data on external servers removing the bind of a particular physical device, and the smart objects populating our homes.

The term "cloud" may sound technical, and for many families, cloud services operate almost invisibly in the background of daily life. Photos, videos, contacts, documents, and even device settings are often synchronised automatically across multiple devices linked to the same Google, Apple, Microsoft, or similar online account, meaning information can be stored on remote servers without requiring any active action from the user. This is why many people only become aware they are using cloud storage when they receive a notification that their available space is running low or when a new device instantly displays years of photos and files from a previous one. In many cases, cloud storage is not something families actively choose to use every day; it is simply enabled during the setup of a device and continues operating automatically in the background. Every time a family saves photos to an online backup service, synchronises files between devices, or stores documents in a cloud account, copies of that information are managed on external systems that can often be accessed from multiple locations and devices. While this provides convenience and protection against data loss, it also means that personal information is no longer stored exclusively within the home.

Nowadays, protecting your family means managing an interconnected ecosystem where internet privacy, cloud storage, and home devices constantly overlap: every website we visit, every application on our smartphone, and every smart object in our homes represents a potential data pipeline to the outside world, creating a continuous trail of tracking cookies, browser histories, and online account profiles. This boundary becomes especially critical when we look at cloud storage and modern photo applications. Most families use automated cloud backups, which simply means your device automatically saves a copy of your photos to the internet, to ensure they never lose

precious family memories if the phone breaks or gets lost; however, cloud storage is often misunderstood because many people assume that their photos and files exist only on the device where they were created. In reality, cloud platforms continuously synchronise information across servers, smartphones, tablets, and computers linked to the same account. As a result, deleting a file from one device does not always guarantee that it has been removed from backups, shared folders, archived copies, or other synchronised locations. Families should therefore periodically review their cloud accounts, check which devices are connected, verify who has access to shared albums or folders, and remove information that is no longer needed. These controls can usually be found in the account, privacy, or storage settings associated with the cloud service being used. In any case, you can always choose to disconnect entirely or manage them with extreme granularity, as modern platforms like OneDrive, iCloud, Google Drive, and Dropbox offer precise configuration options. If you want to completely sever the link between your local device and the cloud, you can choose to un-link or log out of the account. This action immediately stops the machine from actively communicating with remote servers without deleting any of the files already stored in the cloud. From a security standpoint, this ensures that if a physical device is ever lost, stolen, or compromised, it cannot be used as an open backdoor to access the family's entire historical archive. Furthermore, families are not forced to save every single file to the cloud and can utilize selective synchronization or files-on-demand features. Through selective synchronization, parents can adjust cloud preferences to only sync specific folders, such as a work directory, while leaving large personal folders exclusively on the website server to save local storage space. By right-clicking any file or folder, users can explicitly dictate its behaviour: choosing an option like 'always keep on this device' ensures the file is saved both locally and online with automatic updates active, represented by a green checkmark icon, while choosing 'free up space' removes the local copy entirely, turning it into a cloud icon that downloads instantly only when double-clicked. Finally, it is entirely possible to leave the cloud service active and vigilant to access shared files without allowing it to automatically hoard personal documents. By default, operating systems often automatically clone local system folders like Desktop, Documents, and Pictures directly into the cloud. To block this intrusive behaviour in OneDrive, parents can open the backup settings, select manage backup, and turn off the toggles for these primary folders, which forces the software to only sync files that are manually dragged into the specific OneDrive folder. For Mac users, a

similar boundary is established by navigating to iCloud Drive settings and disabling the automatic backup option for the Desktop and Documents folders, ensuring the family remains in absolute control of what leaves the physical machine. Strategically dividing data—using the cloud strictly for non-sensitive material like school assignments, while keeping intimate family photographs, work projects and financial records strictly on local, encrypted hard drives—drastically shrinks the family's digital attack surface, guaranteeing that a single cloud server breach cannot compromise their entire private life.

In recent years, this cloud-based privacy risk has expanded into a highly delicate frontier: the widespread adoption of generative Artificial Intelligence tools and chatbots. When family members interact with these AI systems—whether a teenager is pasting a school essay for feedback, a parent is uploading a financial document for analysis, or a child is sharing personal stories with an AI companion—they are often unknowingly triggering severe data leakage. It is crucial for parents to understand that these platforms do not operate as closed, private diaries. In standard free AI models, every prompt typed, document uploaded, or image shared is processed and stored on external servers to be utilized as raw material for training future algorithmic models. Furthermore, these conversations are routinely subjected to human review, meaning that real human engineers and third-party contractors read through dialogue transcripts to evaluate performance, completely stripping away the anonymity of the interaction. While paid subscription tiers or enterprise models sometimes offer advanced privacy toggles that allow users to opt-out of data training, free AI models inherently monetize user inputs. This structural architecture means that sensitive family anecdotes, proprietary work data, or identifiable details about a child's life are vulnerable to data exfiltration via server breaches, or worse, can be accidentally regurgitated to other users globally through algorithmic errors.

While incredibly convenient, this creates an immense privacy risk because modern digital photos contain hidden metadata—including the exact date, time, and geographic coordinates of where the picture was taken. Additionally, tech companies use advanced facial recognition algorithms on these cloud servers to scan, categorize, and profile your children's faces as they grow. Because cloud accounts often contain years of family photographs, personal documents, contact information, school records, and location histories, they have become one of the most attractive targets for cybercriminals. Protecting a cloud account should therefore be considered just as

important as protecting online banking or email accounts. If a family cloud account uses a weak password or lacks two-factor authentication, a hacker doesn't just gain access to a random file; they gain a chronological, geotagged visual diary of your family's entire life, school locations, and daily routines.

Yet, this invisible data trail does not remain confined to remote internet servers; it actively crosses our thresholds and takes physical shape right inside our domestic sanctuary.

Our homes are populated with “smart” objects: Smart TVs, voice-controlled assistants, security cameras, and even connected appliances. Most of us enjoy the convenience of these devices in our homes, but we rarely stop to think about what they are “listening” to or “seeing.”

In 2026, the "Smart Home" is not just a technological home, but an ecosystem that requires active privacy management to prevent private conversations or children's habits from becoming a commodity. Many of these devices are connected to the internet, can record sound, track viewing habits, or store information about what we say and how we use them. In fact, modern smart devices often gather data to improve voice recognition, offer recommendations, or personalise content, but the same features can also expose private conversations, search habits, or even the times when the family is at home or away.

Official European cybersecurity assessments reveal that many smart entertainment devices lack robust security, often relying on weak authentication models like basic 4-digit PINs that are easily compromised. Furthermore, manufacturers frequently discontinue critical software and firmware updates after just 3 to 5 years, leaving older but fully functional home devices permanently exposed as the weakest link in the family network. A major factor highlighted by European research is that the primary smart device business model has increasingly shifted toward generating new revenue streams through data monetization rather than focusing on user privacy. This environment creates a multi-layered ecosystem of third-party data controllers—including equipment manufacturers, OS developers, and application platform providers—all collecting and potentially exchanging percentages of revenue based on your family's personal data.

When this technological infrastructure enters the children's bedrooms through Baby Monitors and Smart Toys (connected dolls, interactive games, or robotic stencils), the structural vulnerabilities become acute. European safety audits and case studies highlighted by cybersecurity agencies

reveal that many mass-market smart toys utilize unencrypted Bluetooth or Wi-Fi local connections. This design flaw allows remote third parties within physical proximity to intercept audio streams or establish direct communication with the child without any prior authentication challenge. Furthermore, the back-end cloud databases where children's voice recordings and profile data are processed frequently suffer from inadequate structural protection, presenting clear vectors for data exfiltration that violate baseline GDPR (General Data Protection Regulation) mandates.

In the European context, this is not just a matter of convenience: under the GDPR, this information can count as personal data, so manufacturers and service providers are expected to follow principles such as data minimisation, transparency, and privacy by design and by default. To explain it simply, data minimisation means that companies are legally forbidden from hoarding your information; they are required to collect only the absolute minimum amount of data necessary to make their specific service work, and nothing more. If a smart toy needs an internet connection just to download updates, it has no legal right to collect your child's voice recordings or location history.

Far from being just a dry set of rules, the GDPR establishes strict guardrails that grant families powerful, actionable rights. It allows you, as a parent, to demand full access to any tech company or toy manufacturer's database to see exactly what information they have gathered about your children. It gives you the "right to be forgotten," meaning you can legally force these companies to permanently delete your family's stored voice snippets, profile data, or behavioural history from their servers. Finally, it gives you the right to object to data processing, allowing you to legally shut down their ability to track your lifestyle habits or trade percentages of revenue based on your family's personal life, giving you total ownership over your domestic privacy.

Security researchers and investigative reports have demonstrated that several mass-market smart home devices, including smart fridges, can reveal detailed patterns of behaviour, such as when a household is likely to be empty, simply by analysing appliance usage data. In controlled tests, attacks on poorly secured smart-home devices have shown how information from a connected fridge or similar appliance can be used to infer when a family is away, information that could be attractive to a burglar or malicious actor: for example, a smart speaker might store snippets of normal conversation; a connected TV might log what you watch and when you watch it; a smart

fridge or other smart-appliance might reveal when you leave the house or during which hours the kitchen is used.

For families, this means that privacy settings on home devices are not just about turning off a microphone but about understanding what each device is allowed to do. Smart TVs often ask for permission to collect viewing habits, voice assistants collect audio to improve recognition, and smart-home hubs store lists of connected devices and schedules. If these permissions are not reviewed, everything from children's bedtime routines to parents' work calls can become part of a detailed profile of your family life. In practical terms, this is exactly where European privacy rules matter: if a device asks for more data than it needs, or keeps data longer than necessary, that may conflict with GDPR principles even if the device still "works" normally.

Step-by-Step: How to Unlink Your Devices from the Cloud

- **Windows Users (OneDrive):** Open your OneDrive settings, navigate to the **Account** tab, and select the option to **Unlink this PC**.
- **Mac and iPhone Users (iCloud):** Access your **System Settings**, click on your **Apple ID name** at the very top, and choose **Sign Out**.
- **Google Drive Users (Desktop):** Open the application's internal **Preferences** menu (usually found via the gear icon) and select **Disconnect account**

Why is it important to audit your privacy settings?

The primary reason is "Passive Data Collection" as modern applications and smart device collects data passively and silently. As highlighted by European Union impact studies, users generally accept default privacy settings, unknowingly allowing third-party services to track and profile their daily viewership and family habits. Because modern smart devices are equipped with specialized sensors like integrated microphones and facial-recognition cameras to facilitate voice and gesture controls, they actively capture, filter, and store surrounding audio and images right inside the domestic environment. Limiting these settings across your internet browsers, cloud photo apps, and home devices drastically reduces your family's "attack surface: the less data that leaves your home and enters the cloud, the less information is available for hackers or data brokers to build detailed profiles on your children or your daily routines.

Example from everyday life

A family just bought a brand-new Smart TV for their living room. Instead of simply plugging it in and jumping straight to their favourite shows, they decide to spend ten minutes reviewing the privacy settings during the initial setup. They discovered that the TV was pre-configured to automatically record and share their viewing habits with third-party advertisers. Together they turned off the "Automatic Content Recognition" feature and disabled the integrated voice control microphone when not actively in use.

By taking these quick steps, your family's private weekend conversations and late-night movie choices remain strictly confidential, safely shielded from automated tracking and commercial profiling.

Activity: The "Device Mute" Walk

Walk around the house with your children and identify every device that has a microphone or a camera.

1. Check if there is a light or signal indicating when they are active.
2. Go into the settings of each device and look for "Privacy" or "Shared Data".
3. Turn off the "Improve service by sending usage statistics" feature.

This exercise teaches children that we have the power to decide what our objects can "say" about us to the outside world.

Attention: Physical covers and hardware switches

For cameras integrated into laptops, Smart TVs, or baby monitors, do not rely on software alone. A simple physical cover (a sliding webcam cover or even a small piece of dark tape) is the only way to be 100% sure no one is watching. For connected toys, look for physical hardware switches that completely disconnect the internal battery or cut the power supply to the microphone module when the toy is not in active use.

3.5 Recognizing secure websites (HTTPS vs. HTTP)

Every day, we browse dozens of websites to read news, check school updates, play online games, or make purchases without thinking too much about how the connection works. However, the infrastructure connecting a home device to a web server can vary significantly in its level of security. What matters is that not every website protects data in the same way, and the address bar gives us an important clue: understanding the technical distinction between HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) is the first step in establishing a baseline for safe data transmission, preventing sensitive information from being exposed in transit.

A website that starts with **HTTP** does not encrypt the connection, which means information can be easier to intercept or modify while it is moving across the internet. When a browser connects to a legacy HTTP website, the data is exchanged in "plain text." This means that any entity positioned along the network pathway—such as an attacker on a public Wi-Fi router, an internet service provider, or an intermediate data controller—can view, intercept, or even modify the content of the transmission. In the context of European data privacy legislation, utilizing unencrypted HTTP connections for pages that handle authentication credentials, credit card details, or personal identifiers constitutes a major structural vulnerability that fails to meet basic standards for secure data processing.

On the other hand, a website that uses **HTTPS** does encrypt the connection between the browser and the website, making it harder for others on the network to read what is being sent. HTTPS implements a cryptographic layer known as Transport Layer Security (TLS). This protocol ensures that all communication between the user's browser and the web server is thoroughly encrypted.

However, a critical distinction must be made: encryption does not automatically equal honesty. This is where many people misunderstand the meaning of the padlock icon. The padlock means that the connection is encrypted, but it does **not** prove that the website itself is genuine, trustworthy, or safe in every sense. A fake shop, a phishing page, or a scam website can still use HTTPS if the attacker has set up a secure connection for their own fraudulent site. In other words, HTTPS protects the path between the user and the site, but it does not automatically guarantee that the site behind it is honest, well managed, or respectful of your data. It also does not stop the

website from collecting information that the user willingly enters, such as names, email addresses, or payment details. In 2026, cybercriminals can easily obtain legitimate HTTPS certificates for fraudulent or phishing websites within seconds. Therefore, while HTTPS guarantees that the data layer between the device and the server is encrypted and protected against local eavesdroppers, it does not verify whether the destination company itself is trustworthy or malicious. For that reason, families need to look beyond the padlock. A site that asks for passwords, payment information, or school-related data should use HTTPS, but the presence of HTTPS alone should never be treated as a final sign of safety. It is still important to check the full web address, the spelling of the domain name, and whether the page looks consistent with the service it claims to be. If a browser warning appears, or if the site address looks slightly different from the official one, that is a reason to stop and verify before continuing. This distinction is especially important in a European context, where secure communication is encouraged, but where data protection also depends on transparency, lawful processing, and responsible handling of personal information by the service itself.

Why is it important to check the protocol?

The primary technical reason is "Data Confidentiality and Server Authentication." Encryption transforms legible data into scrambled code, ensuring that even if a cybercriminal intercepts the transmission, the information remains mathematically unreadable. Furthermore, modern HTTPS implementation includes a validation mechanism: it verifies that the website actually belongs to the organization it claims to represent. For families, this prevents basic "spoofing" attacks, where a malicious actor replicates the visual appearance of a legitimate school portal or bank login page to harvest credentials.

Signs of a secure browsing connection

A secure connection is visually indicated in modern browsers by a padlock icon located to the left of the website address (URL). Clicking this icon allows users to inspect the digital certificate, verifying the identity of the domain owner and the issuing Certificate Authority. A safe browsing habit also involves checking that the URL explicitly begins with *https://* rather than *http://*. Crucially, safe browsing requires looking past the padlock icon to verify the exact spelling of the domain name (e.g., checking for most subtle alterations like *paypal.com* instead of *paypal.com*).

where the final 'l' is replaced by a 1), as a perfectly encrypted connection to an illegitimate server remains a severe threat. Additionally, up-to-date web browsers actively support privacy by default by displaying prominent, full-screen warnings before loading unencrypted HTTP pages that prompt for input.

Example from everyday life

At 8:30 PM, twelve-year-old kid rushed his mother to download a school file he forgot about. Searching on her phone, the mother clicked a link, but her browser displayed a "Not Private" warning. Despite the kid urging her to ignore it due to a lack of time, she noticed the unsafe *http://* prefix. Instead of proceeding, she typed the official address directly into the bar, reaching the secure *https://* portal and protecting her son's login credentials.

Activity: The Padlock Inspection

Gather the family around a computer or tablet and open three websites you use frequently—such as a favourite online store, a local news site, and a video streaming platform.

1. Instruct your children to locate the padlock icon next to the URL on each site.
2. Click the padlock together and read the certificate information to see who officially owns the domain.
3. Look for an older website that still uses HTTP and observe how the browser flags it as insecure. This quick exercise trains children to automatically look for structural security indicators before typing any username or password.

Attention: Let Technology Double-Check the Domain

Because human eyes can easily miss tiny spelling variations in a domain name, only in the case you have to fill in your personal credentials or information in a form, you can consider using a reliable Password Manager on family devices because a password manager acts as an excellent second line of defence as its automated systems will refuse to auto-fill your saved credentials if the domain name changes even by a single character, instantly alerting your children that they might be on a sophisticated phishing site.

Don't forget to always double-check because also a technology tool can make mistakes. For any other scenario keep your attention high!

4: Internet usage control for parents and children

The modern digital landscape offers children unprecedented opportunities for learning, socialization, and entertainment, but it also exposes them to structural risks that their developing cognitive skills are not yet equipped to navigate. For parents, establishing a safe domestic online environment is no longer just about setting ground rules; it requires a coordinated strategy that combines technical guardrails with active psychological mediation. Managing a minor's internet usage in a hyper-connected society requires shifting from simple restrictive parenting to a sophisticated blend of systemic defence and collaborative design.

This section provides a rigorous overview of the architectural tools available to safeguard minors, analysing their functionalities, operational boundaries, and practical enforcement ensuring the respect of the fundamental privacy principles mandated by European frameworks that outline the regulations to be followed in the online environment safeguarding the individuals.

In today's hyper-connected environment, drawing this distinct line between protective oversight and invasive spying has become a critical daily necessity. Modern families must navigate these boundaries carefully to ensure that household interventions safeguard the child without crushing their privacy, data dignity, and psychological autonomy. These values are no longer just optional parenting philosophies; they are foundational rights heavily protected by European legal frameworks such as the GDPR and the Digital Services Act. Fostering true digital resilience within the home therefore requires an everyday approach. It demands that parents look realistically at what software filters can and cannot achieve, adapt screen time management to the specific age and developmental stage of the child, and recognize that their own daily digital habits serve as the ultimate blueprint for their children's online behaviour.

4.1 Establishing a family digital understanding

In an era where digital devices are deeply integrated into daily family life, relying solely on verbal commands or unilateral restrictions often leads to domestic friction and ineffective security enforcement. A "Family Digital Understanding" is a formal, collaborative, and written agreement co-drafted by parents and children; a simple but effective way to agree on how the internet will be used at home. Far from being a mere list of prohibitions, this document serves as a shared regulatory framework that defines rights, responsibilities, acceptable boundaries, risks and clear consequences within the household if these shared directives of digital usage are not followed, establishing accountability from an early age. It may include how much screen time is reasonable, which apps or websites are suitable for each child, whether devices can be used during meals or before bedtime, and what information children may share online. It also helps set expectations on respectful behaviour, because online safety is not only about avoiding danger but also about learning how to act responsibly toward others.

The value of this approach is that it turns online safety into a family discussion instead of a list of rules imposed from above, creating clarity around everyday issues that otherwise lead to conflict. From a structural perspective, a digital contract should address four core areas: time distribution, physical zones of usage, data privacy commitments, and the reporting of anomalies. First, it defines clear windows for connectivity, ensuring that devices do not interfere with sleep hygiene or fundamental offline responsibilities. Second, it establishes "device-free sanctuaries" within the home, such as the dining room during meals or bedrooms during overnight hours, preventing the passive, unmonitored isolation that often accelerates digital dependency. Third, it codifies basic security protocols, explicitly binding children to seek parental authorization before downloading new software, making in-app purchases, or revealing personal identifiers on public profiles. Finally, it guarantees that if a child encounters a disturbing, suspicious, or inappropriate situation online, they can report it to their parents with the awareness of linked risks that they can encounter and on the basis of the mutual trust established with their parents.

This kind of Understanding could also be written with the support of the EU child online protection policy. In fact, the European Commission's guidance on the protection of minors under the Digital Services Act, stresses that children should be protected from harmful content, manipulative design, cyberbullying, and unwanted contact, while platforms should support safer defaults and effective

reporting tools. A family digital understanding complements this approach at home by helping children build habits that make those protections more meaningful in daily life.

A good Understanding should be practical, age-appropriate, and reviewed over time. Younger children may need simpler rules, such as asking permission before downloading an app or using a device in shared spaces, while older children may need more detailed discussions about privacy, social media behaviour, and the risks of oversharing. The point is not to control every click, but to create a stable framework that children can understand and gradually help shape as they grow.

Why is it important?

The primary pedagogical and technical reason is "Mutual Accountability and Predictability." Psychological data indicates that children are significantly more likely to respect boundaries when they are actively involved in drafting them, rather than having them imposed arbitrarily. A written agreement transforms abstract expectations into predictable rules. This structural approach ensures that when a rule is violated, the consequences (e.g., a temporary reduction in gaming time) are applied systematically as an agreed-upon outcome, eliminating emotional arguments and reinforcing behavioural discipline. It also reduces misunderstandings, because the rules are discussed in advance instead of being introduced only after a problem appears.

In practice, this makes it easier to talk about boundaries, trust, and responsibility in a way that is consistent with a child's age and maturity.

Signs of an effective Digital Understanding

An effective Understanding is clearly characterized by its physical visibility and balanced reciprocity. It should be printed, signed by every family member, and displayed in a central household location, such as the refrigerator or a study area. Crucially, a robust agreement includes "parental clauses," proving to children that adults are also bound by digital rules, such as committing to put away smartphones during family meals or play time.

Example from everyday life

A family noticed that weekends were becoming a constant battleground over tablet usage, with a twelve-year-old daughter refusing to log off her games. Instead of simply confiscating the device,

the parents held a family meeting to draft a written Digital Understanding. The daughter negotiated for an extra thirty minutes of weekend gaming, but in exchange, she agreed to keep her bedroom a device-free zone after 8:30 PM and signed the agreement.

Activity: The Family Drafting Session

Gather the family around the table with a blank sheet of paper to write your first official Digital Understanding.

1. Propose one rule regarding online safety (e.g., "Always ask before downloading an app") for your children and let your child propose one rule that parents must follow (e.g., "No phone calls at the dinner table").
2. Write down three clear, non-negotiable rules regarding data privacy and unexpected contact, along with the precise technical consequence if a boundary is crossed.
3. Have every family member formally sign the bottom of the page and hang it in a shared space. This exercise demonstrates that digital citizenship is not about blind obedience, but an active negotiation based on understanding the rationale behind digital safety and the mutual respect for shared rules.

4.2 Parental Controls within the European Regulatory Landscape

One of the most important developments in European child online protection is the move toward more reliable age assurance: while a Family Digital Understanding establishes the behavioural and ethical foundation for digital consumption, relying solely on human willpower is often insufficient against the hyper-optimized algorithmic triggers of modern applications. To support parental mediation, technology offers structural enforcement mechanisms known as Parental Control tools such as Google Family Link one of the most widely used parental control systems within the Android ecosystem, you can install, from the Apple store or Play store, on both the parent's and the child's devices to monitor, manage, and secure their digital experience. Essentially, this tool acts as a bridge between the two phones. You download the app on your own phone to act as the master controller, and you link it to your child's phone during a quick setup process. Once connected, it serves as a remote dashboard that allows you to manage their digital habits from afar.

In brief, you can use it to set daily screen time limits, lock their device when it is bedtime, approve or block app downloads from the store, filter out inappropriate websites, and even track their real-time location. It bridges the gap between open communication and necessary boundaries, giving you peace of mind while your child explores the digital world. Similar capabilities are also built directly into Apple's ecosystem through Screen Time and Child Accounts on iPhone, iPad, and Mac devices. These features are available within the device's settings and can be configured by parents without installing additional software. These tools often provide additional features such as advanced content filtering, activity monitoring, location sharing, or cross-device management, allowing families to choose the level of supervision that best matches their needs. Note that Apple's parental controls are most effective when configured through Family Sharing that allows up to six family members to share access to dedicated services. One adult act as the "organizer" and manages the group's settings which allow parents to manage restrictions remotely from their own device. Screen Time settings can also be configured directly on a child's device, but should always be protected with a separate parental passcode to prevent unauthorized changes.

Beyond the controls built into Android and Apple devices, some families choose specialised third-party parental control applications for additional flexibility and cross-device management.

For example, Qustodio is widely considered as one of the gold standards because it combines app blocking, web filtering, screen-time management, location features, and activity reporting across phones, tablets, and computers. Unlike basic device controls, these services are designed to work across different operating systems and can help parents apply consistent rules even when children use multiple devices. It features a highly powerful web filtering engine: it doesn't just block apps, but can prevent access to entire categories of websites, monitors searched videos on YouTube, and includes a "Panic Button" —available exclusively on Android devices—system that allows your child to instantly send an emergency alert with their GPS location to a list of trusted contacts.

Bark, on the other hand, is another third-party app that operates differently and less intrusively regarding screen time management, focusing instead on content analysis. It leverages artificial intelligence to scan chats, messages, and social networks for signs of cyberbullying, mental health issues, or grooming, sending an alert to the parent only when a real danger is detected. This allows parents to step in only when necessary, respecting the child's privacy by not exposing their entire conversation history.

Operating at various levels of the digital architecture—device operating systems, application layers, or network gateways—these tools act as automated guardrails to filter inappropriate content and strictly regulate time distribution.

From a technical perspective, traditional parental controls rely on two main technical mechanisms: database-driven content filtering and automated time-allocation locks. Content filtering operates by cross-referencing every outbound web request against large, centrally maintained blacklists categorized by theme (e.g., adult content, gambling, extreme violence), automatically dropping connections to unverified domains. At the network gateway level, this architecture relies heavily on the Domain Name System (DNS), which serves as the automated directory of the internet by translating human-readable website names into numerical internet protocol (IP) addresses: essentially acting just like the contact list on your smartphone that matches a person's name to their actual phone number. By using a family-filtered version of this digital contact list directly at the home router, the network automatically blocks bad or dangerous websites at the root, refusing to resolve the address before a single kilobyte of harmful data can even reach a household device. Crucially, because this protection is applied directly to the router, it automatically covers every connected device in the house, extending safety barriers to gaming consoles (such as PlayStation and Xbox) and Smart TVs, which often lack robust built-in parental controls. This is especially important for consoles, as they are no longer just for gaming; they feature fully functional web browsers and integrated streaming apps that allow children to bypass standard computer protections and access unrestricted internet content. It is important to note that this implementation on the household's router, is a particularly technical process that should be handled by a qualified IT professional to ensure network stability and data integrity.

However, the landscape of digital minor protection is undergoing a major structural evolution driven by the European Union's safety-by-design frameworks.

The European Commission has published guidelines on the protection of minors under the Digital Services Act and has also developed an age-verification app prototype designed to let users prove they are old enough to access restricted content without revealing unnecessary personal information. In April 2026, the Commission said the European age verification app was technically ready and urged Member States to accelerate rollout so that citizens could use it by the end of 2026.

This system connects directly to the European Digital Identity (EUDI) Wallet, a secure digital ID pouch on your smartphone officially issued by the government to safely store digital versions of your real ID card, allowing youth-restricted platforms to verify a user's age bracket. Operating on strict cryptographic principles of data minimization and privacy-by-design, the system does not transmit the child's full identity, name, or date of birth to third-party servers.

This application operates on strict cryptographic principles known as Zero-Knowledge Proofs (ZKP), transforming how age is verified online. Instead of forcing users to upload high-risk personal identifiers—such as photos of physical passports, birth certificates, or credit cards, which commercial databases often store and leak—the EUDI Wallet acts as a secure local validator. When a child attempts to access an age-restricted platform, the platform's server cannot query the child's name, exact birth date, or address. Instead, it sends an encrypted, standardized mathematical query to the device (e.g., "Is the holder of this wallet over 18 years old?"). The EUDI Wallet app, which is securely linked to official government identity registries, processes this query locally on the device's secure hardware enclave. It checks the verified birth date and returns an immutable, digitally signed cryptographic token which is a completely automated, invisible digital receipt generated by the system to unlock the website instantly, requiring zero action from the user automatically granting or denying access in milliseconds without revealing any personal details. It provides simple binary feedback: (e.g., "Age Verified: Yes/No"), establishing a secure browsing ecosystem without creating central databases of children's online habits.

At the same time, it is important not to oversell age verification as a complete solution. No age check can replace parental guidance, critical thinking, or good platform design, and any system that claims to solve every risk would be misleading. What the new European approach does offer is a more realistic balance: it makes access control stronger where needed, while trying to avoid turning every online interaction into a data collection exercise.

“Screen Time” Step-by-step guide on iPhones

- Open Settings on the child's iPhone.
- Tap Screen Time.
- Select Turn On Screen Time if it is not already enabled.
- Create a dedicated Screen Time Passcode that is different from the child's device passcode.

Configure the available parental control features, including:

- Downtime – automatically restricts access to most apps and device functions during selected hours (for example, bedtime or school hours).
- App Limits – sets daily usage limits for specific apps or categories, such as social media, games, or entertainment.
- Communication Limits – controls who the child can communicate with through calls, messages, and supported applications.
- Content & Privacy Restrictions – allows parents to manage access to websites, purchases, explicit content, privacy settings, and other age-sensitive features.

For more advanced parental supervision, Apple recommends using Family Sharing and Child Accounts, which allow parents to manage many of these settings remotely from their own device and to enable features such as Ask to Buy, requiring parental approval before apps, purchases, or subscriptions can be downloaded.

Why is it important?

Age verification helps create a more age-appropriate online environment, especially where children could otherwise reach content or services that are clearly unsuitable for them, such as adult entertainment websites, online gambling platforms, violent video games, or unrestricted social spaces. It also gives parents a clearer framework when explaining why some platforms are restricted and why certain services need stronger checks. In a European context, the key point is that safety measures should be effective and privacy-preserving, not one at the expense of the other.

✓ Signs of a professional parental control configuration

A truly secure setup is characterized by combining different layers of defence rather than relying on a single tool. A professional configuration connects local device restrictions (such as screen time limits on a tablet) with network-wide secure DNS filtering (such as Cloudflare for Families

or CleanBrowsing) configured directly at the home router. Furthermore, a future-proof setup is designed to integrate seamlessly with the new European EUDI Wallet infrastructure. In this way, instead of parents having to manually hunt down and block every inappropriate website, the platforms themselves automatically adjust their ecosystem to a child's verified age bracket from the very first click.

Example from everyday life

A family wanted to ensure their ten-year-old daughter could research school projects safely on her tablet without stumbling into content not suitable for their age. Instead of just downloading a standard app like Google Family Link, they asked a trusted and qualified person to change the DNS settings on the home router to a secure, family-filtered address, instantly protecting every device in the house. When their daughter later tried to access an online gaming store that required user verification, the platform requested her age via the new European Age Verification system. By approving the check through the family's secure digital wallet app, her age bracket was verified instantly and anonymously without uploading her ID, ensuring she could play safely while keeping her identity hidden from the game developer.

Activity

Review one platform or app used in the family and check:

- whether the child's profile is private by default.
- whether blocking, muting, and reporting are easy to find.
- whether the feed (the main screen showing a continuous scroll of posts and videos) can be controlled or reset.
- whether the platform sends unnecessary recommendations or contact requests.

Then discuss whether the platform's settings really match the child's age and level of maturity. If the answer is no, the family can decide whether to tighten the settings, limit use, or replace the service with something more appropriate.

4.3 Monitoring vs. Spying: finding the right balance of trust

The deployment of technical safeguards inevitably introduces a profound ethical and operational dilemma for parents: the boundary between legitimate monitoring and invasive spying. In the domestic digital ecosystem, the capability to oversee a child's online trajectory is technologically trivial; software can easily intercept keystrokes, log private chat logs, and map coordinates in real time. However, transforming parental oversight into covert surveillance fundamentally alters the family dynamic. It shifts parental authority from a framework of structural guidance into a regime of digital policing, and can provoke resistance, concealment, or withdrawal in children and adolescents. Parental monitoring tools are often presented as safety devices, but their use raises a more difficult question: when does protection become surveillance? The balance depends on whether the control is transparent, proportionate, and limited to a clear safeguarding purpose, or whether it collects excessive data and operates in hidden ways that undermine trust and autonomy. From an architectural and psychological perspective, monitoring and spying differ not by the data they collect, but by the transparency of their application. Monitoring is an overt, educational practice where the parameters of oversight are clearly defined, mutually understood, and aligned with the child's developmental age. Spying, by contrast, relies on stealth—such as hidden stalkerware applications or unannounced log audits—that deliberately keep the minor unaware of the technical surveillance. This hidden approach is highly dangerous, as cybercriminals know all too well how to exploit these invisible monitoring systems. By operating in the dark, these apps inadvertently create backdoor access points that experienced hackers can easily intercept, turning a tool meant for parental protection into an open window for external threat actors. To an attacker, a stalkerware server is the ultimate jackpot: it neatly aggregates private chats, real-time GPS locations, photos, and passwords all in one single place, making it incredibly convenient for them to steal a child's entire digital life in one swift move. Children are exposed to real online risks, and the European Commission explicitly notes dangers such as cyberbullying, privacy breaches, harmful content, online grooming, commercial manipulation, and radicalisation. The same EU policy framework also stresses that privacy online is protected by ePrivacy (a legal framework governing privacy, data protection, and confidentiality in the electronic communications sector) and GDPR rules, while children's safety is supported through the Digital Services Act and the Better Internet for Kids strategy. Unlike the strictly binding and punitive regulations of the GDPR,

the Better Internet for Kids strategy operates as a non-regulatory policy framework focused on digital literacy, funding educational initiatives like Safer Internet Centres, and promoting the active empowerment of minors online.

The psychological implications of covert spying are deeply counterproductive to a child's cognitive and emotional growth. Developmentally, children and adolescents require a progressive degree of privacy to form an independent identity, practice self-regulation, and learn from low-stakes errors. When parents breach this boundary through secret surveillance, they replace internal motivation with external coercion. If a child discovers or suspects they are being spied on, the feeling of chronic exposure can trigger anxiety, resentment, and strategic avoidance. Instead of internalizing safety rules, the minor's cognitive energy shifts entirely toward circumvention and systemic deception. That policy context matters because parental control tools can easily drift beyond support into intrusion. Recent research from University College of London found that some unofficial parental control apps hid their presence on the device, requested excessive permissions, transmitted sensitive data unencrypted, and in some cases showed stalker ware-like indicators. Those findings show that the technical design of a monitoring tool can itself create privacy and security risks, even when the stated purpose is child protection. European child welfare frameworks and data privacy standards increasingly emphasize that children possess a developing right to privacy. Parental mediation should aim to gradually reduce technical data capture as the child matures, replacing automated blocks with critical cognitive autonomy.

To prevent this drift, parents must structurally adjust their behaviour, shifting their domestic role from a digital detective to a technical mentor. In practice, this means establishing some behavioural transparency rules: no monitoring tool should ever be installed without an upfront, face-to-face conversation explaining its presence and purpose. Parents should behave as partners in safety, explicitly framing the software not as a tool of suspicion, but as a temporary safety net. When the monitoring dashboard reveals an anomaly, an inappropriate search, or a policy violation, the immediate behavioural response must not be a sudden punitive ambush or device confiscation. Instead, parents should use that data point to initiate an open, calm inquiry into the child's underlying curiosity or intent, teaching them how to evaluate online risks rather than punishing them for crossing a software boundary. As the child matures, parental behaviour must dynamically

transition from active surveillance to strategic autonomy, systematically reducing data tracking in exchange for demonstrated responsibility.

European child-welfare and data-protection standards increasingly recognise children's developing right to privacy. Parental mediation should therefore progressively reduce technical data capture as the child matures, replacing automated restrictions with informed autonomy. The core principle, therefore, is proportionality. Monitoring is easier to justify when it is visible, bounded, and focused on specific risks; it becomes spying when it is covert, excessive, or impossible for the child to understand. In that sense, trust is not a soft extra but part of the control model itself, because children are more likely to develop safe digital habits when adults combine guidance with transparency rather than relying only on technical intrusion.

Why is it important to balance monitoring and trust?

The primary technical and developmental reason is "The Reactive Resistance Paradox." When parents deploy covert spying software, they create an adversarial environment. Data shows that tech-savvy minors who discover they are being secretly monitored do not curtail their risky online behaviours; instead, they migrate to deeper, more unsecure digital environments or they deploy advanced evasion techniques—such as hidden secondary operating profiles, burn phones, encrypted peer-to-peer messaging networks, or local log-wiping scripts. Furthermore, deploying covert surveillance software introduces severe technical vulnerabilities; many of these hidden monitoring apps suffer from poor encryption and security flaws, making them easy targets for hackers as they are already spying apps, perfect for malicious intents. This inadvertently exposes the child's most sensitive data—including real-time location, private chats, and photos—to external cybercriminals through massive data leaks.

✓ Signs of an ethical, trust-based monitoring approach

A healthy monitoring setup is completely transparent. The child knows exactly which software layers are installed on their device, what categories of data are tracked (e.g., total screen hours or domain categories), and why those parameters exist. An ethical deployment also features collaborative log reviews, where parental control dashboards are examined together with the child

during scheduled check-ins, converting automated metrics into active educational discussions rather than punitive ambushes.

Example from everyday life

A family installed a management app on their thirteen-year-old daughter's new smartphone. Instead of tracking her real-time location and chat logs in secret, the father sat down with her to open the software's parental dashboard together. They reviewed the weekly report, noting a massive spike in usage on a specific video-sharing app. Rather than issuing an automated device lock or scolding her, he asked her daughter about the content she was watching, leading to an open conversation about algorithmic loops and time management. By reviewing the automated data openly, the tool was treated as a health tracker rather than a digital wiretap.

Activity: The "Open Cards" App Audit

Sit down with your child and perform an open, mutual audit of the management tools active on their devices:

1. Open the parental control app or system settings on your phone and show your child exactly what data the software records and collects.
2. Navigate to the child's device and locate the local management profile, explaining clearly that the software is visible and present as a safety framework, not a secret tracker.
3. Invite your child to express how these tools affect their sense of autonomy, and negotiate one specific category of data (such as app-specific usage breakdown) that will be un-monitored one they hit their next age milestone, once you feel confident, they fully understood everything and ready for this step.

⚠Attention: Never Use Covert "Stalker ware"

Avoid any commercial software that markets itself as "invisible," "stealth," or "hidden monitoring." These applications, commonly classified as stalker ware, require parents to intentionally disable native security features on the child's device (such as rooting Android or jailbreaking iOS) to hide their presence. By lowering these core operating system defences, stalker

ware exposes the entire device to massive security vulnerabilities, making it easy for third-party hackers or malicious actors to intercept the exact same personal logs, photos, and location coordinates you are trying to monitor.

4.4 Managing screen time across different ages

Managing digital consumption requires a dynamic approach that evolves alongside a child's neurological and psychological development. A static, one-size-fits-all time limit is architecturally and pedagogically obsolete. Screen-time rules should therefore be age-sensitive, developmentally realistic, and reviewed over time rather than applied as a fixed lifetime formula. For infants up to three years old, digital exposure should be minimal to absent, as developing brains require physical, sensory-motor interactions to build neural pathways. For children under 2, major paediatric guidance discourages screen use except for video chatting, and for ages 2 to 5 it generally recommends around one hour of high-quality content per day, ideally with adult co-viewing. In early childhood (ages three to six), screen access must be limited to a maximum of one hour per day of high-quality, co-viewed educational content. This is broadly consistent with the World Health Organization guidance for preschoolers and with paediatric recommendations that emphasize high-quality programming over passive entertainment. As children enter school age (six to twelve), the focus shifts to balancing digital exploration with structural offline responsibilities, with screen use guided less by a rigid ceiling than by its impact on sleep, homework, exercise, and family routines. For adolescents, absolute temporal ceilings become less effective than teaching digital self-regulation, focusing instead on protecting sleep cycles and preventing compulsive consumption patterns. At this stage, the goal is not only time restriction but habit formation: adolescents need to learn how to budget attention, notice algorithmic pull, and understand when digital use starts displacing rest or schoolwork. To implement these boundaries successfully, parents must actively adjust their own mediation strategies rather than relying on abrupt, automated device lockouts. Practical transitions matter: giving children advance warnings before screen time ends helps reduce conflict and makes the boundary easier to understand. Using a smartphone as an emotional pacifier to calm a frustrated child structurally impairs their ability to develop natural self-soothing mechanisms. Parents should instead integrate clear verbal

transitions, notifying younger children ten minutes before a screen session ends to prevent emotional crashes. Structured redirection works better than sudden interruption, especially when children are told what comes next rather than simply being told to stop. For older children, parental behaviour should focus on teaching proactive time-budgeting. This means guiding them to review their own screen-time metrics on their devices, helping them identify algorithmic hooks, and allowing them to decide how to distribute their weekly allowance of digital hours, transforming time management from an external restriction into an internalized habit. In practice, this turns screen-time management into a learning process: children gradually move from parent-enforced limits to self-monitored discipline.

Why is it important to adapt limits by age?

A teenager treated like a toddler will rebel and bypass security, while a toddler exposed to teenage limits suffers structural cognitive disruption. Time rules must match biological maturity, not parental convenience.

Signs of healthy screen time management

A balanced domestic environment is clearly visible when children transition away from devices without systemic emotional outbursts or behavioural manipulation. Digital consumption is considered healthy when it remains active or creative rather than purely passive, and when it never encroaches upon fundamental biological requirements such as family meals, physical exercise, and a minimum of nine hours of uninterrupted sleep.

Example from everyday life: The Age-Gap Update

A family originally enforced a rigid one-hour daily screen limit for both their thirteen-year-old son, Luca, and his seven-year-old sister. This blanket rule caused intense friction, as the son genuinely needed more device access for school research and peer socialization. Recognizing the design flaw, the parents updated the family framework. They granted Luca an extended digital budget paired with strict overnight device-free boundaries, while maintaining a firm one-hour limit

for the younger sister. By aligning the rules with developmental age, the family eliminated daily arguments and restored domestic peace.

Activity: The Family Device-Free Audit

Sit down together on a Sunday evening to review the household's automated screen-time logs. Open the native digital well-being settings on each smartphone and tablet to analyse which applications consumed the most hours over the past seven days. Work collaboratively to identify the top three time-wasting platforms, and collectively agree to limit the usage of those specific applications during fixed family windows, such as homework hours or dinner time. If the problem persists you can choose to block those apps, even though we know is a more obstructive method.

Attention: Establish a Physical Charging Dock

Never allow smartphones, tablets, or gaming consoles inside bedrooms during overnight hours. Set up a centralized charging station in a common area of the house, such as the living room or kitchen, and mandate that all family devices be plugged into the dock at least sixty minutes before bedtime, ensuring that blue-light exposure does not disrupt melatonin production.

4.5 Leading by example: parental digital habits

The efficacy of any technological framework or family contract is ultimately determined by the behaviour of the adults who enforce it. Children do not learn digital discipline only from rules; they learn it from what they observe at home. Parents' own screen behaviour is therefore part of the family's digital environment, because inconsistent or distracted use can weaken the credibility of any rule imposed on the child. In cybersecurity, behavioural psychology, and digital sociology, this principle is known as behavioural modelling. Children are instinctive observers, and their cognitive understanding of digital boundaries is shaped far more by interpreting parental routines than by listening to verbal instructions. When parents repeatedly check their phones during meals, conversations, or family time, they signal that constant connectivity is normal, and this can quietly undermine any rule they impose on their children. This adult dependency introduces a dangerous dynamic known as "technoference," where technological interruptions actively damage interpersonal relationships and emotional development. When adults are physically present but

digitally absent, children may experience reduced emotional security and a heightened sense of isolation. This relational disconnect can also manifest in compensatory behaviours, such as attention-seeking outbursts or retreat into solitary screen use. Furthermore, a parent's careless digital footprint—such as "sharenting," the compulsive posting of a child's private life, milestones, and images on public social networks—compromises the minor's data privacy from infancy. It may also feed commercial data brokers and create a lasting digital trail that contradicts the very idea of privacy-by-design. Healthy parental modelling matters for at least three reasons. First, children are sensitive to whether adults use devices during meals, family time, or conversations. Second, parents who openly explain their own device use help normalise self-awareness rather than secrecy. Third, a household that applies the same expectations to adults and children is more likely to produce rules that feel fair and therefore easier to follow. A practical family strategy is to build a shared media plan that applies to everyone, not just the child. The American Academy of Paediatrics recommends family media planning, screen-free times and places, regular family discussions about online activity, and setting an example through adult behaviour. That approach is especially useful because it shifts digital guidance from punishment to household routine, which is easier for children to internalise over time. Parents should also be aware that using screens as a default emotional pacifier sends the wrong message. If adults routinely reach for a phone during stress, boredom, or family interaction, children may copy that pattern and use devices to avoid frustration rather than learning to tolerate it. For that reason, leading by example means more than limiting one's own screen time; it also means showing how to pause, switch off, and stay present when the situation calls for it. To cultivate a healthier digital environment, parents should actively reform their own screen habits and practise deliberate digital discipline. If an adult needs to use a device for urgent work during family time, the reason should be stated out loud, so that screen use remains a transparent, task-oriented action rather than a passive distraction. At a more advanced level, modelling also includes transparency. When parents need to use a device, explaining what they are doing and why helps children see screen use as a purposeful activity rather than an automatic habit. Parents should also model the exact boundaries they expect children to respect, such as turning off notifications during shared activities, keeping devices out of sight when interacting, and reserving specific periods for fully analogue engagement.

In practice, this section completes the logic of the whole chapter: digital safety works best when technical limits, family rules, and adult behaviour point in the same direction. Parents who model healthy habits make every other rule more believable, and that consistency is often what turns guidance into long-term behaviour change. By demonstrating that technology is a tool to be put away rather than an extension of the self, parents provide the most durable structural framework for their children's digital well-being.

Why is it important to lead by example?

The core reason is the psychological concept of "Cognitive Hypocrisy." When parental actions directly contradict domestic rules, children perceive digital restrictions as an arbitrary exercise of power rather than a protective safety measure. This breach of trust completely invalidates the ethical authority of the Family Digital Understanding, driving minors to justify their own rule-breaking and secret device usage as a logical response to adult double standards.

Signs of exemplary parental habits

Adults demonstrate healthy digital leadership when they can leave their smartphones in another room without experiencing situational anxiety or phantom vibration syndrome. A positive parental profile is characterized by the conscious choice to prioritize immediate human interaction over digital alerts, creating a domestic atmosphere where screens are subservient to family relationships.

Example from everyday life: The Notification Pause

A family was having dinner when the parent's phone buzzed with an email notification. Out of habit, the father reaches for the device and he notices his daughter watching him intently. Catching himself, he actively pulls his hand back, leaving the phone face down, and explains that whatever the message was, it can wait until after dinner because family time was the priority. By making this small, conscious gesture in front of his children, he demonstrates that human connection takes precedence over algorithmic alerts, reinforcing the family rules far more effectively than any lecture.

Activity: The "Device Basket" Challenge

First, place a decorative basket or box in the centre of the living room or dining area before a shared family activity. Second, have every family member—parents included—power down their mobile devices and place them inside the basket for a fixed duration of two hours. Third, spend that time engaging in an entirely offline activity, such as playing a board game, preparing a meal together, or reading. This collective exercise establishes a shared baseline of analogue presence, showing children that adults are fully committed to the exact same digital boundaries.

⚠ Attention: Audit Your Notification Architecture

Do not allow your phone to control your attention. Go into your own smartphone settings and disable all non-essential push notifications from news apps, social media platforms, and games, leaving active only direct communication channels like calls or urgent text alerts. By stripping your device of its ability to constantly interrupt your day, you drastically reduce your own screen-checking reflexes, making it significantly easier to model an attentive, present lifestyle for your children.

5. Risks for minors on the Internet

The digital ecosystem is not a neutral utility; it is a hyper-optimized infrastructure engineered to capture attention, process behavioural data, and maximize user engagement. When minors navigate this architecture, they step outside the protected boundaries of age-gates and enter a complex landscape where technical vulnerabilities and psychological manipulation intersect. While the internet offers unprecedented access to knowledge and community, its decentralized and often anonymous nature exposes developing minds to severe, compounding risks that traditional parental frameworks must be continuously strengthened and updated to effectively confront.

To effectively protect minors in this environment, parental mediation must transcend simple restrictive commands and adopt a systemic, threat-aware approach. This section analyses the

primary vectors of digital risk endangering modern youth, classifying them into distinct operational matrices. We will examine the structural mechanics of peer-to-peer digital violence, the sophisticated psychological frameworks utilized in online grooming, the unseen surveillance capabilities embedded within powered devices, and the predatory monetization strategies hidden inside mainstream gaming ecosystems. By understanding the technical and behavioural architecture of these threats, parents can transition from passive monitoring to proactive, structural defence.

5.1 Cyberbullying and online harassment

Many parents might still think of bullying as something that only happens in school hallways or playgrounds, but widespread access to digital devices has fundamentally changed how young people attack one another. Today, traditional schoolyard harassment has transitioned into cyberbullying—which is the intentional and repeated use of digital technology, such as smartphones, social media apps, group chats, or gaming platforms, to torment, humiliate, threaten, or socially isolate a peer. For a parent unfamiliar with these spaces, this does not look like physical shoving; instead, it takes the form of sending cruel text messages, spreading false rumours in group chats, posting embarrassing or altered photos on Instagram, or deliberately banning a classmate from a multiplayer gaming session. Unlike physical harassment, digital violence is amplified by two structural vectors of the internet architecture: persistent availability and infinite scalability. Online harassment does not terminate at the school gate; it follows the minor into the domestic sanctuary through their personal devices, operating twenty-four hours a day: it can enter the child's private space at any time, follow them across platforms. The capacity for viral distribution ensures that a single defamatory post, non-consensual image, or coordinated exclusion campaign can be replicated across thousands of data nodes within minutes, inflicting compounding psychological trauma through a permanent digital footprint that remains accessible indefinitely through screenshots, reposts, and anonymous accounts. This persistence makes the harm harder to escape and often harder for adults to notice, especially when the abusive behaviour is fragmented across messages, group chats, gaming spaces, and social media. While online harassment is frequently amplified by the online disinhibition effect—where the physical distance of a screen lowers an aggressor's natural empathy—it is a dangerous misconception to assume cyberbullying is primarily

driven by anonymous trolls. In reality, digital harassment is overwhelmingly perpetrated by known peers, including classmates, teammates, and local social acquaintances. When the aggressor's identity is completely transparent to the victim, the psychological trauma intensifies significantly, as the child cannot escape their tormentors online and is forced to confront them face-to-face in physical spaces every day. This cross-contamination of digital and physical environments eliminates any sense of a safe haven for the minor, making the hostility feel absolute and inescapable. Confronting this borderless threat requires parents to look at the crisis from both sides of the screen, recognizing that a child can easily slip into the role of the victim or, just as easily, become the aggressor. When approaching a victimized child, parents must look beyond technical fixes and initiate a profound emotional dialogue, focusing on rebuilding their self-esteem, validating their pain, and establishing an unshakeable sense of safety at home. On the other hand, parents must remain vigilant for warning signs that their own child may be the one perpetrating the harassment—such as sudden secrecy with their devices, a hyper-fixation on social status, or a noticeable drop in real-world empathy. If a child is discovered to be a bully, the parental approach must shift from defensive anger to a firm ethical intervention. This means addressing the root causes of peer pressure and digital disinhibition through open moral conversations about the real human suffering caused by online actions. Parents must actively dismantle the dangerous illusion of impunity created by a smartphone, explaining to the child that typing an insult behind a screen is not a harmless game. They need to understand that the total absence of immediate visual feedback—such as not seeing a classmate's tears, distress, or social isolation in real time—often tricks developing minds into feeling completely detached from reality. In fact, parents must emphasize that digital cruelty can be as devastating as a spoken insult or even worse precisely because text creates an indelible, permanent record that hundreds of peers can witness, screenshot, and share indefinitely, meaning their moral and legal responsibility remains entirely real even when the device is turned off. Recognizing the severity of this psychological violence, modern legal frameworks have evolved to treat cyberbullying not as a simple school disciplinary issue, but as a prosecutable criminal offense. Across several European nations, specific penal codes have been updated to enforce strict legal accountability against perpetrators. In France, for instance, while adult perpetrators face up to ten years of imprisonment and a fine of €150,000 in the most tragic outcomes, the law applies distinct thresholds for minors under the juvenile justice system;

maximum penalties for minor offenders over the age of thirteen are generally halved, while children under thirteen are subject to strict judicial educational measures and rehabilitation protocols rather than criminal detention. Ireland enforces the Harassment, Harmful Communications and Related Offences Act, commonly known as "Coco's Law," which criminalizes cyberbullying and the non-consensual sharing of intimate images with severe penal consequences. Similarly, Italy operates under Law No. 71/2017, updated by Law No. 70/2024, which grants minors over the age of fourteen the direct legal right to demand the immediate takedown of defamatory content from digital platforms, backing this up with penal provisions for persecutory conduct and stalking.

To address this crisis on an international scale, the European Commission launched its comprehensive Action Plan Against Cyberbullying anchoring its digital defences in the "Better Internet for Kids" (BIK+) mobile safety application blueprint. This institutional framework establishes a coordinated defensive front across all Member States, updating digital literacy guidelines for educators and tightening platform responsibilities under the Digital Services Act to target manipulative algorithmic practices. A core operational pillar of this Action Plan is the rollout of a standardized, EU-wide mobile safety application, implemented at the national level through official platforms like the BIK Help Gateway app, connected directly to national helplines so that victims of cyberbullying have a clear and easy way to report harassment and get help. This dedicated application provides children and parents with an accessible, trusted gateway to instantly report harassment, access tailored mental health resources, and safely store and transmit verified digital evidence to enforcement authorities, setting a new European standard for minor protection. With this legal and institutional backing, parents must implement a standardized protocol of objective forensic preservation and emotional containment. The immediate behavioural response to discovered cyberbullying must focus on securing evidence before it can be deleted or altered by the platform's automated cache refreshes. Parents must guide the child to capture high-resolution screenshots of the defamatory text, media, user handles (the unique public usernames, nicknames, or profile account IDs, typically marked by an "@" symbol, that identify exactly who is sending the messages), and platform URLs, storing these assets in a secure, encrypted drive or utilizing the secure storage environments of official European safety application infrastructures. Once the forensic trail is secured, the technical step involves deploying the platform's native block and

report mechanisms, followed by an immediate application of the "Safety Reporting Clause" from the Family Digital Understanding to initiate open dialog, reassuring the minor that their access to technology is not in jeopardy.

Why is it important to address cyberbullying structurally?

The core reason is the severe risk of "Isolated Psychological Escalation." Because digital harassment operates without physical boundaries, victims experience a total erosion of safe spaces, leading to rapid declines in academic performance, acute clinical anxiety, and profound social withdrawal. Leaving a child to navigate this algorithmic hostility alone ensures they feel completely trapped, transforming what began as a peer-level conflict into a severe mental health crisis.

Signs of ongoing cyberbullying exposure

A minor experiencing online harassment rarely discloses the issue verbally, but exhibits distinct psychosomatic and behavioural shifts. Look for immediate emotional volatility or physical shielding of the screen when receiving notifications, sudden reluctance to attend school or engage in offline sports, unexplained changes in sleep architecture, and a sudden, anxious hyper-fixation on device metrics or peer comments.

Example from everyday life: The Edited Photo

A family noticed their fourteen-year-old daughter became sullen and refused to leave her room after school, constantly monitoring her phone with visible panic. Instead of seizing the device, the parents sat down quietly and asked if something stressful was happening online. After discovering that classmates had created a modified, humiliating meme of her and circulated it across a private messaging group. Moving calmly, the parents helped their daughter screenshot every comment and profile ID, saved the data to a backup drive, and reported the group to the platform administration to ask for removing the images.

Activity: The "Digital Safe Zone" Walkthrough

Sit down together with your teenager to review the direct privacy architecture of their most active social profiles. Together, open the application settings and navigate to the privacy controls, manually configuring the account to reject direct messages from unknown accounts, filter out specific offensive keywords from comment sections, and obscure their online status, demonstrating how technical parameters can build a secure emotional buffer. Crucially, establish one universal rule with your teenager that applies across the entire digital landscape: regardless of whether an inappropriate message, toxic comment, or suspicious link comes from a total stranger or a familiar face, it is absolutely fundamental to always **report** the behaviour to the platform immediately.

Note: Beyond managing strangers, expand the walkthrough to address how to handle known profiles, as personal boundaries are just as crucial with friends and acquaintances. Teach your teenager that they have the absolute right to control their digital space even with people they know, showing them how to utilize subtle tools like 'Mute' or 'Restrict' to silence peers who cross emotional lines, spread negativity, or share inappropriate content without triggering the social friction of an outright block. Finally, emphasize that if a known contact's account suddenly begins sending unusual requests, high-pressure messages, or suspicious links, they must treat it as a potential account hijack, pausing the conversation immediately to verify their friend's identity through an alternative, offline channel before interacting further.

⚠ Attention: Never Delete the Harassment Evidence

When encountering highly disturbing or abusive messages directed at your child, your natural protective instinct may be to immediately delete the content to erase the insult. This is a critical operational mistake. In cases of severe cyberbullying, hate speech, or extortion, these raw digital logs constitute vital legal evidence. Deleting them destroys the forensic chain of custody, making it exceptionally difficult for law enforcement agencies or school administrators to trace the perpetrator's IP address and enforce accountability.

5.2 Grooming: recognizing the signs of “stranger danger” 2.0

Many of us grew up with the golden rule “Don’t talk to strangers,” but children today face a new kind of danger, one not as easily identifiable as a man in a trench coat. This modern threat to safety is virtually invisible, hidden in plain sight by the digital age. Online grooming has evolved far beyond the legacy cliché of the suspicious stranger in a public chatroom, transforming into a highly sophisticated, technologically augmented form of psychological engineering known as Stranger Danger 2.0.

To understand this threat, we must observe how it targets children differently across their developmental stages, beginning in **early childhood and infancy** through physical household vulnerabilities. This digital grooming cycle often accelerates before a child can even type, specifically through the exploitation of unencrypted smart toys and compromised baby monitors. Far from being minor hardware glitches, these vulnerabilities represent severe systemic hazards formally recognized in the official Annexes of European Union risk-assessment legislation, including the Cyber Resilience Act and the Toy Safety Directive. These EU legislative frameworks explicitly categorize connected children’s products containing integrated cameras, microphones, or geolocation trackers as high-risk digital assets due to their widespread structural failure to implement basic cryptographic standards, secure firmware signatures, and authenticated local pairing protocols. Many internet-connected child products are manufactured with severe architectural flaws, utilizing default factory credentials, lacking firmware encryption, and leaving local wireless protocols entirely unauthenticated. From a threat-modelling perspective, an unhardened baby monitor or interactive doll function as a silent, bidirectional surveillance bridge leading straight into the child's private sanctuary. If these devices are left exposed on the local network, a remote attacker can intercept their data streams or actively hijack the hardware interface. The real danger of this hardware vulnerability lies in how predators weaponize the stolen data for psychological manipulation. By eavesdropping on ambient audio or analysing voice interactions, an external actor can gather highly intimate family intelligence, including the child's nicknames, fears, daily schedules, and favourite cartoon characters. This chilling form of use is one of the reasons why the European Commission’s official guidelines on the protection of minors

sound the alarm, warning that network vulnerabilities and the abuse of private data can inherently weaponize a child's private domestic environment against their own psychological well-being.

Because this data collection happens so early, parents must initiate protection before a child ever begins exploring the digital world independently. It is vital to talk to children pre-emptively, laying a defensive foundation before they create their first profiles or enter multiplayer spaces. Parents need to explicitly teach young children that online manipulation does not look mean or frightening; instead, sometimes it may look friendly, incredibly patient, and emotionally supportive. By explaining early on that a bad actor will deliberately pretend to share their exact hobbies, offer them virtual gifts, provide intense emotional validation, and adopt peer jargon, we strip away the element of surprise. Instead of launching immediate, aggressive approaches, they execute a calculated, multi-phase manipulation strategy. Children must be taught before entering the network that anyone who asks them to keep a secret from their parents, or who seems to know intimate details about their lives without a clear reason, is crossing a dangerous boundary.

As children **grow into adolescence and older youth**, they transition into open digital spaces where predators actively weaponize this stolen context during peer-to-peer interactions. The digital environment makes grooming harder to detect because interactions usually begin with seemingly harmless contact, but the underlying aim is to manipulate a child into secrecy, dependence, and eventually abuse or exploitation; these encounters can take place in private chats, gaming spaces, social media messages, and even comment threads that appear ordinary at first glance. When teenagers enter public chatrooms (such as Discord channels), competitive gaming lobbies, online discussion forums, or interest-based blogs, the grooming strategy shifts into a highly structured methodology called “tactical friendship” utilizing the intimate intelligence they have quietly collected and accumulated over an extended period through earlier hardware surveillance, waiting patiently for the most opportune moment to deploy these insights and present themselves as an impossibly perfect, omniscient friend who already understands the child’s world, gradually separating the child's loyalty from their family unit to establish a dangerous code of absolute secrecy. Once a bond is formed in these public spaces, the predator executes a multi-platform migration, intentionally shifting the teenager into private, unmonitored, and end-to-end encrypted messaging applications meaning that messages are converted into a secure code that only the sender and recipient can read, keeping the content entirely hidden from the application company

and outside networks. This digital isolation allows predators to effectively decouple the minor from parental supervision and exploit their developmental need for isolation and autonomy. Parents should therefore treat unexplained secrecy, sudden attachment to a new online contact, and pressure to move conversations into private channels as early warning signs of this advanced manipulation. This technical pincer movement completely bypasses the minor's natural defence mechanisms, accelerating the path toward identity deception, financial sextortion, or severe emotional coercion. Ultimately, stopping this architecture requires a combination of digital supervision, open dialogue, and prompt reporting, rather than either total trust or total surveillance.

Why is it important to recognize Stranger Danger 2.0?

The fundamental reason is that modern grooming exploits the architectural trust children place in their personal environment. When a predator leverages information stolen from a bedroom baby monitor or toy—information they have quietly cultivated over time to deploy at the most vulnerable moment—the minor does not perceive them as an external threat, but as an empathetic confidant. In fact, because this psychological engineering mimics genuine friendship so flawlessly, children in many cases simply cannot realize they are being targeted or manipulated until the emotional trap has already closed around them. Bypassing this psychological barrier allows malicious actors to manipulate developing minds with unprecedented speed, making early behavioural detection far more critical than relying on reactive software blocks.

✓ Signs of ongoing grooming and device exploitation

A minor targeted by advanced grooming rarely asks for help, but displays clear behavioural tells. Look for an intense, anxious possessiveness over digital devices, characterized by shielding the screen or clearing notification logs instantly when a parent enters the room. Other major indicators include the sudden use of advanced adult terminology, the acquisition of unverified digital assets or gaming currencies, and an uncharacteristic withdrawal from physical family life, often paired with an obsessive isolation around previously normal connected device.

Example from everyday life: The Compromised Monitor

A family utilizes a high-definition, Wi-Fi-connected baby monitor to oversee their young daughter's bedroom. Over several weeks, their older ten-year-old son became uncharacteristically secretive about a new friend he is playing with on an online gaming simulator, boasting that this friend knows everything about his family, even the specific lullabies they sing to his sister. Suspecting a massive information leak, the parents audit the baby monitor's network settings and discover it was still operating on its factory-default administrative password, completely exposed to the open web. An attacker had been passively listening to their private household conversations and using that intelligence to groom the older brother online. The family immediately kills the device's internet access, changes the network architecture, and initiate an open, protective dialogue with their son.

Activity: The "Sensor Isolation" Sweep

Execute a complete technical audit of every voice and video asset in your household alongside your children. First, inspect every baby monitor, connected camera, and interactive toy to locate the physical hardware toggles for the microphone and lens. Second, access your home router's administrative dashboard to verify the exact MAC (the unique network serial number) address of each asset, ensuring no unauthorized device is bridging into the network. Third, open the companion apps for these devices on your smartphone and permanently disable all cloud-storage sharing options or automated voice-recognition telemetry features which refers to the automated process where a device constantly measures, gathers, and transmits real-world data from your home back to the manufacturer's central servers. In the case of a smart toy or camera, these telemetry features act as a background surveillance loop, recording how long the device is used, capturing fragments of your child's voice, and sending those logs to the company for analysis or AI training. Parents can turn off these hidden functions by opening the toy's app, navigating to the main settings or profile menu, looking for tabs explicitly labelled 'Privacy,' 'Data Sharing,' or 'Data Management,' and manually switching off toggles named 'Help improve our products,' 'Share usage diagnostics,' or 'Store voice history.' By turning off these specific options and disabling cloud backups, you block the application from uploading private interactions, keeping all sensory data strictly localized and locked inside your physical home.

⚠ Attention: Implement Physical and Network Air-Gaps

The most effective strategy regarding internet-connected toys and baby monitors is to avoid purchasing them entirely unless they provide an irreplaceable utility, as consumer items designed for wireless play are notoriously prone to severe security flaws. For families who already own these assets, safety cannot rely on a one-time configuration; it requires conducting periodic security audits to ensure the hardware remains safe over time. The primary danger lies within the physical toy itself, which contains built-in microphones, cameras, or wireless components that hackers can exploit directly to spy on the household. Parents can easily perform a simple, periodic safety check by opening the toy's companion app to see if they can manually toggle off the physical microphone or camera features within the settings when they aren't strictly needed for play. While inside the app, they should also look for a straightforward 'update device' button to automatically patch the toy's internal security flaws. A brilliant practical test is to see if the toy can function completely offline by temporarily turning off the home Wi-Fi or smartphone Bluetooth; if the core toy still works without internet, keeping it permanently disconnected is the safest choice. Finally, because no software shield is completely bulletproof, families must enforce a strict rule to completely power down or unplug these devices when not in use, physically shutting down the hardware and leaving hackers with absolutely no window of opportunity to slip into the home.

5.3 Inappropriate content, algorithmic rabbit holes, and radicalization vectors

The exposure of minors to harmful online material is rarely an isolated incident of poor judgment; it represents a profound cognitive hijacking driven by automated curation systems. Recommendation engines, auto-play features, shared links, gaming chats, and algorithmic feeds can bring violent, sexual, hateful, or age-inappropriate material into a child's digital environment with very little warning, rendering accidental exposure a systemic liability rather than a single event. The key issue is therefore not only the temporary presence of harmful content, but the calculated way platforms guide children from one piece of media to the next in ways that are exceptionally difficult to perceive in real time. When a minor interacts with a digital interface, the platform's processing engines do not evaluate content through an ethical or developmental lens.

Instead, they operate on a mathematical model designed to amplify information that triggers intense psychological reactions. This systemic curation constructs an algorithmic rabbit hole, a closed informational loop that progressively narrows the minor's conceptual horizon. The system utilizes a single click or a single view to generate a more extreme sequence of suggestions, transforming an innocent initial interaction into a continuous pathway where the platform actively reinforces the exposure pattern. By systematically replacing diverse perspectives with increasingly extreme viewpoints, these systems alter how a developing mind processes truth, shifting their baseline reality without requiring active or conscious content selection. This architectural isolation creates a psychological phenomenon known as the digital echo chamber, which actively accelerates cognitive distortion across sensitive developmental themes. The psychological impact of this mechanism depends heavily on age and context: younger children are frequently frightened or confused by aggressive or inappropriate material they lack the developmental architecture to interpret, whereas older children are highly vulnerable to systematic repetition, gradual desensitisation, or an intense fascination with extreme ideas. For a teenager, the risk shifts away from immediate fear and toward subconscious normalization; seeing shocking or hateful content hundreds of times in their feed erodes their moral boundaries, slowly making harmful rhetoric appear standard, acceptable, or a fascinating form of edgy, counter-cultural rebellion. These extreme ideas typically span a wide and dangerous spectrum, ranging from misogynistic incel subcultures (online groups of men unable to find romantic partners) and radical, xenophobic political ideologies, to violent conspiracy theories and insulated digital communities that romanticize severe eating disorders or self-harm. This vulnerability is severely compounded when harmful material is deliberately framed through the lenses of entertainment, subversive coded humour, or a false sense of social belonging, which significantly weakens a child's capacity to judge what is normal, acceptable, or safe online. On an ideological level, this structure is actively weaponized by extremist movements and radicalization networks. The European Union has repeatedly treated this form of online radicalisation as a severe, real-world security threat, specifically highlighting the organized recruitment of minors through mainstream social media, encrypted messaging services, streaming platforms, and gaming spaces. These groups deliberately format highly sophisticated political, social, or xenophobic rhetoric into the disarming aesthetic of youth culture, rarely beginning with overt propaganda alone, but starting instead with mixed

content, subtle grievance narratives, or insular digital communities that present themselves as edgy, rebellious, or intellectually exclusive.

For instance, networks driven by racial supremacy groups, factions promoting militant anti-government ideologies, and religious extremist cells, frequently bypass traditional recruitment methods by embedding their operations directly into spaces like custom multiplayer servers in mainstream games like Minecraft or Roblox, or within private Discord channels dedicated to popular esports. Within these digital spaces, bad actors spread seemingly harmless, highly customized memes, anti-establishment jokes, and coded language that slowly desensitize a minor to hate speech. By gamifying the radicalization pathway—such as offering digital rewards, exclusive ranks, or virtual leadership roles within a gaming clan—these networks systematically transform a teenager’s natural search for peer validation and community into a coordinated entry point for extremist ideologies, drawing them into a pipeline that normalizes hostility, exclusion, and systemic violence. The transition from inappropriate content to extremist framing is a gradual, step-by-step pathway that draws the minor deeper into networks that normalise hostility, exclusion, and systemic violence. To confront this invisible manipulation of youth consciousness, modern regulatory frameworks have established explicit boundaries around platform design. The European Parliament’s LIBE Committee (Civil Liberties, Justice and Home Affairs) and the European Commission have both highlighted the urgent need to protect minors from online radicalisation and from the criminal or terrorist exploitation of digital platforms. The European Union’s Digital Services Act (DSA) targets this exact algorithmic vulnerability by legally forcing major tech architectures to provide profiling transparency and allowing users to completely disable behavioural recommendation feeds. Furthermore, the European Commission's guidelines on minor protection emphasize that the passive ingestion of unverified, algorithmically boosted data constitutes a direct threat to a minor's psychological autonomy and democratic resilience. True protection, therefore, requires transitioning from simple external monitoring to an active deconstruction of the informational environment. While technical safeguards like safe-search filters and age-appropriate configurations are necessary to reduce initial exposure, they cannot fully prevent algorithmic amplification or guarantee a perfectly sealed environment. Families must therefore prioritize proactive prevention and early risk exposure, anchoring their defence in open digital literacy and active discussion, ensuring children understand they can instantly close a page,

stop the exposure, and disclose what they encountered to an adult without facing blame, panic, or punitive retaliation, which only drive the problem into dangerous and counterproductive secrecy.

Why is it important to understand algorithmic rabbit holes?

The core danger resides in the "Gradual Cognitive Drift." A developing adolescent brain, which is neurologically primed for peer seeking and identity formation, lacks the fully matured critical framework needed to detect subtle, automated indoctrination. When an algorithm isolates a minor within a highly polarized informational bubble, it does not just show them inappropriate media; it fundamentally rewrites their ethical framework, altering their social empathy, political tolerance, and psychological stability from the inside out.

✓ Signs of algorithmic rabbit hole or radicalization exposure

A minor undergoing ideological or psychological alignment within an online subculture will demonstrate rapid, uncharacteristic shifts in their verbal communication. Look for the sudden, dogmatic repetition of highly polarized social or political slogans, an intense intolerance toward family or real-world peer viewpoints, sudden changes in eating behaviours or body concealment tied to online group aesthetics, and a marked emotional alienation from long-standing real-world relationships in favour of insular digital movements.

Example from everyday life

A family noticed their fourteen-year-old son, suddenly repeating aggressive, hyper-masculine slogans at the dinner table. He had initially looked up basic home workouts to get in shape, but the platform's autoplay function had slowly pushed him into an isolated loop of influencers with radical ideas. Instead of lecturing him or taking the phone away, the parents sat down with the son and opened the app's watch history together. By physically showing him how just three initial clicks weeks prior had triggered an endless stream of increasingly angry videos, they unmasked the platform's manipulation, helping the son realize his new opinions weren't actually his own.

Activity: The Curation Audit and Social Feed Neutralization

Phase 1: Visual Mapping Open the child's primary social media platform together like Instagram, TikTok or YouTube, to audit the main page (feed) and identify how a few past clicks have algorithmically monopolized the feed.

Phase 2: Profile Purging Cleanse the account's predictive model by navigating directly into the deep data settings of these specific platforms. On **YouTube**, go to account settings, select 'Your Data in YouTube,' and completely wipe both the search and watch history; on **TikTok or Instagram**, access the privacy menu to clear the search log and locate the 'Reset FYP' or content preferences option to instantly force a neutral, non-targeted interface state.

Phase 3: Structural Filtering Deactivate the platform's automated autoplay function and manually block accounts or channels utilizing sensationalist, manipulative engagement tactics to lock in a clean informational baseline.

⚠ Attention: Defeat the Algorithm

The "not interested" button is a powerful tool to train social media algorithms, but it often backfires due to a metric called **dwel time**. If a user hesitates, reads a disturbing post, or especially opens the comments just to locate the report button, the engine logs those seconds as active curiosity, completely overriding the subsequent negative click. To win, children must use the **lightning-strike strategy**: hit the feedback option instantly from the main feed and scroll away immediately, starving the engine of engagement data. For a permanent cleanup, families should combine this rapid-fire rejection with hidden word filters in the app's privacy settings, while actively interacting with positive topics to force an immediate algorithmic reset through active substitution.

5.4 Predatory architecture: dark patterns and behavioural manipulation in gaming ecosystems

Modern gaming risks extend far beyond simple recreational overspending, residing within the calculated implementation of predatory software design and deceptive behavioural engineering. Video game developers increasingly employ specialized UX design strategies known as "dark patterns." These are deliberate interface architectures engineered to manipulate, deceive, and exploit users—particularly minors—into making decisions that contradict their best interests.

Instead of relying on transparent commerce, these systems integrate behavioural economics to exploit cognitive vulnerabilities, transforming interactive entertainment into a hyper-optimized financial extraction engine that treats the developing mind as a monetization target. This architecture operates heavily through social dark patterns, such as weaponized reciprocity, where games prompt minors to purchase and "gift" virtual items to friends, turning natural peer-group dynamics and the fear of social exclusion into a powerful, decentralized marketing tool. Many gaming platforms also integrate betting-like mechanics through randomised rewards, prize wheels, card packs, mystery boxes, or competitive wagering systems that encourage repeated spending in pursuit of uncertain outcomes. Although these features do not always constitute gambling in the legal sense, they rely on many of the same psychological principles of chance, anticipation, and intermittent rewards, making them particularly influential for minors.

A primary technical mechanism utilized in this predatory architecture is currency obfuscation, which triggers a psychological phenomenon known as transaction decoupling. By forcing users to convert real currency into in-game virtual tokens, unique to that specific platform, the interface structurally severs the cognitive link between spending and real-world financial consequences. This cognitive disconnect is systematically paired with variable-ratio reinforcement schedules, the exact psychological mechanism that drives traditional gambling addiction. Modern gaming architectures wrap these feedback loops in structural frustration mechanics, where gameplay progression is intentionally restricted by artificial barriers, slow countdown timers, or mathematical disadvantages. The minor is faced with a calculated choice: endure hours of engineered tedium or submit to a microtransaction to bypass the friction, weaponizing behavioural impatience for financial gain. To counter these exploitative methodologies, European regulatory bodies have drastically accelerated their enforcement strategies against manipulative software design. The European Parliament has issued direct resolutions targeting predatory gaming architectures, calling for a ban on deceptive dark patterns and demanding strict harmonization of consumer protection laws regarding hidden monetization. Regulatory enforcement under the Unfair Commercial Practices Directive (UCPD) has increasingly reclassified these architectures not merely as aggressive marketing, but as legally prohibited exploitative practices. The directive specifically targets how pay-to-win loops and time-perishable Battle Passes exploit a minor's lack of commercial experience by manufacturing artificial scarcity. This structural urgency triggers

severe situational anxiety, forcing a psychological state where the child feels compelled to transact to avoid immediate competitive or social exclusion, capitalizing on the sunk-cost fallacy where minors feel they cannot stop playing without wasting prior temporal investments. Consequently, traditional parental safeguards like simple wallet restrictions or spending caps are fundamentally inadequate; they merely treat the financial symptom while leaving the underlying psychological coercion intact, often causing the child to experience extreme distress or actively seek workarounds. True protection requires parents to shift from passive gatekeeping to active architectural exposure, dismantling the illusion of these predatory economic systems directly at the interface level.

Why is it important to understand predatory architecture?

The core reason is the structural erosion of free will and financial literacy. Minors possess an unformed prefrontal cortex, making them neurologically defenceless against multi-layered behavioural traps designed by behavioural psychologists to bypass self-control. When a game uses frustration engineering or currency decoupling, it actively conditions the child to accept manipulative behavioural loops as a normal baseline for digital interaction, desensitizing them to financial risk and creating a direct neurological bridge toward gambling behaviours later in life.

Signs of predatory gaming exploitation

A minor experiencing exploitation within a gaming ecosystem will exhibit distinct behavioural shifts. Look for sudden, intense bursts of rage or anxiety triggered specifically by missing limited-time virtual seasons, an obsessive, anxious preoccupation with maintaining daily log-in streaks to avoid losing digital status, and a growing tendency to treat gaming as a stressful, mandatory chore or employment obligation rather than a voluntary and relaxing hobby.

Example from everyday life

A family noticed their young son went from loving a popular online battle game to having intense, tearful meltdowns over his persistent losses, desperately begging for a premium character upgrade to stay competitive. Suspicious of this sudden shift, the parents monitored his gameplay and realized he was trapped in a predatory matchmaking loop: the game was deliberately pairing his

un-upgraded character against older, fully paying players to exploit his frustration. Instead of simply banning the game, the parents showed how the software was intentionally rigging the matches to make him feel inadequate and force a purchase. Realizing he was being mathematically manipulated by a machine, his anxiety vanished, and he voluntarily deleted the app.

Activity: The 5-Minute Store Check

Take five minutes to sit next to your child while they open their favourite game's store screen and ask them to point out the single most expensive digital item available. Without lecturing, calculate together how many hours of real-world work or how many physical, tangible objects that purchase actually represents, triggering an immediate reality check that breaks the mental separation between virtual tokens and real money. Use this opportunity to introduce a vital safety check: ask your child what they would do if another player, especially a stranger or an online acquaintance, offered to "gift" them that exact item for free. Teach them that unexpected digital gifts should immediately serve as an alarm bell, as they are frequently weaponized as predatory bait for social engineering, hidden microtransaction traps, or account-stealing scams.

5.5 Building digital resilience: what to do when something goes wrong

Acknowledging that no technical guardrail or content filter is entirely foolproof is the foundational step in fostering true digital resilience, which is fundamentally defined as the ability to recognise risk, respond appropriately, recover after a negative online experience, and continue using digital technologies safely and confidently afterwards. In practice, this requires a shift toward proactive education, where raising conscious awareness and providing timely information serve as the primary pillars of prevention. This is practically achieved by embedding digital safety into transparent, everyday communication and actively accompanying minors as they navigate real-world online experiences. Within this framework, children should not be taught that the goal is to avoid every possible danger, because that is unrealistic; instead, they should learn how to react calmly and effectively when something goes wrong. A resilient child is not one who never encounters risk, but one who knows what to do next. This shifting of perspective is crucial because online incidents often happen quickly and leave children feeling confused, ashamed, or afraid of

getting into trouble. A child who receives a disturbing message, sees harmful content, is pressured by a stranger, or becomes the target of bullying may hesitate to tell an adult if they fear punishment, loss of device access, or being blamed for what happened. Consequently, reacting with unilateral anger or abrupt device confiscation is fundamentally counterproductive; may damage the relationship of trust between parents and children, causing young people to hide future problems rather than seek help. The first condition of resilience is therefore trust, meaning children need to know that disclosure will be met with emotional support, not panic.

At the family level, digital resilience begins with clear routines rather than abstract or one-time lessons, operating as a domestic habit built through repeated conversations. Children should know exactly which adult to tell, how to save evidence, when to block or report, and what steps will follow if they come across harmful material or suspicious contact. These steps work best when they are rehearsed in advance, because children are far more likely to act quickly in a real situation if the response has already been discussed calmly at home. When an online crisis materializes, effective remediation requires a synchronized approach that strictly separates emotional support from the technical response. The emotional response should be calm, reassuring, and non-judgmental, while the technical response must be practical and immediate: screenshots need to be preserved as evidence, accounts blocked, privacy settings reviewed, passwords changed, and reports submitted through the relevant platform or service. This immediate domestic intervention connects seamlessly with broader institutional frameworks; parents can leverage the safety tools mandated under the European Union's Digital Services Act, such as platform reporting systems and mechanisms for requesting the removal of illegal content, to demand swift content removal, or turn to the continent-wide network of European Safer Internet Centres for localized helpline support. If the incident involves severe escalation such as grooming, extortion, hate, or repeated harassment, the situation may also require immediate coordination with school staff, safeguarding professionals, or law enforcement, depending on the severity and local reporting pathways.

Furthermore, children need to understand that making a mistake online does not automatically mean they are responsible for what happens next. A child who accidentally clicks on a suspicious link, opens inappropriate content, or responds to a message from a stranger has not necessarily caused the problem; in many cases, they have simply encountered a risk they did not yet know

how to recognise. Making a mistake online should therefore be viewed as an opportunity for learning and guidance rather than immediate blame, provided the situation is recognised and addressed appropriately. In those cases, the key is not punishment but guided learning and architectural exposure, creating a reflective space where parents and children can calmly analyse what happened, identify which warning signs were missed, and discuss how a similar situation could be handled in the future. This approach helps children build judgment rather than fear, transforming the minor from a vulnerable target into a critical examiner of the digital ecosystem and become more aware and independent digital users. For older children and adolescents, resilience must include a stronger element of self-management, training them to recognise when online spaces are becoming emotionally unhealthy, when a conversation is turning manipulative, or when a platform is encouraging compulsive use rather than genuine social interaction. The goal is to help them develop internal warning systems so that they can step back before a problem becomes a crisis. Ultimately, a robust digital resilience model combines three distinct layers: prevention, through age-appropriate settings, parental guidance, and digital literacy; response, through clear reporting and support procedures; and recovery, through discussion, reassurance, and practical lessons that help the child avoid repeating the same mistake. Recovery should not focus only on resolving the incident itself, but also on rebuilding the child's confidence and sense of safety online. If these three layers are in place, digital resilience becomes the vital, practical counterpart to everything covered in the chapter; technical controls matter, but they are only part of the solution, as children need the confidence, knowledge, and family support to act when those controls are not enough, turning digital safety from passive protection into active competence.

Why is it important to understand digital resilience?

The core reason is that no child will navigate the internet without ever making mistakes or encountering risk. Digital resilience ensures that a negative online experience does not become a lasting crisis. Children who know how to ask for help, report problems, and recover from setbacks are more likely to remain confident, responsible, and safe digital users throughout adolescence and adulthood.

Signs of digital resilience in a minor

A minor who is developing strong digital resilience will exhibit distinct behavioural shifts. Look for an openness to actively share uncomfortable, distressing, or confusing online experiences with their parents without prompting or fear of punishment, an instinctive ability to immediately capture screenshots as evidence and block malicious users when encountering cyberbullying or suspicious contact, and a growing capacity for critical self-management, such as independently choosing to log off when an online space or platform begins to trigger emotional strain or compulsive usage.

Example from everyday life

Fifteen-year-old Marco is playing an online multiplayer game when he receives a private message from an unknown user offering free in-game currency through an external website. The message creates a sense of urgency, claiming that the offer will expire within a few minutes. Instead of clicking immediately, Marco remembers previous family discussions about online scams and manipulation techniques. He takes a screenshot of the message, avoids interacting with the link, blocks the user, and reports the account through the platform's reporting system. Later that evening, he shows the message to his parents and explains why it seemed suspicious. Together, they review the warning signs that helped him recognise the scam, including the pressure to act quickly, the promise of free rewards, and the request to leave the official platform. What could have become a security incident instead becomes confirmation that Marco is developing the confidence and judgment needed to navigate online risks independently.

The incident is resolved, but the conversation does not end there. Over the following days, her and his parents continue discussing how similar situations can be recognised and handled in the future. What could have become a source of fear or secrecy instead becomes a learning experience, strengthening her confidence and helping his feel more prepared to deal with future online challenges.

Activity: The Family "What-If" Rehearsal

Take ten minutes during a relaxed family moment to pitch a realistic, hypothetical scenario to your child, such as receiving a strange, uncomfortable message or an unexpected gift from an unknown user while playing online. Without lecturing, map out together the exact immediate steps they

should take: how to take a screenshot on that specific device, where the block and report buttons are located in their favourite app, and exactly who they would tell first, transforming abstract safety rules into a concrete, memorable domestic habit.

6. Recap: the main ideas of the chapter

This chapter provided a comprehensive blueprint for securing the family's digital ecosystem, balancing technical defences with proactive educational strategies. We demonstrated that beyond mere digital infrastructure, true safety depends on raising deep awareness and prioritizing prevention through continuous information and transparent communication, thus promoting active reasoning within minors. We began by debunking the myth of digital invulnerability, establishing that reliable antivirus software and immediate system updates constitute an indispensable first line of defence for both household computers and mobile devices. We then shifted focus to identity management, demonstrating how account security relies on a combination of complex passwords, the elimination of credential reuse, the activation of Two-Factor Authentication (2FA), and the use of Password Managers, all of which can be taught to children as their personal "secret keys."

Data protection was framed as an ongoing household practice that requires recognizing sophisticated phishing and social engineering tactics, utilizing VPNs on public networks, and tightening privacy settings on everyday smart home devices. On the behavioural side, we emphasized that technical tools must be paired with open communication, ideally through a mutually agreed-upon Family Digital Understanding that prioritizes trust over invasive spying. Finally, we analysed the most critical online threats facing minors today—such as cyberbullying, grooming, inappropriate content, and gaming scams—concluding that the ultimate goal is not to isolate children from technology, but to build their long-term digital resilience. This resilience ensures that when an online boundary is breached, families can reason together on corrective actions based on concrete data and observed facts, transforming these complex situations—whether arising from accidental missteps or inevitable external threats—into collaborative, guided learning experiences.

7. Quick Self-Assessment Test

Check what you've learned

Read the statements below and tick the key habits and concepts you feel confident practicing or discussing.

- ☐ Keeping computers, smartphones, tablets, and applications updated is one of the simplest and most effective ways to improve digital security.
- ☐ Antivirus software helps protect devices from many common threats, but it should always be combined with regular software updates and safe online behaviour.
- ☐ Using a different password for each account reduces the impact of a data breach.
- ☐ Two-Factor Authentication (2FA) provides an additional layer of protection even if a password is stolen.
- ☐ Phishing and social engineering attacks often create a sense of urgency, curiosity, or fear to persuade people to reveal personal information.
- ☐ Personal data includes more than names or financial details; it can also include browsing habits, location information, photos, and online activity.
- ☐ Website cookies may collect information about browsing behaviour, and families should check and choose consent choices rather than automatically accepting all cookies.
- ☐ Cloud services can automatically store copies of photos, files, contacts, and other information on remote servers linked to an online account.
- ☐ Smart home devices, such as Smart TVs, voice assistants, and connected toys, may collect and process personal data about how they are used.
- ☐ Parents should periodically review privacy settings, connected devices, and account security features used by the family.
- ☐ Parental control tools can support online safety, but they cannot replace communication, trust, and active parental guidance.

- Children may encounter online risks such as cyberbullying, grooming, inappropriate content, scams, and manipulative online behaviour.
- Online games may use in-app purchases, virtual currencies, limited-time offers, or other design techniques that encourage spending and prolonged engagement.
- Digital resilience means developing the knowledge, habits, and critical thinking skills needed to use technology safely, responsibly, and confidently.

Once you have completed the exercise, discuss your answers with other participants, family members, or your trainer.

8. How can we use this knowledge in everyday life

Translating the lessons of this chapter into daily habits does not require advanced technical expertise, only consistent routine adjustments. You can start immediately by gathering the family to draft a simple Family Digital Understanding, clearly defining screen-free zones and times, such as during meals or an hour before bedtime. Additionally, make it a habit to turn real-world digital interactions into learning moments; if a suspicious phishing text arrives on your phone, show it to your children to teach them how to spot the red flags of social engineering before they encounter them on their own devices.

Finally, dedicate a brief period each month to a household tech check-up. Use this time to ensure that automated backups are running correctly, check that device operating systems are fully updated, and verify that the privacy settings on your Smart TVs or voice assistants haven't been reset to default. By embedding these small checks into your regular family routine, digital security ceases to be a chore and becomes a natural, protective habit for everyone in the home.

8.1 Technical Glossary of Family Digital Safety

Letter A

Antivirus — A specialized computer program that operates in real-time as a digital immune system, responsible for monitoring, detecting, blocking, and removing malicious files before they can compromise digital identity or cause data loss.

Authenticator Apps — Dedicated software (such as Google or Microsoft Authenticator) that generates temporary, offline verification codes to add a layer of security to accounts, eliminating the risks associated with traditional SMS.

Letter B

Bark — A commercial parental control application based on artificial intelligence that target-scans chats, messages, and social networks to detect signs of cyberbullying or grooming, notifying the parent only in case of a real threat to protect the minor's privacy.

Behavioral Monitoring / Heuristics — Advanced antivirus technology that analyzes the actions performed by software in real-time instead of just searching for known code signatures, blocking anomalous behaviors caused by zero-day threats or mutating viruses.

Better Internet for Kids — A European Union strategic and non-regulatory policy framework established to fund safer internet centers, promote digital literacy, and foster the empowerment of minors online.

Biometrics — Local authentication systems (such as Face ID or fingerprint scanning) that utilize the user's biological traits stored within the device's secure hardware to unlock sessions or authorize the use of passkeys.

Letter C

CIE (Italian Electronic Identity Card) — A physical and cryptographic digital identity support that demonstrates the multi-factor approach, requiring a PIN code (something you know) and the smart card or smartphone (something you have) to access institutional services.

Cloud Storage — Internet-based storage networks that transfer and preserve personal data, documents, and photographs on external, remote servers, decoupling them from a single physical device but requiring constant synchronization.

Contextual Security — A modern protection logic that analyses the metadata and timing of a login attempt (the "digital letterhead"), raising authentication barriers only when it detects geographical or behavioural anomalies compared to the user's normal routine.

Cookies (and Tracking/Profiling Cookies) — Small fragments of text stored inside browsers, divided into necessary technical cookies and optional commercial profiling cookies, used by data brokers to map families' browsing habits and create market dossiers.

Credential stuffing — An automated cyberattack technique in which criminals use scripts to massively test databases of stolen emails and passwords across thousands of other websites, exploiting the widespread habit of credential reuse.

Cyberbullying — Repeated bullying, harassment, and aggressive behavior carried out over time by online users against minors through the use of social media and messaging platforms.

Letter D

Deepfake — Hyper-realistic multimedia content (in video, image, or audio format) generated through artificial intelligence tools capable of cloning human likenesses and voices, used by cybercriminals to orchestrate hyper-personalized family scams.

Dictionary attack — A variant of brute-force attacks in which a hacker employs a list of real words or common phrases, supported by artificial intelligence and specialized software, to attempt to guess a user's access key in sequence.

Digital Services Act (DSA) — A European regulation that establishes strict protections for minors on online platforms, banning manipulative designs and imposing default protection systems to counter the spread of harmful content.

DNS (Domain Name System) — A digital registry that translates website names typed by users into machine-readable numerical IP addresses; filtered DNS versions allow connections to dangerous domains to be blocked directly at the home router level.

Dwell time — A tracking parameter used by social media algorithms to measure to the millisecond how long a user stops scrolling on a post, exploited to outline psychological profiles and create cycles of digital dependence.

Letter E

Encryption — A mathematical process that transforms readable information into a scrambled, incomprehensible code, ensuring the confidentiality and integrity of personal data both in transit over networks and within storage servers.

ePrivacy — A European Union regulatory framework focused on protecting privacy, data protection, and confidentiality within the electronic communications sector.

EUDI Wallet (European Digital Identity Wallet) — An institutional digital wallet issued by European governments to host citizens' identities and connect to future online age-verification systems without exposing demographic data unrelated to the request.

Evil twin — Counterfeit Wi-Fi hotspots set up by attackers with names identical or similar to legitimate public networks to trick users into connecting, thereby intercepting their credentials and data traffic.

Letter F

Family Link (Google) — A centralized parental control application within the Android ecosystem that establishes a communication channel between the parent's and the child's phone to manage screen time, approve apps, and monitor geographical location.

Firewall — A cyber security barrier integrated into operating systems tasked with examining and filtering inbound and outbound data flows to prevent unauthorized access to the home network.

Forced consent — A digital tracking and aggressive marketing tactic where a website or social platform blocks access to its services unless the user selects extended data sharing or indiscriminate acceptance of all cookies.

Letter G

GDPR (General Data Protection Regulation) — A European data protection regulation that establishes legal ownership of information for individual citizens, guaranteeing rights of access, control, restriction, and the right to be forgotten on corporate servers.

Generative Artificial Intelligence — Advanced computational models used by cybercriminals to create dynamic attacks and error-free phishing messages, and integrated into commercial chatbots that store and analyze texts and files entered by users in prompts.

Grooming — A manipulative and psychological online practice used by malicious adults against children or adolescents, often disguised behind false identities within games or social networks.

Letter H

HTTP (Hypertext Transfer Protocol) — An obsolete network protocol for data exchange that does not apply any encryption, transmitting information in plain text and exposing it to interception and manipulation by third parties along the path.

HTTPS (Hypertext Transfer Protocol Secure) — A secure communication protocol that integrates the TLS protocol to encrypt the transit channel of data between the user's browser and the destination server, preventing local interceptions.

Letter I

In-app purchases — Financial transactions that occur within applications or video games downloaded onto digital devices, often used as bait for financial fraud against minors.

IP Address (Internet Protocol Address) — A unique numerical code assigned to each device connected to a network, used both to route communications and by security systems as verification metadata for access authenticity.

Letter K

Keylogger — A type of malicious software or surveillance tool that silently records every keystroke made on a digital device, frequently used by cybercriminals to steal sensitive data such as passwords, private messages, and financial credentials.

Letter M

Malware — A generic term grouping all malicious computer programs (including viruses, trojans, spyware, and ransomware) designed to compromise devices or steal personal information.

Malvertising — The insertion of malicious advertisements into legitimate and famous websites, capable of silently infecting visitors' devices without requiring explicit interaction.

Man-in-the-Middle (MitM) — A network cyberattack where a malicious actor positions themselves between the victim's device and the web access point to intercept, decrypt, or alter the transmitted data flow.

Metadata — Structured, hidden information embedded within digital files; in the case of photographs, it includes sensitive details such as the exact time, camera model, and GPS coordinates of the location.

MFA Fatigue — A fraudulent tactic based on mass-sending repeated push notifications for access authorization to the victim's smartphone, hoping they will approve the request by mistake or simply to clear their screen.

Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA) — Multi-level security protocols structured to validate the user's identity through a combination of three distinct pillars: something you know (the passphrase), something you have (the smartphone), and something you are (biometric data).

Letter P

Parental Control — Software systems and network filters acting at the operating system or router level to restrict access to entire categories of content unsuitable for minors and regulate device usage schedules.

Passkeys — Modern digital credentials that eliminate the use of textual passwords, replacing them with a cryptographic public-and-private key system linked to the user's device and activated via local biometrics.

Passphrase — An extended string composed of a sequence of words or an entire sentence, characterized by high mathematical entropy that makes it unassailable by cracking software, while remaining easy for the human mind to remember.

Password Manager (Digital Vault) — Digital safes protected by end-to-end encryption dedicated to the automatic generation, storage, and secure filling of long, complex, and unique login credentials for each web service.

Phishing — A cyber scam spread through deceptive communications via email, SMS (Smishing), or phone calls (Vishing) designed to replicate the aesthetics of trusted brands and induce the victim to enter passwords or payment details on fake portals.

Public-key cryptography — The mathematical infrastructure behind passkeys that relies on a public key stored on the website's server and a private key residing exclusively on the user's device, neutralizing phishing attempts.

Letter Q

Qustodio — A cross-platform parental control application that combines application blocking tools, web filters based on semantic categories, monitoring of searched videos, and SOS alarm systems with active geographical location.

Letter R

Ransomware — A class of malware that holds the infected device's files hostage by irreversibly encrypting them, subsequently demanding a ransom payment from the victim to obtain the decryption key.

Letter S

Scareware — Deceptive warnings and pop-ups designed to generate immediate panic and an artificial sense of urgency in the user, showing fake system infection messages to prompt them to buy useless software or surrender personal data.

Screen Time — A native control panel (present, for example, in Apple systems) that allows monitoring device usage and configuring usage restrictions, app limits, and downtime protected by a dedicated parental passcode.

Session tokens — Temporary digital credentials generated by web servers to keep a user logged into a service without forcing them to continuously type their password; if intercepted by criminals, they can allow unauthorized access to the account.

Signature Matching — A traditional scanning method used by antivirus programs that analyses the digital signature of a downloaded file, comparing it against a static database of already known and catalogued threats.

SIM swapping — A cyber fraud where criminals, using social engineering techniques on phone carriers, manage to transfer the victim's mobile number to a new SIM card in their possession, intercepting security codes sent via SMS.

Smart Home — A domestic ecosystem composed of connected appliances and smart objects that requires strict permission control and turning off hardware listening modules to prevent the monetization of private habits.

Smishing — A subcategory of phishing activities conducted exclusively through sending fraudulent SMS text messages to the victim's mobile phone.

Social Engineering — A set of manipulative techniques based on the study of human psychology aimed at inducing victims to perform imprudent actions or reveal confidential data by exploiting emotional levers such as anxiety, fear, or urgency.

Spear-phishing — A targeted evolution of classic phishing that uses real personal information about the victim (such as name or recent purchase details) gathered from the web to structure highly personalized and extremely convincing bait.

SPID (Public Digital Identity System) — An Italian digital identification infrastructure that adopts multi-factor protocols to guarantee secure and certified access to Public Administration portals.

Spyware — Malicious software configured to operate in the background without the user's knowledge, aiming to collect private data, monitor movements via GPS, or activate the microphone and camera to record the surrounding environment.

Stalkerware — Commercial applications for covert monitoring that require disabling the operating system's native defenses (rooting or jailbreaking) to hide, creating severe structural vulnerabilities that expose data to external leaks and hacking.

Synthetic Identity Theft — A fraud technique where criminals combine a minor's real, unblemished data (such as identification codes or birth dates) with entirely fabricated elements, creating a "ghost" profile to open fraudulent credit lines.

Letter T

Trojan — Harmful software disguised as legitimate applications, text documents, or free video games, designed to trick users into voluntarily installing it on their device, opening a breach for data theft.

Letter V

Vishing — A variant of phishing executed through direct voice calls, where scammers use social engineering and sometimes voice cloning to impersonate bank operators or relatives in distress.

VPN (Virtual Private Network) — A software service that creates an encrypted communication tunnel between the user's device and the internet, masking the IP address and protecting sensitive data from interception when connecting to public or unsecured Wi-Fi networks.

Letter W

Windows Defender — A security and antivirus suite natively integrated within the Microsoft Windows operating system, developed to offer basic protection and a system firewall at no additional cost.

Letter Z

Zero-Knowledge Architecture — A structural security model applied to personal password managers where data is encrypted on the device and the service provider holds no master key, making account recovery impossible in case of loss.

Zero-Knowledge Proofs (ZKP) — Advanced cryptographic protocols used in modern age-verification systems (like the European EUDI Wallet) that allow a software to answer a specific question (e.g., "Is the user of legal age?") by providing a binary answer without transmitting or revealing the underlying demographic data to the external server.

Bibliography

Chapter I

1. European Commission. (2022). *The Digital Competence Framework for Citizens (DigComp 2.2): With new examples of knowledge, skills, and attitudes*. Publications Office of the European Union.
2. European Commission. (2021). *Digital Education Action Plan 2021–2027*. Brussels: European Commission.
3. OECD. (2021). *21st Century Readers: Developing Literacy Skills in a Digital World*. OECD Publishing.
4. Livingstone, S., & Helsper, E. (2008). *Parental mediation of children's internet use*. Journal of Broadcasting and Electronic Media.
5. UNESCO. (2021). *Media and Information Literacy Curriculum for Educators and Learners*. UNESCO Publishing.
6. Council of Europe. (2019). *Digital Citizenship Education Handbook*. Strasbourg: Council of Europe Publishing.
7. European Commission. (2022). *Better Internet for Kids Strategy (BIK+)*.
8. Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe, Strasbourg.
9. European Commission. (2018). *Final Report of the High Level Expert Group on Fake News and Online Disinformation*. Brussels: European Commission.
10. Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel (Eds.), *Digital Literacies: Concepts, Policies and Practices* (pp. 17–32). New York: Peter Lang.

11. Ilomäki, L., Paavola, S., Lakkala, M., & Kantosalo, A. (2016). Digital competence – an emergent boundary concept for policy and educational research. *Education and Information Technologies*, 21(3), 655–679. <https://doi.org/10.1007/s10639-014-9346-4>
12. European Parliament and Council of the EU. (2006). *Recommendation on key competences for lifelong learning*. Official Journal of the European Union, L 394/10.
13. King, D. L., Delfabbro, P. H., & Griffiths, M. D. (2010). Video game structural characteristics: A new psychological taxonomy. *International Journal of Mental Health and Addiction*, 8(1), 90–106.
14. Marchionini, G. (2006). Exploratory search: From finding to understanding. *Communications of the ACM*, 49(4), 41–46.
15. European Commission. (2020). *European Digital Competence Framework for Educators (DigCompEdu)*. Publications Office of the European Union. https://joint-research-centre.ec.europa.eu/digcompedu_en

Useful online resources

1. European Commission – Digital Skills and Jobs Platform
<https://digital-skills-jobs.europa.eu>
2. European Commission – Safer Internet for Kids
<https://www.betterinternetforkids.eu>
3. EU Kids Online Research Network
<https://www.eukidsonline.net>
4. Common Sense Media – Digital Parenting Resources
<https://www.commonsensemedia.org>
5. Google Safety Center – Family Online Safety
<https://safety.google>
6. Microsoft Digital Safety Resources
<https://www.microsoft.com/digitalsafety>

7. European Centre for Child Online Safety – Resources for Parents
<https://www.insafe.eu>
8. JRC Digital Competence Centre – DigComp Framework
https://joint-research-centre.ec.europa.eu/digcomp_en
9. Romanian National Consumer Protection Authority (ANPC) – Online Shopping Guide
<https://anpc.ro>
10. FactCheck.org – Verifying information and countering disinformation
<https://www.factcheck.org>
11. Sigur.info – Internet safety for families (Romanian initiative)
<https://www.sigur.info>

Chapter II

1. European Commission. (2022). The Digital Competence Framework for Citizens (DigComp 2.2): With new examples of knowledge, skills and attitudes. Publications Office of the European Union.
2. European Commission. (2021). Digital Education Action Plan 2021-2027. Brussels: European Commission.
3. Livingstone, S., & Helsper, E. (2008). Parental mediation of children's internet use. *Journal of Broadcasting and Electronic Media*.
4. Anderson, M., & Jiang, J. (2018). Teens, Social Media and Technology 2018. Pew Research Center.
5. Royal Society for Public Health. (2017). #StatusOfMind: Social media and young people's mental health and wellbeing. London: RSPH.

6. Blum-Ross, A., & Livingstone, S. (2016). Families and Screen Time: Current Advice and Emerging Research. Media Policy Brief 17, London School of Economics.
7. Council of Europe. (2019). Digital Citizenship Education Handbook. Strasbourg: Council of Europe Publishing.
8. European Commission. (2022). Better Internet for Kids Strategy (BIK+).
9. World Health Organization. (2019). Guidelines on physical activity, sedentary behaviour and sleep for children under 5 years of age. Geneva: WHO.
10. Hiniker, A., Schoenebeck, S. Y., & Kientz, J. A. (2016). Not at the Dinner Table: Parents' and Children's Perspectives on Family Technology Rules. CSCW '16.

Useful online resources

European Commission: Digital Skills and Jobs Platform : <https://digital-skills-jobs.europa.eu>

European Commission: Safer Internet for Kids : <https://www.betterinternetforkids.eu>

EU Kids Online Research Network : <https://www.eukidsonline.net>

Common Sense Media: Digital Parenting Resources : <https://www.commonsensemedia.org>

Google Safety Center: Family Online Safety : <https://safety.google>

ConnectSafely: Parents' Guides to Technology : <https://www.connectsafely.org>

Internet Matters: Online Safety Advice for Parents : <https://www.internetmatters.org>

UNICEF: Digital World Resources for Parents : <https://www.unicef.org>

Chapter III

1. American Academy of Child and Adolescent Psychiatry. (s.d.). *Screen Time and Children*.
2. Better Internet for Kids (European Commission). (s.d.). *Guidance for parents on protecting children's privacy*.
3. Burr, W. E., Dodson, D. F., & Grassi, E. M. (2017). *NIST Special Publication 800-63B: Digital Identity Guidelines*. National Institute of Standards and Technology.
4. Childnet International. (s.d.). *Family Agreement*.
5. ENISA. (s.d.). *Homing on Smart Home Security? Smart! and related IoT security guidance*.
6. EU General Data Protection Regulation (GDPR). (2016). *Article 4 — Definition of personal data*.
7. European Commission. (2026). *Commission launches action plan to protect young people from cyberbullying*.
8. European Commission. (s.d.). *Action plan against cyberbullying – protecting children online*.
9. European Commission. (s.d.). *Children's rights in virtual worlds / Better Internet for Kids (BIK+)*.
10. European Commission. (s.d.). *Common approach for EU-wide age-verification technologies*.
11. European Commission. (s.d.). *Commission publishes guidelines on the protection of minors*.

12. European Commission. (s.d.). *EU age verification approach*.
13. European Commission. (s.d.). *Guidelines on the protection of minors under the DSA*.
14. European Commission / Better Internet for Kids. (s.d.). *Protection of minors and safer platforms*.
15. Internet Matters. (2026). *Online Grooming advice and risks*.
16. Nature. (2024). *Associations between media parenting practices and early adolescent screen use*.
17. NIH/PMC review. (s.d.). *Effects of Excessive Screen Time on Child Development*.
18. NSPCC. (s.d.). *Online safety family agreement*.
19. Livingstone, S., & Sefton-Green, J. (2016). *The Class: Living and Learning in the Digital Age*. New York University Press.
20. "Public WiFi Security Risks: The Complete Guide". (2026).
21. Raising Children Network. (2024). *Parents & screen time: role-modelling*.
22. Regulation (EU) 2016/679 (GDPR). (2016). *Article 8*.
23. Shay, R., & Kelley, P. G. (2016). *Can Long Passwords be Secure and Memorable?* In Proceedings of the CHI Conference on Human Factors in Computing Systems.
24. UCL. (2025). *Unofficial parental control apps put children's safety and privacy at risk*.
25. UNISOB article. (s.d.). *GDPR and children rights in EU data protection law*.
26. US Federal Trade Commission. (2026). *"Public WiFi Networks – Security Tips" – practical advice for nontechnical users*.
27. World Health Organization. (2019). *To grow up healthy, children need to sit less and play more*.
28. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power Public Affairs*.