

Trainer's Guide



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



**Co-funded by
the European Union**

Erasmus+ Programme – Strategic Partnership

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

Project coordinated by: SMART EDUCATIONAL PROJECTS Association



<https://departproject.eu/>

Partnerships



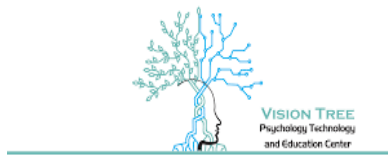
<https://www.sep-ngo.eu/>



<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

About This Guide	5
How to Use This Guide	6
CHAPTER I	7
WORKSHOP 1. Understanding, Searching and Organising Information	8
Module 1 - Information Literacy and Types of Content (45 min)	9
Module 2 - Information Searching and AI Tools (45 min)	12
Module 3 - Saving and Organising Information (45 min)	15
Module 4 - Useful Apps in Everyday Life + Ghişeu.ro (45 min)	17
WORKSHOP 2. Online Services, Children's Safety and Critical Thinking	37
Module 1 - Participating in Online Meetings (45 min)	38
Module 2 - Safe Online Shopping (45 min)	41
Module 3 - Online Games, Betting and Children's Safety (45 min)	43
Module 4 - Online Disinformation and Deepfakes (45 min)	47
Annex A - Participant Feedback Form	51
Annex B - Logistical Checklist for Trainers	52
Annex C - List of Useful Resources for Participants	53
Annex D - Consolidated Worksheets for Participants	54
WORKSHOP 1 - Understanding, Searching and Organising Information	54
Module 1 - Information Literacy and Types of Content	54
Module 2 - Information Searching and AI Tools	57
Module 3 - Saving and Organising Information	60
Module 4 - Useful Apps in Everyday Life	62
Worksheet for Workshop 2 - Online Services, Children's Safety and Critical Thinking	63
Module 1 - Participating in Online Meetings	63
Module 2 - Safe Online Shopping	65
Module 3 - Online Games, Betting and Children's Safety	68
Module 4 - Online Disinformation and Deepfakes	70
CHAPTER II	74
Workshop 1	75
Module 1. Let's Talk Online! (45 min)	75
Module 2. Social Media: Friend or Enemy? (45 min)	78
Module 3. Protect Yourself Online (45 min)	82
Module 4: Your Online Identity (45 min)	86
Workshop 2	89
Module 1. Your Digital Shadow (45 min)	89
Module 2. Breaking the Scroll (45 min)	93
Module 3. The Digital Parent Toolkit (45 min)	97

Module 4. When the Internet Hurts: Understanding Cyberbullying (45 min)	101
Annex A - Participant Feedback Form	106
Annex B - Logistical Checklist for Trainers	108
Annex C - List of Useful Resources for Participants	110
Annex D - Parent Worksheets for Chapter II	112
Workshop 1	112
 WORKSHEET 1	112
 WORKSHEET 2	114
 WORKSHEET 3	116
 WORKSHEET 4	118
Workshop 2	120
 WORKSHEET 5	120
 WORKSHEET 6	122
 WORKSHEET 7	125
 WORKSHEET 8	128
CHAPTER III	133
WORKSHOP 1	134
Workshop 1 Agenda	135
Module 1 - Device Protection & Updates (45 min)	137
Module 2 - Strong Passwords & Passphrases (45 min)	144
Module 3 - 2FA, MFA & Password Managers (45 min)	150
Module 4 - Personal Data & Recognising Phishing (45 min)	156
WORKSHOP 2	164
Module 5 - Public Wi-Fi, VPNs & Secure Websites (45 min)	167
Module 6 - Smart Devices, Cloud Privacy & Family Digital Contract (45 min)	173
Module 7 - Parental Controls, Screen Time & Leading by Example (45 min)	179
Module 8 - Online Risks for Children: from Cyberbullying to Digital Resilience (60 min)	186
Annex A - Participant Feedback Form	195
Annex B - Logistical Checklist for Trainers	197
Annex C - List of Useful Resources for Participants	199
Annex D - Notes for Translators and National Adaptors	201
Annex E - Parent Worksheets for Chapter III	202
WORKSHOP 1	202
 WORKSHEET 1	202
 WORKSHEET 2	
—	203

	WORKSHEET 3	205
	WORKSHEET 4	207
	WORKSHEET 5	209
	WORKSHEET 6	211
	WORKSHEET 7	213
	WORKSHEET 8	215
	WORKSHEET 9	217
	WORKSHEET 10	219
	WORKSHOP 2	221
	WORKSHEET 11	221
	WORKSHEET 12	222
	WORKSHEET 13	224
	WORKSHEET 14	227
	WORKSHEET 15	229
	WORKSHEET 16	230
	WORKSHEET 17	232
	WORKSHEET 18	234
	WORKSHEET 19	235
	WORKSHEET 20	237
	WORKSHEET 21	239
	WORKSHEET 22	240

About This Guide

This Trainer's Guide is the methodological companion to the DEPART Digital Education Guide for Parents. It was developed 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. Where the Parents' Guide provides the content, examples, and activities addressed directly to parents, this Trainer's Guide provides the facilitation script for the corresponding workshops - the agenda, step-by-step trainer instructions, key messages, facilitation tips, and solutions for common challenges. The two documents are meant to be used together and are addressed to different readers: the Parents' Guide is written for adults with children, regardless of their digital competence level; this Trainer's Guide is written exclusively for trainers.

For whom it is intended: trainers in the DEPART network, partners involved in dissemination, adult educators working with parents with limited access to technology, community mediators, and volunteers involved in digital literacy projects for parents.

Workshop philosophy: across all three chapters, facilitation starts from parents' real, everyday experience rather than abstract theory or technical jargon. The tone is warm, non-judgmental, and normalizing - digital skills and digital security are treated as a natural extension of things parents already do to look after their families, not as a specialist subject. Content is kept small, practical, and repeatable at home, and the trainer's role throughout is to guide participants alongside them, not to position themselves as an expert above them.

This guide is organized into three chapters, each developed by a different DEPART project partner:

- **Chapter I – Information literacy and the use of online services**, developed by Asociația SMART EDUCATIONAL PROJECTS, Romania, the project coordinator;
- **Chapter II – Communication and collaboration in the online environment**, developed by Vision Tree – Center 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.

How to Use This Guide

Each chapter is primarily a trainer's tool for the DEPART project, delivered by a trained trainer to a group of 8–14 parents. Chapters I and III are each structured as two 3-hour-45-minute workshops of four 45-minute modules (plus opening, closing, and a break); Chapter II is structured as eight shorter, self-contained 45–60 minute workshops, one per section of its corresponding chapter of the Parents' Guide, delivered with no break required. Trainers should follow the agenda given at the start of each workshop or module, and may also refer to the project's separate Methodological Guide for further facilitation support.

Every module or workshop follows a consistent internal structure: learning objectives, the materials needed, a step-by-step activity plan with timings, the key messages to be repeated at the end, and a set of trainer tips drawn from previous or pilot deliveries. As a basic principle, the Parents' Guide is for the eyes of participants; this Trainer's Guide (Part II) is for the eyes of the trainer and is never read aloud during a workshop. Before each workshop, trainers should check their logistical preparation using that chapter's own Annex B - Logistical Checklist for Trainers.

Throughout all three chapters, a small set of shared icons flags different kinds of content:

 Trainer Note (for the trainer only, not to be read aloud),

 Group Activity (an interactive exercise for the whole group or small teams),

 Discussion (an open discussion prompt), and

 Handout Moment (the point at which the matching parent worksheet is distributed and used).

Each workshop or module has a corresponding parent worksheet, printed in advance and handed out during the session. Chapter I's worksheets are already compiled in its own Annex D - Consolidated Worksheets for Participants. Chapter II and Chapter III did not previously include a consolidated worksheet annex of their own; for this integral edition, the full worksheet booklets developed for each of those chapters have been added as a new final annex at the end of each chapter's section - Annex - Parent Worksheets for Chapter II, and Annex E - Parent Worksheets for Chapter III (continuing the letter sequence after Chapter III's own Annexes A–D). Each chapter also ends its workshops with a short participant feedback exercise (Annex A) and, where useful, a list of resources for participants (Annex C).

CHAPTER I

WORKSHOP 1. Understanding, Searching and Organising Information

Total duration: 3 hours 45 minutes (225 minutes) | Target group: parents | Break: 15 minutes at mid-point

Covers sections 1–4 of Chapter I of the theoretical part.

General Objective

By the end of the workshop, parents will be able to search for, verify, save, and use online information more consciously, using applications useful in everyday life.

Specific Objectives

- They recognise that not all online information is correct and that the first result in a search is not automatically the best.
- They apply the 3-Check Rule before believing or sharing information.
- They can formulate a clear search, recognise sponsored results and the AI summary at the top of the search page.
- They save and organise files using a simple structure (folders, clear names, backups).
- They identify a minimum of 3 useful applications for organisation, navigation and payments.
- They leave with 1–3 concrete actions they will apply at home.

Workshop 1 Agenda

Time	Activity	Description
00:00–00:15	Arrival, introduction, ice-breaker	"Who am I, what do I most often search for online."
00:15–01:00	M1: Information literacy	3-Check Rule, difference between Information/Opinion/Ad (sec. 1).
01:00–01:45	M2: Information searching + AI	Search rules, AI Overview, ChatGPT (sec. 2).
01:45–02:00	Coffee break	-
02:00–02:45	M3: Saving and organising information	3-2-1 Rule + 10-Second Test (sec. 3).
02:45–03:30	M4: Useful apps + Ghișeul.ro	Categories + practical simulation (sec. 4).

03:30–03:45	Summary, personal plan, feedback	"One thing I will do starting tomorrow."
-------------	----------------------------------	--

Opening (15 min) - Welcome and Ice-Breaker

Objectives:

- Creating a relaxed, pressure-free atmosphere.
- Identifying participants' previous experiences with online information.

Step by step:

- Greet participants individually at the entrance; help them write their first name on a name badge (3 min).
- Introduce yourself briefly (name, role in the project, two sentences about how you also use the internet in everyday life). Demystify the role of "expert". (2 min)
- Present the group rules in 30 seconds: we listen to the end, there are no stupid questions, phones stay on the table (we will use them). (1 min)
- Quick introduction circle: "My name is... and the last thing I searched for on the internet was..." (8 min, max 30 sec/person).
- Briefly announce the agenda and what they will take home. (1 min)

Trainer tips:

- If someone says "I don't really use the internet", respond: "then you are exactly the right person for today's workshop."
- Do not correct technical language ("the tablet", "the Google page"). Use the participant's own wording.
- Distribute the folders with Chapter I from Part I (for parents) at the beginning of the workshop, not at the end.
- Do not skip the introductions - they are essential for building trust.

Module 1 - Information Literacy and Types of Content (45 min)

↪ Correspondence with Part I: Section 1 (1.1–1.4) - "Information and Data Literacy".

Learning Objectives

- The participant recognises that not all online information is correct.
- The participant distinguishes between information, opinion, and advertising (including hidden advertising - sponsored content from influencers).
- The participant applies the 3-Check Rule before believing or sharing information.

Materials Needed

- Flipchart with "THE 3-CHECK RULE" (covered until the right moment).
- Projector + 3–4 examples for the same search: official site, personal blog, exaggerated title, sponsored result.
- Folders with Part I open at section 1.4.
- Worksheets 1, 3 and 4 from the Workbook (Workshop 1, Module 1).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation	Opening question: "When you search for something on the internet, do you usually choose the first result?" Write 2–3 answers on the flipchart. If they answer quickly, go deeper: "Has it happened that you were not sure whether online information was correct?"	-
5–15 min	"What do I choose and why?" (Worksheet 1)	Project 3 examples for the same search. In pairs, participants decide which one they would open. Plenary: what inspires trust, what makes you more careful, what is more useful.	The first result is not always the best.
15–25 min	Information / Opinion / Advertising / Hidden Advertising (Worksheet 3)	Present 2–3 examples: official announcement, blog article, advertisement, emotional headline, influencer paid recommendation. In pairs, identify the type. Highlight hidden advertising - the new and most problematic concept for parents.	Not all online messages have the same purpose.

25–40 min	The 3-Check Rule (Worksheet 4)	Reveal the flipchart with the 3 questions: Who published? When? Does it appear on other trusted websites? Apply together on a real example. For sensitive subjects (health, finances), introduce the 5 Independent Sources Rule.	I check before I believe or share.
40–45 min	Summary and transition	Brief recap of the 3 checks. 2-min discussion: common mistakes - choosing the first result, not checking the source, confusing an ad with information, sharing too quickly.	Pause before you believe or pass it on.

Key Messages of the Module

1. Anyone can publish information online; not all of it is correct.
2. Not all messages have the same purpose - some inform, others sell. Hidden advertising looks like an ordinary article.
3. Before we believe or share information, we apply the 3-Check Rule.

Trainer Tips

- Use LOCAL examples: the child's school website, the local council, an announcement on Facebook.
- Avoid technical jargon ("algorithm", "indexing", "SEO") - say "how Google arranges results".
- Insist on "hidden advertising" - it is the new and surprising concept for parents.
- If someone says "I always trust the first result", normalise it: "that's what we all do, it's how we're used to it".

Final message for participants: We don't need to know everything about the internet to use it better. It is enough to pause for a moment, compare, and ask a few simple questions.

Module 2 - Information Searching and AI Tools (45 min)

Updated module: includes AI Overview (the AI summary at the top of the Google search page) and conversational AI tools (ChatGPT, Gemini, Copilot).

↪ *Correspondence with Part I: Section 2 (2.1–2.4) - "Searching for information on the internet".*

Learning Objectives

- The participant formulates more precise searches, with relevant details.
- The participant distinguishes between the AI Overview summary, sponsored results and organic results.
- The participant knows conversational AI tools and their limitations.
- The participant recognises and applies the 4-Step Search Rule.

Materials Needed

- Laptop connected to a projector, browser open with Google.
- Demo account on ChatGPT, Google Gemini or Microsoft Copilot prepared.
- Flipchart with "4 STEPS TO A BETTER SEARCH".

- Worksheets 1, 2, 3 and 4 from the Workbook (Workshop 1, Module 2).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation	Question: "What did you last search for on the internet and didn't find immediately?" Write 2 real examples on the flipchart - they will be used in the following activities.	-
5–15 min	"General vs. Clear" demo + AI Overview (Worksheet 1)	On screen: a real search. Step 1 - general search "activities for children". Show the 3 zones: AI Overview summary (in a box), sponsored results ("Ad"/"Sponsored"), organic results. Step 2 - clearer reformulation: "educational activities for 8-year-old children, weekend". Compare. Participants complete Worksheet 1.	A clearer search brings more useful results.
15–20 min	What AI Overview is and isn't	Limitations of the AI summary: may contain errors (sometimes serious); does not always include verifiable sources; not written by a human expert. Rule: scroll down to read the original articles.	-
20–30 min	Ads and sponsored results (Worksheet 3)	Show the "Sponsored"/"Ad" label. Discussion: how do you know a result is paid? Participants complete Worksheet 3.	Not all results have the same value or purpose.
30–35 min	Conversational AI tools	Quick demo in ChatGPT/Gemini with a practical question ("What educational activities for 10-year-old children?"). Highlight: they can be useful, they can be inaccurate, do NOT share sensitive personal data (ID number, address, medical or financial data).	-
35–45 min	The 4-Step Rule (Worksheet 4)	Reveal the flipchart: Start simply → Add details (age, place, purpose, time) → Compare 2–3 results → Observe what I choose. Apply on a real example from participants.	Online searching is better step by step.

Key Messages of the Module

1. A clearer search brings more useful results.
2. The AI summary and sponsored results appear above organic results - scroll down.
3. AI tools are useful for quick explanations, but not for sensitive data.

Trainer Tips

- Ask participants to do the search on their own phone, not just on the projector.
- Pair a more confident participant with a more withdrawn one - it works as mentoring.
- Check the AI tool BEFORE the workshop - interfaces change frequently.
- Do NOT go into details about AI model training. The subject is use, not the technology.
- If the question "but what if AI lies?" comes up - respond calmly: "it sometimes happens; that's why we check with other sources".
- Do not go into advanced operators ("site:", quotation marks) - they confuse the audience.

Final message for participants: We don't need to search perfectly. It is enough to search more clearly, compare, and choose more carefully.

Break - 15 minutes

The break is not eliminated. Stay in the room with participants and answer individual questions - this is where real trust is built.

Module 3 - Saving and Organising Information (45 min)

↪ Correspondence with Part I: Section 3 (3.1–3.2) - "Storing and managing information".

Learning Objectives

- The participant identifies the main storage methods (computer, USB, external HDD, cloud) and the advantages/risks of each.
- The participant applies the 3-2-1 Rule: 3 copies, 2 different media, 1 in the cloud.
- The participant uses a simple naming formula: [Type]_[Content]_[Date].
- The participant knows the 10-Second Test for organisation.

Materials Needed

- Folders with Part I open at sec. 3.
- Flipchart with the storage methods matrix (prepared in advance).
- 6 "bad" file names written on cards (e.g.: "Document1", "Final", "Final_final2", "New_photo", "IMG_2023", "Contract").
- Worksheets 1 and 2 from the Workbook (Workshop 1, Module 3).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation - "The frustrating moment"	In pairs, participants complete: "The most frustrating moment when I couldn't find a file was...". Plenary: 2–3 examples. Questions: "How much time did you lose?", "How did you feel?"	We have a real need, not just a theoretical one.
5–15 min	Storage methods + Smart choice (Worksheet 2)	Matrix of methods × advantages × risks: computer (fast, but fragile); USB (portable, easy to lose); external HDD (capacity, depends on cable); cloud (access from anywhere, depends on internet); CD/DVD (long archive, old technology). Participants choose 2	We combine methods, we don't store in just one place.

		combined methods for: family photos, work documents, long archive, multi-device files.	
15–25 min	Top 3 mistakes + The 3-2-1 Rule	Common mistakes: weak passwords for cloud (e.g. "123456"); no backup; saving in only one place. For each: "what is the risk?", "what could they do differently?". Introduce the 3-2-1 Rule: 3 copies, 2 different media, 1 in the cloud. Mini-exercise "Raise your hand if you've done this" - normalises the problem.	3 copies, 2 media, 1 in the cloud.
25–35 min	The 10-Second Test + organisation	"How long does it take you to find a bill on your phone or laptop?" Write down answers. Golden rule: "If you can't find it in 10 seconds, the system isn't good." Present 2 structure models: by type (Documents/Photos/Work) or by role (Personal/Professional). Naming formula: [Type]_[Content]_[Date] with examples.	If you can't find it in 10 seconds, change the system.
35–45 min	"Order from chaos" (Worksheet 1)	On cards, "bad" file names: Document1, Final, IMG_2023, New_photo, Contract, Final_final2. Participants rename them using the formula. Competitive element: "Who renames most clearly?"	I name files for myself a year from now, not just for today.

Key Messages of the Module

1. We don't keep everything in one place.
2. We organise regularly, not rarely. We name files so that we understand them even a year from now.
3. Backup is essential - the 3-2-1 Rule.

Trainer Tips

- Do not go into details about specific cloud providers - mention Google Drive and Dropbox (from Part I) and move on.
- Passwords are the subject of the applications workshop (M4). Here just mention "strong passwords for the cloud account".

- Use real examples: the child's kindergarten photo, the electricity bill, a copy of the ID card.
- Emphasise that the 10-Second Test is a practical indicator, not a reprimand.
- Limit the concrete action to 3 steps: "Tomorrow I will create the folder Personal/Bills", "I will move the photos to Drive", "I will change the password".

Final message for participants: Don't keep everything in one place. Organise regularly, not rarely. Name files so you understand them a year from now, not just today.

Module 4 - Useful Apps in Everyday Life + Ghișeul.ro (45 min)

↔ Correspondence with Part I: Section 4 (4.1–4.3) - "Utility applications - Digital tools for everyday life".

Learning Objectives

- The participant identifies 3 categories of useful applications and concrete examples in each.
- The participant carries out a practical exploration of Ghișeul.ro.
- The participant consciously compares the "at the counter" option with the online option.
- The participant applies security rules: passwords of 10–12 characters, apps only from official stores, no sensitive data on public Wi-Fi.

Materials Needed

- Internet connection and participants' phones (announce in advance).
- Table prepared on flipchart: "At the counter vs. online".
- Ghișeul.ro website open as demo on laptop.
- At least 3 spare phones or laptops for those who don't have one or have problems.
- Worksheets "Useful apps" and "At the counter vs. online" from the Workbook.

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation - "Without a phone?"	Question: "What would be hardest to live without if your phone was missing tomorrow?" Quick discussion in pairs (2 min). Plenary: write down 4–5 answers (alarm, map, weather, payments, messages with the child).	We already use apps - the question is how to use them better.
5–15 min	3 categories with concrete examples (Categories Worksheet)	Organisation/productivity (Google Calendar, Todoist, OneNote - "tomorrow morning"); Navigation/transport (Google Maps, Waze - "trip to a new address"); Payments/public services (Romania: Ghişeu.ro; Italy: PagoPA/App IO; Slovenia: eUprava/eDavki; Belgium: MyMinfin/MyGov.be; Poland: obywatel.gov.pl; PayPal, Google Pay - "paying local tax without going to the counter"). Participants write down their own examples.	Apps solve real, not abstract, problems.
15–25 min	Ghişeu.ro simulation (Ghişeu.ro Worksheet)	In pairs, practical navigation: where to create an account, what payments are available, what the steps of a payment look like (up to the completion moment - NO real data). Have the local example ready: the name of the local council + local tax payment.	We apply to real examples.
25–35 min	At the counter vs. online (Comparative Worksheet)	Table on 6 criteria: time, travel, schedule, comfort, stress, control. Participants complete the worksheet with their own comparison. Plenary: "What would help you move from the counter to online?"	The choice is personal: there is no "correct", there is what's "right for you".
35–45 min	Security rules + mini-task	Passwords of 10–12 characters (letters, numbers, symbols); apps only from official stores; regular updates; no sensitive data on public Wi-Fi; do NOT tick "Remember my password" on public computers. Mini-task: each person writes down 2 changes they will make.	Security depends on us.

Key Messages of the Module

1. We already use apps - the question is how to use them better.
2. The choice between the counter and online is personal: there is no "correct" option, there is what's right for you.
3. App security depends on us: strong passwords, official apps, care with personal data.

Trainer Tips

- Never ask participants to enter real personal data (ID number, passwords, bank account).
- If someone gets stuck at a step, go TO that person; don't correct from a distance.
- Have the local example ready: the local council + local tax payment for that locality.
- For banking apps: only say "it is downloaded from the official store, through your bank", without recommending any particular bank.
- Use the 3 spare devices for participants without their own or with difficulties.

Final message for participants: We already use technology - the question is how to use it more safely and more to our advantage.

Workshop 1 Closing (15 min)

Objectives:

- Summary of the 4 modules in simple messages.
- Personal plan: 1–3 concrete actions for the coming week.
- Collecting feedback.

Step by step:

- Visual summary on flipchart (3 min): recap the 4 key messages in one sentence each.
- "Word wheel" (5 min): each participant says, in one sentence, one thing they will do starting tomorrow.
- Referral to Part I (2 min): "At home, re-read Chapter 1 of your guide - you will find everything we discussed today, with additional examples."
- Feedback form - Annex A (3 min).
- Announcing Workshop 2: date, location, what we will do (2 min).

Final message for participants - Workshop 1: We don't need to know everything about the internet to use it better. It is enough to pause for a moment, compare, and ask a few simple questions. Thank you for being here today.

WORKSHOP 2. Online Services, Children's Safety and Critical Thinking

Total duration: 3 hours 45 minutes (225 minutes) | Target group: parents | Break: 15 minutes at mid-point

Covers sections 5–8 of Chapter I of the theoretical part.

General Objective

By the end of the workshop, parents will be able to confidently participate in online meetings, shop safely online, talk with their children about online games and betting, and recognise disinformation before sharing it.

Specific Objectives

- They can participate step by step in an online meeting, with a preparation checklist.
- They use a short verification list before paying online.
- They know the main types of games and betting platforms to which children are exposed and can have a calm conversation with the child.
- They apply simple steps to recognise a fake news story, including a deepfake.

Workshop 2 Agenda

Time	Activity	Description
00:00–00:15	Recap + ice-breaker	What did we apply last week? + opinion barometer.
00:15–01:00	M1: Participating in online meetings	Steps + checklist + real simulation (sec. 5).
01:00–01:45	M2: Safe online shopping	Comparing 2 shops + checklist before payment (sec. 6).
01:45–02:00	Coffee break	-
02:00–02:45	M3: Online games + betting	Types, risks, conversation with the child (sec. 7).
02:45–03:30	M4: Online disinformation + deepfakes	5 signs + 3-Check Rule (sec. 8).
03:30–03:45	Summary, personal plan, feedback	"One thought I take with me."

Opening (15 min) - Recap and Ice-Breaker

Objectives:

- Reactivating connections established in the first workshop.
- Identifying concrete changes made by participants in the previous week.

Step by step:

- Welcome + name badges (2 min).
- Quick circle: "My name is... and since the last workshop I tried / I noticed..." (5 min).
- "Opinion barometer" (6 min). Three corners of the room: YES / NO / DON'T KNOW. Read statements, participants move physically: "I participate easily in an online meeting" • "I shop online at least once a month" • "I know what games my child uses" • "It sometimes happens that I'm not sure whether an online story is true".
- Announce the agenda (2 min).

Trainer tips:

- The barometer breaks the ice physically. Adults who didn't speak at the first workshop will smile when they move between corners.
- Don't comment on the choices. Just ask "why did you choose here?" and listen.
- Validate the changes made last week, however small. "You created a folder? Excellent."

Module 1 - Participating in Online Meetings (45 min)

↔ Correspondence with Part I: Section 5 (5.1–5.4) - "Using videoconferencing services".

Learning Objectives

- The participant knows the basic steps to join an online meeting.
- The participant uses a pre-meeting checklist.
- The participant identifies a minimum of 2 common problems and a solution for each.

Materials Needed

- A Zoom, Google Meet or Microsoft Teams meeting link prepared in advance, functional.
- At least 3 devices available for practice (trainer's laptop + participants' phones + spare tablets).
- Worksheets 1, 2, 3 and 4 from the Workbook (Workshop 2, Module 1).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation - "Starting situation" (Worksheet 1)	Launch the situation: "You have an online meeting with the child's teachers in 2 minutes. The link comes via email or message. The microphone, camera or connection may not work. What do you do first?" Participants complete Worksheet 1.	-
5–15 min	Basic steps (Worksheet 2)	On-screen demonstration of the 6 steps: open the message/email; find the link; click the link; enter name (if required); check microphone and camera; join the meeting. Participants tick on Worksheet 2 the steps where they feel they need more help.	Joining an online meeting is learned step by step.
15–25 min	Actual simulation	Send participants the test link. Each person joins from their own device. The trainer stands next to those with difficulties. Steps: receive the link (SMS/email); open the link; enter name; check microphone (speak with a partner); check camera; leave the meeting and rejoin.	"Actually doing it" is much more than "hearing how it's done."
25–35 min	Common problems and solutions (Worksheet 3)	No sound - check microphone/volume/app permissions. Camera doesn't work - check permissions (phone: Settings). Link doesn't open - copy into another browser; ask for the link again. Weak internet - move closer to the router; turn off camera. Don't know where to click - ask for help in the chat or by phone.	Technical problems are normal and can be solved step by step.
35–45 min	Pre-meeting checklist (Worksheet 4)	List: have the link; device is charged; know where to click; microphone works; camera works; in a quiet place; know what question I want to ask. Participants complete Worksheet 4.	Simple preparation reduces stress more than anything else.

Key Messages of the Module

1. Joining an online meeting is learned step by step - it's normal not to get it right the first time.
2. "Actually doing it" is much more than "hearing how it's done."
3. Simple preparation reduces stress more than anything else.

Trainer Tips

- Test the link BEFORE the workshop. Nothing kills trust like a broken simulation.
- Keep the simulation short (10 min), but make everyone join at least once.
- For those who genuinely cannot do it: sit with them and guide them individually.
- Don't promise "it will always work like this" - technical problems are normal.

Final message for participants: You don't need to be a technology expert to join an online meeting. You need a link, a device, a quiet minute - and to follow the steps.

Module 2 - Safe Online Shopping (45 min)

↪ Correspondence with Part I: Section 6 (6.1–6.4) - "Online shopping".

Learning Objectives

- The participant identifies signs of trust and signs of risk.
- The participant uses a verification list before paying.
- The participant understands that a price that is too low may hide a risk.

Materials Needed

- 2 online shops prepared (one well-known - eMag/Amazon, one less known).
- Flipchart with "SIGNS OF TRUST / SIGNS OF RISK".
- Worksheets 1, 2, 3 and 4 from the Workbook (Workshop 2, Module 2).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation - "Would I buy or not?"	Situation: "You want to buy something for your child. You find an unknown website, very low price, little information. Do you buy?" Quick discussion in pairs (2 min), then 2–3 reactions in plenary.	-
5–15 min	"Would I buy or not?" with examples (Worksheet 1)	Present 2–3 examples: well-known, well-structured site; unknown site with little information; attractive but unclear offer ("today only"). Participants complete Worksheet 1 with the reasons.	A good price is not enough.

15–25 min	What we compare beforehand (Worksheet 2)	Criteria: price (realistic? suspiciously low?); delivery (cost, time, collection); returns (duration, who pays?); reviews (visible? positive vs negative?); company details (company number, address, phone); security (HTTPS/padlock). In pairs, compare 2 shops.	Before buying, we compare more than just the price.
25–35 min	Signs of trust / risk (Worksheet 3)	On the flipchart, 2 columns. Trust: known site, visible reviews, company details, clear conditions, HTTPS, clean appearance. Risk: suspiciously low price, no company details, no reviews, grammatical errors, pressure ("only now"), unnecessary requests for personal data.	Sometimes, a good deal hides a risk.
35–45 min	Pre-payment checklist (Worksheet 4)	8 points: site known or clear; realistic price; reviews exist; clear delivery; return option exists; company details visible; site secured (HTTPS); no unnecessary personal data requested. Participants use the worksheet on their own example.	We check before payment, not after.

Key Messages of the Module

1. A good price is not enough.
2. Before paying, we compare and pause for a moment.
3. If an offer seems too good to be true, it probably is.

Trainer Tips

- Don't turn the module into an e-commerce lesson. Focus on making a better decision, not on features.
- Don't use examples of famous frauds - they induce panic. Use ordinary examples.
- Normalise hesitation: it's good to pause and check, it's not a weakness.
- Highlight the padlock (HTTPS) and that you can click on it to see who owns the site.
- Don't recommend any particular shop; mention 2–3 as examples.

Final message for participants: We don't need to buy fast to buy well. It is enough to pause for a moment, compare, and check before payment.

Break - 15 minutes

Module 3 - Online Games, Betting and Children's Safety (45 min)

Module with 2-part structure: online games (25 min) + online betting (20 min).

↪ *Correspondence with Part I: Section 7 (7.1–7.2) - "Online games, betting and associated risks".*

Learning Objectives

- The participant knows the main types of online games to which children are exposed and the associated risks.
- The participant recognises 4–5 warning signs (games and betting).
- The participant practises a conversation with the child, without an accusatory tone.
- The participant knows where to find parental control settings.

Materials Needed

- Prepared lists with popular games and PEGI ratings.
- Flipchart with "WARNING SIGNS".
- Worksheets 1, 3 and 4 from the Workbook (Workshop 2, Module 3).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	Activation games	- Open questions: "What online games do your children use?", "How much time do you think they spend daily?", "What worries you most?" Write down 2–3 answers.	Games are not automatically dangerous; the problem arises when we don't know what our children are doing.
5–15 min	4 categories of games (Worksheet 1)	Multiplayer with chat (Roblox, Fortnite, Minecraft) - contact with strangers, cyberbullying. Microtransactions (EA Sports FC (formerly FIFA UT), Genshin, "loot boxes") - spending, gambling-type behaviour. Violent/horror (GTA, Outlast, FNAF, CS2) - anxiety, nightmares. Dangerous challenges (e.g.: Skull Breaker, Blackout Challenge, self-harm challenges on TikTok - note: Blue Whale and Momo were largely media-amplified moral panics; verify the currency of examples before each workshop) - serious injuries, manipulation.	Different categories, different risks.

15–20 min	Myth or reality	Show of hands: "All online games are dangerous" → MYTH. "Children can talk to strangers in many games" → REALITY. "Most children tell parents if something happens online" → MYTH. Brief explanations (30 sec each).	-
20–25 min	Signs + solutions (Worksheet 3)	5 possible signs: hides what they're doing on the phone; quickly closes apps when a parent enters; stays online very late; becomes withdrawn or irritable; unexplained scratches/bruises. Important: one sign alone is not necessarily a problem, but it is an indicator. Solutions: open conversation, PEGI (pegi.info), play together, parental controls (iOS Screen Time, Android Digital Wellbeing, Microsoft Family Safety, Google Family Link).	It's not prohibition that protects, it's the relationship.
25–30 min	How children get to betting	Channels: social media ads, sports apps, streamers (Twitch, YouTube, Instagram), TV ads, conversations with friends, games with gambling mechanics (loot boxes). Question: "Which seems most common for your child?"	Exposure is greater than it seems.
30–35 min	Risks for children and adolescents	Addiction (system designed to keep them engaged); financial (pocket money, sometimes parents' accounts); emotional (frustration, anxiety); academic (concentration, fatigue). Mini "Myth or reality": "if you win once, you have better chances" → MYTH; "adolescents become addicted more quickly" → TRUE.	Betting is designed for the house's profit.
35–40 min	Role play "How do we react" (Worksheet 4)	2 volunteers play: the wrong version ("You're wasting time again! You do what you want all day!") vs. the constructive version ("I noticed you	Curiosity, not accusation.

		often follow sports scores. Would you like to tell me what you're passionate about?"). 2-min discussion: what difference does the tone make? Participants formulate a phrase on Worksheet 4.	
40–45 min	Family rules	On Worksheet 4, each person decides 3 rules: time limits, no phone at night, online payments only with parental consent, transparency on apps, no unknown friends. Reflection: "How can we discuss this with the child so they are more easily accepted?"	Simple rules, agreed with the child, work better.

Key Messages of the Module

1. Online games and betting are not automatically dangerous - the problem arises when we don't know what the child is doing.
2. The best protection is not prohibition, but the RELATIONSHIP with the child.
3. An early conversation, without accusations, is the most effective form of prevention.

Trainer Tips

- Avoid a "specialist" tone. You are not a clinical psychologist; you are a trainer presenting reference frameworks.
- Recommend that parents seek professional support if they see serious signs (isolation, radical change).
- Do not ask participants to disclose serious personal situations in plenary - invite them to a private discussion after the workshop.
- For the helpline: 116 111 (Save the Children) - used if a real need arises.
- In the role play, do not ask parents to participate if they don't volunteer.

Final message for participants: Online games are part of the child's life. Prohibition will not protect them, but the relationship will. Talk to your child about what they do online, without accusation, with curiosity.

Module 4 - Online Disinformation and Deepfakes (45 min)

↪ Correspondence with Part I: Section 8 (8.1–8.3) - "Online disinformation".

Learning Objectives

- The participant distinguishes between disinformation, fake news and manipulation.
- The participant applies a list of 5 signs to recognise a fake news story.
- The participant knows what a deepfake is and what to do when they encounter one.
- The participant formulates a personal rule: "don't share until you verify".

Materials Needed

- 3 prepared examples: a clearly false story, a true one, one "on the borderline" (neutral - health, "miracle cures").
- 1–2 deepfake examples (or articles explaining a recent one).
- Flipchart with "SIGNS OF FAKE NEWS".
- Cards with terms and definitions for the matching activity.
- Worksheets 1, 2, 3, 4 and 7 from the Workbook (Workshop 2, Module 4).

Workshop Activities

Time	Activity	How it runs	Key message
0–5 min	"True or false?" (Worksheet 1)	3 statements (politically neutral). Participants raise their hand TRUE/FALSE and complete Worksheet 1. Examples: "A medicine cures all diseases" → FALSE; "Shocking headlines can be a sign of fake news" → TRUE; "If information appears on a single website, it is correct" → FALSE. Debrief: "How did you decide?"	-
5–10 min	Quick concepts (Worksheet 2)	Disinformation = the spread of false or misleading information. Fake news = false news presented as true. Manipulation = presentation that influences how people think (part of the	-

		truth, exaggeration, repetition, emotions). "Match the definition" activity on Worksheet 2.	
10–20 min	"News detectives" (Worksheet 3)	In groups of 3, analysis of an example (e.g.: "Doctors don't want you to know this! One ingredient cures everything!"). 5 signs: who published it? are there sources/evidence? is the title exaggerated? does the information seem realistic? does it appear on other credible websites? Debrief on the flipchart.	5 signs help us distinguish.
20–30 min	Verify before sharing + Deepfakes (Worksheet 4)	Scenario: "You receive an alarming message on WhatsApp about a major danger. What do you do?" Groups complete Worksheet 4. Guide (without saying it): check the source; look on other websites; analyse the title; look for evidence; don't share immediately. Then: deepfake = video/audio created by AI, very realistic, showing real people saying things they never said. Rule: at least 2 credible sources. Fact-checking: factual.ro, antifake.eu, eufactcheck.eu.	Verify at least 2 credible sources before sharing.
30–35 min	The 3-Check Rule + 5 Sources	Integrative recap: Who published it? When? Does it also appear on other trusted websites? For important subjects: 5 independent sources. Critical thinking questions: does it seem realistic? who would have an interest? is there evidence?	The same rule works here too.
35–45 min	My personal rule (Worksheet 5)	Each person formulates: "From now on, I will NOT _____ until I _____." Examples: "I will NOT share an alarming message until I search on other websites"; "I will NOT believe a shocking headline until I read the whole article"; "I will NOT share a surprising video until I check it on 2 sources". Plenary: 2–3 volunteers read theirs.	Each of us can stop the spread of false information.

Key Messages of the Module

1. Not everything you see online is true. Checking takes a little time, but it matters a lot.
2. Deepfakes exist and are increasingly realistic - we check with at least 2 credible sources.
3. Each of us can stop the spread of false information.

Trainer Tips

- Use recent examples, but avoid sensitive political or religious news. Choose universal themes (health, "miracle cures").
- Don't mock people who "fall" in the true/false test. The tone remains warm.
- For deepfakes: have a short visual example ready (15–20 sec). Don't go into the theory of generative AI.
- Mention fact-checking sites: factual.ro, antifake.eu, eufactcheck.eu. Say it, don't insist.
- Don't use examples from current Romanian politics - they generate reactions that take you off topic.

Final message for participants: Not everything you see online is true. Checking takes a little time, but it matters a lot. Every person can stop the spread of false information.

Workshop 2 Closing (15 min)

Objectives:

- Summary of both workshops.
- Final personal plan: 1–3 concrete actions for the coming month.
- Feedback and thanks.

Step by step:

- Recap of "4 big ideas" from Workshop 2 (3 min).
- "One thought I take with me" (5 min): each participant says a word or sentence, what they are taking away.
- 30-day personal plan worksheet (3 min): "What will I do in the next 30 days? (max. 3 things)".
- Feedback form - Annex A (3 min).
- Thanks and Annex C (useful resources) printed for each person (1 min).

Final message for participants - Workshop 2: We don't need to be experts to use technology safely. It is enough to pause for a moment, compare, verify, and ask. Thank you for taking these steps with us.

Annex A - Participant Feedback Form

Distribute at the end of each workshop. Anonymous. Maximum 5 minutes to complete.

1. How useful was the session for your everyday life?

1 2 3 4 5 (1 = not very useful; 5 = very useful)

2. What did you like most?

.....
.....

3. What would you have liked to discuss more?

.....
.....

4. One single change you will make at home:

.....

5. Would you recommend this workshop to another parent?

☐ Yes ☐ No Why?

.....

6. Other comment / suggestion:

.....
.....

Annex B - Logistical Checklist for Trainers

One Week Before

- I have read the methodological guide + Part I in full.
- I have prepared 2–3 relevant local examples.
- I have reserved the room (with written confirmation).
- I have sent a reminder message/SMS to participants.

48 Hours Before

- I have checked the room's Wi-Fi connection.
- I have tested the videoconference link for the "Online Meetings" module.
- I have prepared 2 online shops for comparison in the shopping module.
- I have prepared Ghișeul.ro for exploration.
- I have tested an AI tool (ChatGPT/Gemini/Copilot).
- I have printed all worksheets (1 set per participant + 2 spares).
- I have printed Annex A (feedback) and Annex C (resources) for each participant.

On the Day of the Workshop

- I arrive 45 minutes early.
- I arrange the room in a "U" shape or in groups.
- I put on the tables: pens, name badges, folders with worksheets (Part I + Workbook).
- I check projector + sound + lighting.
- I prepare the flipcharts (those pre-written are already covered).
- I put out water + a small welcome platter.
- I check the internet connection again.

After the Workshop

- I collect the feedback forms (anonymous).
- I note 3 things that worked and 1 thing to improve.
- I send a short report (1 page) to the project coordinator within 48 hours.

Annex C - List of Useful Resources for Participants

Distribute at the end of Workshop 2. Maximum 1 A4 page, clearly printed.

Note: this list does not need to be memorised. It should be kept on the fridge or in the documents folder. Refer to it when you have a question.

Topic	Resources
Checking information	Official websites (ministries, local councils). Fact-checking (RO): factual.ro, antifake.eu, eufactcheck.eu. 3-Check Rule: who? when? where else does it appear? For important subjects: 5 independent sources.
Saving and organising files	Google Drive (drive.google.com); Dropbox (dropbox.com); OneDrive (Microsoft). 3-2-1 Rule: 3 copies, 2 different media, 1 in the cloud.
Payments and public services	Romania: Ghişeu.ro - local tax payments; Italy: PagoPA/App IO; Slovenia: eUprava/eDavki; Belgium: MyMinfin/MyGov.be; Poland: obywatel.gov.pl. Romania: ANAF (anaf.ro) - Private Virtual Space. Banking apps (only from App Store / Google Play).
Online meetings	Zoom, Google Meet, Microsoft Teams (downloaded in advance). Checklist: link, device charged, microphone, camera, quiet place, question prepared.
Online shopping	Check: known site, HTTPS, reviews, company details, return conditions. If the price seems too good - it probably is a trap.
Children's games	PEGI (pegi.info) - age ratings. Google Family Link / iOS Screen Time / Microsoft Family Safety - parental controls. Save the Children Helpline: 116 111 (free).
AI tools	ChatGPT (chat.openai.com), Google Gemini (gemini.google.com), Microsoft Copilot. Do NOT share sensitive personal data (ID number, address, medical or financial data). Check with an additional source.
In case of problems	Save the Children Helpline: 116 111. Online fraud: local police + report on the Romanian Police website.

Annex D - Consolidated Worksheets for Participants

General instructions: the worksheets are designed to be completed by participants individually or in pairs / small groups, as instructed by the trainer during the workshops. Each worksheet can be printed as a standalone page to allow selective distribution.

WORKSHOP 1 - Understanding, Searching and Organising

Information

Module 1 - Information Literacy and Types of Content

Worksheet 1 - What do I choose and why?

Instructions: Look at 2–3 examples of online results or headlines (projected by the trainer). Choose what you would open first and answer the questions.

1. Which result would I choose first?

.....

2. Why would I choose this one?

.....

3. What inspires trust in this result?

.....

4. What makes me more careful or uncertain?

.....

5. Would I choose the same if searching for my child? Why?

.....

Worksheet 2 - Search and compare

Instructions: Choose a search topic and compare 2–3 results.

1. What did I search for?

.....

2. What results did I find?

.....

3. Which result seemed most useful?

.....

4. Why did it seem more useful?

.....

5. Which result seemed safer or more credible?

.....

6. What differences did I notice between results?

.....

7. Did I notice any ads or sponsored results?

☐ Yes ☐ No

If yes, what did I notice?

.....

Worksheet 3 - Information, opinion, advertising or hidden advertising?

Instructions: Look at the examples given (projected by the trainer) and try to identify the type of message.

Example 1

This is: ☐ information ☐ opinion ☐ advertising ☐ hidden advertising

Why do I think this?

.....

Example 2

This is: ☐ information ☐ opinion ☐ advertising ☐ hidden advertising

Why do I think this?

.....

Example 3

This is: ☐ information ☐ opinion ☐ advertising ☐ hidden advertising

Why do I think this?

.....

Final question: What elements helped me tell the difference?

.....

Worksheet 4 - I verify information (The 3-Check Rule)

Instructions: Choose an example of online information (discussed in the group) and apply the 3-Check Rule.

1. Who published this information?

.....

2. Is it a known or official source?

.....

3. When was it published?

.....

4. Is the information up to date?

.....

5. Do I find it on other sources too?

.....

6. Would I trust it enough to share it? Why?

.....

Reflection Worksheet M1 - What will I do differently?

Instructions: Think about what you discussed in the workshop and note one concrete thing you want to change.

1. What did I learn today?

.....

2. What will I check more carefully next time I search for something online?

.....

3. What question will I ask myself before believing or sharing something?

.....

4. One concrete thing I will do differently:

.....

Module 2 - Information Searching and AI Tools

Worksheet 1 - General search vs. clear search

Instructions: Compare two searches: a general one and a more specific one (exemplified by the trainer).

1. First search (general):

.....

2. Second search (clearer):

.....

3. What details were added?

.....

4. Which results seemed more useful?

.....

5. Why?

.....

6. What did you learn from this comparison?

Worksheet 2 - Compare 2 results from the same search

Instructions: Choose two results from the same search and compare them.

Result 1: What site is it? / What does it offer? / Does it seem useful? Why?

.....

Result 2: What site is it? / What does it offer? / Does it seem useful? Why?

.....

Final question: Which would you choose and why?

Worksheet 3 - I notice ads or sponsored results

Instructions: Look at a search results page (projected by the trainer) and try to notice the differences between result types.

1. Did I notice a sponsored result / advertisement? ☐ Yes ☐ No

2. How did I tell?

.....

3. What difference do I notice between a sponsored result and an ordinary one?

.....

4. Would I click on the ad? Why / why not?

.....

Worksheet 4 - I search better (The 4-Step Rule)

Instructions: Apply the 4-Step Rule to a real search.

Step 1 - I start simply: What am I looking for initially?

Step 2 - I add details: What can I add? ☐ age ☐ place ☐ purpose ☐ time ☐ other detail:

New search formulation:

Step 3 - I compare results: Which two results am I comparing?

Step 4 - I observe what I choose: What do I choose and why?

Final question: What will I do differently next time I search for something online?

Reflection Worksheet M2 - What will I do differently in my searches?

Instructions: Think about the way you search for information online and note one concrete change.

1. What did I learn today?

.....

2. What mistake do I make most often when searching online?

.....

3. What details will I try to add next time?

.....

4. What will I check before choosing a result?

.....

5. One concrete thing I will do differently:

.....

Module 3 - Saving and Organising Information

Worksheet 1 - "Order from chaos" (renaming files)

Instructions: You have the following file names. Rename them correctly using the formula [Type]_[Content]_[Date] or a clear variant.

Old name	New name
Document1	
Final	
IMG_2023	
New_photo	
Contract	
Final_final2	
Scan	

Reflection: What naming rule will I use from now on?

.....

Worksheet 2 - How do I store files?

Instructions: For each type of file, choose the storage method(s) you would use.

Type of file	Method(s) I would use	Why?
Family photos		
Work documents		
Long-term archive		
Files I need on multiple devices		

Question: Have I applied the 3-2-1 Rule? ☐ Yes ☐ No ☐ Partially

What would I change?

.....

Reflection Worksheet M3 - What will I do differently with my files?

1. What did I learn today?

.....

2. What is the biggest problem with my current file system?

.....

3. One concrete thing I will do differently:

.....

Module 4 - Useful Apps in Everyday Life

Useful Apps Worksheet

Instructions: For each category, write an app you already use or one you would like to try.

Category	App I already use	App I'd like to try
Organisation / productivity		
Navigation / transport		
Payments / public services		

At the Counter vs. Online Comparative Worksheet

Instructions: Compare the two options on 6 criteria.

Criterion	At the counter	Online
Time		
Travel required		
Schedule (hours)		
Comfort		
Stress level		
Feeling of control		

Conclusion: For which types of tasks would I prefer online?

.....

Worksheet for Workshop 2 - Online Services, Children's Safety and Critical Thinking

Module 1 - Participating in Online Meetings

Worksheet 1 - Starting situation

Instructions: Read the situation presented by the trainer and answer the questions.

1. What would I do first?

.....

2. What worries me most?

.....

3. What do I already know about online meetings?

.....

Worksheet 2 - Steps for joining an online meeting

Instructions: Tick the steps you feel confident about and mark with ? the ones where you need more help.

☐ I find the meeting link

☐ I click on the link

☐ I enter my name

☐ I check the microphone

☐ I check the camera

☐ I join the meeting

1. Which step seems easiest to me?

.....
2. Which step seems most difficult?

.....
3. What would I like to practise?
.....

Worksheet 3 - Common problems

Instructions: Think about problems that may arise and note what you would do.

1. If there is no sound, what would I check?
.....

2. If the camera doesn't work, what would I do?
.....

3. If the link doesn't open, what would I try?
.....

4. If the internet connection is weak, what could I do?
.....

5. When would I ask for help?
.....

Worksheet 4 - Before the online meeting (Checklist)

Instructions: Use this checklist before joining an online meeting.

☐ I have the meeting link

☐ My device is charged

☐ I know where to click to join

☐ The microphone works

☐ The camera works

☐ I am in a quiet place

☐ I know what question I want to ask

1. What do I usually remember to check before a meeting?

.....

2. What do I most often forget to check?

.....

3. What will I do differently next time?

.....

Module 2 - Safe Online Shopping

Worksheet 1 - Would I buy or not?

Instructions: Look at the examples presented by the trainer and answer the questions.

1. From which offer / website would I buy?

.....

2. Why would I choose this website?

.....

3. What makes me trust it?

.....

4. What makes me more cautious or less trusting?

.....

5. Would I recommend this website to someone else? Why?

.....

Worksheet 2 - Comparing two websites

Instructions: Choose two websites or two offers and compare them.

Website / Offer 1

Price:

Delivery conditions:

Return policy:

Reviews:

Company details:

Website security (HTTPS, padlock):

Website / Offer 2

Price:

Delivery conditions:

Return policy:

Reviews:

Company details:

Website security (HTTPS, padlock):

1. Which website seems safer?

.....

2. Why?

.....

Worksheet 3 - Signs of trust and signs of risk

Instructions: Think of a website or online offer and note what you observe.

Signs of trust: What makes me trust it?

.....

Signs of risk: What makes me more cautious?

.....

Would I continue with the purchase?

☐ Yes ☐ No ☐ Not sure

Why?

.....

Worksheet 4 - Before paying (Checklist)

Instructions: Use this checklist before completing an online purchase.

☐ The website seems known or clear enough

☐ The price seems realistic

☐ Reviews exist

☐ The delivery conditions are clear

☐ There is a return option

☐ Company details are visible

☐ The website is secured (HTTPS)

☐ No unnecessary personal data is being requested

1. What do I usually check before buying?

.....

2. What do I most often forget to check?

.....

3. What will I do differently next time?

.....

Module 3 - Online Games, Betting and Children's Safety

Worksheet 1 - What do I know about my child's games?

Instructions: Complete the table below with the information you know about your child's games.

Question	Answer
What online games does my child most often play?	
On what device do they play? (phone, tablet, PC, console)	
Who do they usually play with? (friends, classmates, strangers)	
How much time do they spend on games in a day?	
Do I know if the games allow chat or discussions with other people?	

Worksheet 2 - I talk with my child about games

Instructions: Tick the questions you have already asked your child and those you would like to discuss in the future.

☐ What games do you like most?

☐ Who do you usually play with?

☐ Have you ever talked to strangers in games?

☐ What do you do if someone insults you or upsets you in a game?

☐ Have you ever seen dangerous challenges or games online?

Which question would you like to ask this very week?

.....

Worksheet 3 - Signs I should be aware of

Instructions: Tick the signs you have sometimes noticed in your child.

☐ The child hides what they are doing on the phone or computer

☐ They quickly close apps when a parent enters the room

☐ They stay online very late at night

☐ They become irritable when interrupted during a game

☐ They become more withdrawn or more anxious

☐ Unexplained small cuts or bruises appear

Reflection: What behavioural change would make me want to talk more carefully with my child?

.....

Worksheet 4 - Family rules for online games and betting

Instructions: Think of 3 simple rules you could establish in your family.

Rule 1:

.....

Rule 2:

.....

Rule 3:

.....

Reflection: How can you discuss these rules with your child so they are more easily accepted?

.....

What phrase would you use to open the discussion about games / betting with your child?

.....

Worksheet 5 - One single thing I will do differently (M3)

Instructions: After this workshop, think of one single concrete step you will take at home.

Possible examples: I will ask my child what games they play this week. I will install parental controls today. I will look at the PEGI ratings with my child.

The step I will take:

.....

Module 4 - Online Disinformation and Deepfakes

Worksheet 1 - True or false?

Instructions: Read the statements and tick the correct answer.

Statement	True	False	Why do I think this?
"A medicine cures all diseases."	☐	☐	
"Not everything that appears on the internet is true."	☐	☐	
"If information appears on a single website, it is correct."	☐	☐	
"Shocking headlines can be a sign of fake news."	☐	☐	

Reflection: What makes you trust information?

.....

Worksheet 2 - Match the concepts

Instructions: Match the terms with the correct definitions.

Terms: Disinformation / Fake news / Manipulation

Definitions:

- ☐ Presenting information in a way that influences how people think.
- ☐ The spread of false or misleading information.
- ☐ False news presented as true.

Worksheet 3 - News detective

Instructions: Read the story (projected by the trainer) and analyse it.

Example: "Authorities are hiding a secret! A common ingredient cures all diseases, but doctors don't want you to know this!"

- ✓ Who published this information?
- ✓ Are there sources or evidence?
- ✓ Is the headline exaggerated or emotional?
- ✓ Does the information seem realistic?
- ✓ Have you seen this story on other sources too?

Conclusion: This story is: ☐ Credible ☐ Suspicious

Why?

.....

Worksheet 4 - Verify before sharing

Instructions: Situation: You have received an alarming message on your phone about a major danger. Answer:

1. What do you do first?

.....

2. How do you verify the information?

.....

3. Where do you look for confirmation?

.....

4. Do you share the message? ☐ Yes ☐ No

5. Why?

.....

Worksheet 5 - Signs of fake news

Instructions: Tick the signs that indicate a fake news story.

☐ Very shocking headline

☐ Clear and verified sources

☐ Claims without evidence

☐ Emotional language (fear, anger)

☐ Unknown author

☐ Information appears on multiple credible websites

☐ Many grammatical errors

Note: tick only the signs that indicate a fake news story, not those that indicate a credible story.

Worksheet 6 - Critical thinking

Instructions: Answer the questions.

1. Does this information seem realistic?

.....

2. Who might benefit from spreading it?

.....
3. Is there clear evidence?

.....
4. Why was it published?
.....

Worksheet 5 - My personal rule

Instructions: Complete the following:

After this workshop, my rule is: "I will NOTuntil I....."

.....

CHAPTER II

Workshop 1

Module 1. Let's Talk Online! (45 min)

Related Chapter	Section 1: Effective Communication in the Online Environment
Duration	50 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, whiteboard/flipchart, markers, scenario cards
Group Size	10-20 participants
Handouts	Worksheet 1 from the Parent Worksheets Booklet

Objectives

- Understand synchronous vs. asynchronous communication
- Choose the right digital tool for different situations
- Practice basic netiquette (online communication etiquette)
- Gain confidence communicating with schools and institutions online

Session Plan

Time	Activity	Method	Materials
0:00-0:08	Icebreaker: "The Last Message I Sent"	Group circle	None
0:08-0:18	Mini-lesson: How We Communicate Online	Presentation + Q&A	Projector
0:18-0:30	Group Activity: "Which Tool Would You Use?"	Team game	Scenario cards
0:30-0:42	Hands-on: Writing a Good Message	Individual + pairs	Smartphones

0:42-0:48	Role-play: The Misunderstanding	Small groups	Role-play cards
0:48-0:50	 Handout + Wrap-up	Individual	Worksheet 1

Detailed Activity Guide

Icebreaker: “The Last Message I Sent” (8 min)

Trainer Note

Fast-paced and fun. Shows everyone already communicates online. Keep it to 30 seconds per person.

You can find a funny video about the miscommunication example as an icebreaker.

1. Everyone opens their phone and finds the last message they sent.
2. Going around, each person shares: WHO they sent it to, WHAT it was about, and WHICH app they used.
3. After everyone shares: “Did anyone use the same app? Same type of message?”
4. Conclude: “We all communicate online every day. Today we’ll learn to do it even better.”

Group Activity: “Which Tool Would You Use?” (12 min)

Trainer Note

Read scenarios aloud. Teams of 3-4 discuss the best tool. No single correct answer - the goal is to think about WHY.

Scenarios:

1. Tell the teacher your child will be absent tomorrow.
2. Send a birthday photo to your parents in another country.
3. Complain about a wrong delivery from an online store.
4. Explain something complicated to a friend.
5. Organize a meeting with other parents for a school event.
6. You received a suspicious message from a stranger.

Hands-on: Writing a Good Message (12 min)

Trainer Note

Walk around and help. Encourage pairs to give feedback.

Part A - Fix the Bad Message (5 min)

Show on screen:

"HEY!!! WHERE IS THE HOMEWORK??? MY KID DOESNT HAVE IT. YOU NEED TO SEND IT NOW!!!!"

Discuss what's wrong (all caps, demanding, no greeting). Each participant rewrites it on their phone.

Part B - Write Your Own (7 min)

Write an email to your child's school asking about the next parent-teacher meeting. Include a subject line.

Work individually, then share with a partner.

Role-play: The Misunderstanding (6 min)

Trainer Note

Quick! Pick 1-2 scenarios. Groups prepare a 1-minute role-play showing the misunderstanding, then the better version.

- Scenario A: A parent sends "OK." to the class group. Others think they're angry.
- Scenario B: A parent shares a photo of all children at a school party publicly without permission.
- Scenario C: A parent sends a voice message at 11 PM asking about tomorrow's schedule.

Handout + Wrap-up (2 min)

Distribute Worksheet 1. Ask participants to fill in "My 3 personal rules" and "One thing I learned."

Module 2. Social Media: Friend or Enemy? (45 min)

Related Chapter	Section 2: Social Networks - What They Are, How They Work (2.1-2.3)
Duration	50 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, flipchart, markers
Group Size	10-20 participants
Handouts	Worksheet 2 from the Parent Worksheets Booklet

Objectives

- Understand what social networks are and how they differ from each other
- Discover how algorithms shape what they see online
- Experience the “filter bubble” firsthand
- Learn to actively manage their feed instead of passively consuming

Session Plan

Time	Activity	Method	Materials
0:00-0:08	Icebreaker: “Guess the App”	Quiz game	Projector
0:08-0:20	Mini-lesson: How Social Media Really Works	Presentation + demo	Projector
0:20-0:32	The Algorithm Experiment	Pairs on phones	Smartphones
0:32-0:42	Hands-on: Reset Your Feed	Individual on phones	Smartphones
0:42-0:48	Discussion: Passive Scrolling vs. Active Connection	Group	None

0:48-0:50	 Handout + Wrap-up	Individual	Worksheet 2
0:50-0:55	Interactive Game: “True or Fake?”	Full group game	Projector/cards

Detailed Activity Guide

Icebreaker: “Guess the App” (8 min)

Trainer Note

Fast quiz. Round 1: show app icons without names. Round 2: read descriptions. Make it competitive.

Round 1 - Show icons: Facebook, Instagram, TikTok, WhatsApp, YouTube, LinkedIn, Snapchat, X, Telegram, Discord, Signal, BeReal., Viber, Twitch, Kick, Pinterest

Round 2 - Read descriptions:

- “A platform where videos disappear after 24 hours” (Snapchat/Instagram Stories)
- “A platform where you can watch cooking videos for 3 hours without realizing it” (TikTok/YouTube)
- “A platform your boss might check before hiring you” (LinkedIn)
- “The app that replaced your family phone tree” (WhatsApp)

The Algorithm Experiment (12 min)

Trainer Note

Powerful eye-opener. Participants see that two people on the same app see completely different content.

1. Pair up with someone you don’t know well.
2. Both open the same app (Instagram Explore, TikTok For You, or YouTube home).
3. Hold up your phones. Compare: is your feed the same or different?

4. Discuss in pairs: Why do you think they're different?
5. Group share: "Who had a completely different feed from their partner?" (almost everyone)
6. Explain: "This is the algorithm. It learns what you like and shows you more. That's why scrolling feels endless and you can end up in a 'bubble.'"

Hands-on: Reset Your Feed (10 min)

Trainer Note

Practical steps they can do RIGHT NOW. Walk through on projector, they follow on phones.

1. Open your main social media app.
2. Find a post you don't like → tap the three dots (...) → select "Not Interested" or "Hide."
3. Find an account you followed but whose content annoys you → Mute or Unfollow.
4. Actively like and comment on 2-3 posts you genuinely enjoy - this trains the algorithm.
5. Check: are there any accounts you follow that you don't remember following? Unfollow them.

Discussion: Passive Scrolling vs. Active Connection (6 min)

Ask: "What's the difference between scrolling for 30 minutes and actually talking to someone online for 30 minutes?"

Key insight: Passive consumption (scrolling, watching) tends to make us feel worse. Active engagement (messaging, commenting, creating) tends to make us feel better.

Challenge: "This week, try replacing 15 minutes of scrolling with one meaningful message to someone you care about."

Handout + Wrap-up (2 min)

Distribute Worksheet 2. Participants fill in their app inventory and feed changes they made.

Interactive Game: "True or Fake?" (12 min)

https://ec.europa.eu/programmes/erasmus-plus/project-result-content/ee766887-db5d-4976-af9c-df990987fdbc/FAKE%20OFF!%20Examples%20News_EN.pdf



Trainer Note

*Show 6-8 claims on screen. Participants vote TRUE or FAKE (hand raise or colored sticky notes).
Reveal and explain each. Adapt claims to your local context.*

Module 3. Protect Yourself Online (45 min)

Related Chapter	Section 2.4: Risks and Challenges of Social Networks
Duration	55 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, printed fake post cards (6-8), sticky notes (green + red), flipchart, markers
Group Size	10-20 participants
Handouts	Worksheet 3 from the Parent Worksheets Booklet

Objectives

- Complete a thorough privacy audit on their own phones
- Apply the fact-checking method to real social media posts
- Recognize the “highlight reel” effect and develop strategies against comparison
- Create a personal online safety action plan

Session Plan

Time	Activity	Method	Materials
0:00-0:07	Icebreaker: “Two Truths and a Lie - Online Edition”	Full group	None
0:07-0:20	Hands-on: The Full Privacy Audit	Individual on phones	Smartphones
0:20-0:35	Game: “Fake Post Detectives”	Small groups	Printed cards
0:35-0:47	Discussion + Exercise: The Comparison Trap	Group + individual	Sticky notes

0:47-0:52	 Handout + Wrap-up	Individual	Worksheet 3
-----------	---	------------	-------------

Detailed Activity Guide

Icebreaker: “Two Truths and a Lie - Online Edition” (7 min)

Trainer Note

Each person says three things about their digital life - two true, one false. Others guess the lie.

1. Each person thinks of 3 statements about their digital life: 2 true, 1 false.
2. Examples: “I have 500+ Facebook friends” / “I once fell for a WhatsApp scam” / “I check Instagram before brushing my teeth.”
3. Go around: share statements. Others vote on the lie.
4. Quick debrief: “Were you surprised by anyone’s truths?”

Hands-on: The Full Privacy Audit (13 min)

Trainer Note

More thorough than a quick check. Walk through ALL steps on projector. Go slowly.

Phase 1 - Profile visibility (5 min)

1. Open your main social media app. Go to your profile.
2. Use “View As” / “View Public Profile” to see what strangers see.
3. Check: phone number, email, birthday, workplace, address visible?
4. Remove or hide anything you don’t want strangers to see.

Phase 2 - Connected apps (4 min)

1. Go to Settings → Apps and Websites (Facebook) or Security → Apps (Instagram).
2. Do you recognize all these apps?
3. Remove any you don’t recognize or no longer use.

Phase 3 - Location and tagging (4 min)

1. Check: Is location sharing enabled for social media apps? Turn it off unless necessary.
2. Which apps have access to your photos and messages? Turn it off unless necessary.
3. Enable “Review tags before they appear on your profile.”

Game: “Fake Post Detectives” (15 min)

Trainer Note

Prepare 6-8 printed cards with fake/real posts. Teams sort into REAL/FAKE piles. They can use phones to fact-check.

Sample cards (adapt locally):

- Card 1: “[Local supermarket] is giving away €500 gift cards to everyone who shares this!” (FAKE)
- Card 2: News article about new EU digital safety regulation (TRUE)
- Card 3: “Doctors don’t want you to know: this ingredient cures headaches instantly!” (FAKE)
- Card 4: Dramatic weather photo with wrong location caption (FAKE)
- Card 5: Official school announcement about schedule change (TRUE)
- Card 6: “WhatsApp will charge €0.99/month unless you forward this” (FAKE)

After the game, teach the 3-second rule: 1) Who wrote this? 2) Can I verify it? 3) Am I sharing because of emotion?

The Comparison Trap (12 min)

Trainer Note

Start with short discussion, then sticky note exercise. Be sensitive.

Discussion (4 min):

Ask: “Have you ever seen something on social media that made you feel bad about yourself or your family?” Explain the “highlight reel” concept.

Sticky note exercise (8 min):

1. Give everyone a green and a red sticky note.
2. GREEN: one account/content that makes you feel GOOD.
3. RED: one account/content that makes you feel BAD.
4. Stick on flipchart in two columns. Read some aloud.
5. Key takeaway: “You control your feed. Unfollow the red. Follow more green.”

Handout + Wrap-up (5 min)

Distribute Worksheet 3. Participants fill in audit results and feed detox plan.

Module 4: Your Online Identity (45 min)

Related Chapter	Section 3: Social Media Profiles
Duration	55 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, paper and colored pencils, flipchart
Group Size	10-20 participants
Handouts	Worksheet 4 from the Parent Worksheets Booklet

Objectives

- Understand what their social media profile reveals about them
- Review and improve their own profile on the spot
- Recognize fake accounts and impersonation
- Understand Two-Factor Authentication and set it up

Session Plan

Time	Activity	Method	Materials
0:00-0:08	Icebreaker: “Who Am I Online?”	Drawing activity	Paper, pencils
0:08-0:18	Mini-lesson: Your Profile = Your First Impression	Presentation	Projector
0:18-0:30	Hands-on: Profile Review on Your Phone	Individual	Smartphones
0:30-0:38	Game: “Spot the Fake Account”	Full group	Projector
0:38-0:48	Hands-on: Setting Up Two-Factor Authentication	Individual	Smartphones

0:48-0:52	 Handout + Wrap-up	Individual	Worksheet 4
-----------	---	------------	-------------

Detailed Activity Guide

Icebreaker: “Who Am I Online?” (8 min)

Trainer Note

Fun, no tech needed. Participants draw their “online self” in stick figures/shapes/words.

1. Give everyone paper and colored pencils.
2. Ask: “If someone only knew you from social media, what would they think you’re like? Draw it!”
3. 4-5 minutes to draw.
4. Each person holds up their drawing, explains in 20 seconds.
5. Ask: “Is your online self the same as your real self? What’s different?”

Hands-on: Profile Review (12 min)

Trainer Note

Display checklist on projector. Walk through together. Give time to make real changes.

Profile review checklist:

- ☐ What photo do you use? Does it reveal anything private?
- ☐ Read your bio. Information strangers shouldn’t see?
- ☐ Check posts from the last month. Comfortable if a stranger saw them?
- ☐ Check friends/followers. Anyone you don’t actually know?
- ☐ Is your profile Public or Private?

If anything needs changing - change it now!

Game: “Spot the Fake Account” (8 min)

Trainer Note

Show 5-6 screenshots of profiles on the projector (a mix of real and fake/bot accounts). Participants vote: REAL or FAKE. Discuss the clues.

Clues to teach:

- Stock photo or no photo = suspicious
- Username with random numbers (e.g., jane_smith89457) = suspicious
- Very few posts but following thousands = suspicious
- Generic comments like “Great post!” on every post = likely a bot
- No personal information that can be verified = suspicious

Rule: “If you’re not sure, don’t accept. Verify through another channel.”

Hands-on: Two-Factor Authentication (10 min)

Trainer Note

Live demo on projector. This is the single most effective security measure. Go slowly - many parents have never done this.

General steps (works for most platforms):

1. Open your social media app → Settings → Security / Privacy.
2. Find “Two-Factor Authentication” or “2-Step Verification.”
3. Choose a method: Text message (SMS) or Authenticator app.
4. Follow the setup prompts. The platform will send a code to verify.
5. SAVE your backup codes somewhere safe (screenshot or write down).
6. Test: log out and log back in - you should be asked for a code.

Explain: “Even if someone steals your password, they can’t get in without the code on YOUR phone.”

Handout + Wrap-up (4 min)

Distribute Worksheet 4. Participants tick the changes they made and their 2FA status.

Workshop 2

Module 1. Your Digital Shadow (45 min)

Related Chapter	Section 4: Digital Footprint
Duration	50 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, flipchart, markers, paper
Group Size	10-20 participants
Handouts	Worksheet 5 from the Parent Worksheets Booklet

Objectives

- Understand what a digital footprint is (active vs. passive)
- Discover what the internet “knows” about them by searching their own name
- Reflect critically on “sharenting” and how they share their children’s information
- Learn how to audit and clean up their digital presence

Session Plan

Time	Activity	Method	Materials
0:00-0:07	Icebreaker: “What Does Google Know About You?”	Individual prediction	Paper
0:07-0:15	Mini-lesson: Active vs. Passive Footprint	Presentation	Projector
0:15-0:28	Group Activity: “Google Yourself”	Pairs on phones	Smartphones
0:28-0:40	Discussion: Sharenting - Is It Safe to Share?	Group circle	Projector (stock photos)

0:40-0:48	Hands-on: The Digital Cleanup	Individual on phones	Smartphones
0:48-0:50	 Handout + Wrap-up	Individual	Worksheet 5

Detailed Activity Guide

Icebreaker: “What Does Google Know About You?” (7 min)

Trainer Note

Creates curiosity. Before they actually Google themselves, ask them to PREDICT what they’ll find.

1. Give everyone a small piece of paper.
2. Ask: “If you Googled your full name right now, what do you think you’d find? Write your prediction: a lot / a little / nothing.”
3. Collect predictions on the flipchart: how many said “a lot” vs. “nothing”?
4. Say: “Let’s find out. We’ll Google ourselves in a moment.”

Group Activity: “Google Yourself” (13 min)

Trainer Note

Often surprising and memorable. Many have never done this. Pair people up for support.

1. Pair up. Each person opens Google and types their full name.
2. Check: Web results, Images tab, any other results.
3. Discuss with partner: What did you find? Surprised? Anything to remove?
4. Now search your child’s name (if applicable). What comes up?
5. Group share: “Was your prediction correct? How does it feel to see what the internet ‘knows’ about you?”

Explain: “This is your digital footprint. Some of it you created (active). Some of it was collected without you knowing (passive). And some was created by OTHER people (your digital shadow).”

Discussion: Sharenting (12 min)

Trainer Note

Show 3-4 stock photos (NOT real children). For each, ask: “What info does this reveal? Would you post this?” Goal: critical thinking, not guilt.

Example photos to discuss:

- Photo 1: Child in school uniform in front of school (reveals: school name, child’s appearance, location)
- Photo 2: Birthday cake with child’s name and age (reveals: name, exact age)
- Photo 3: Child playing in a park you visit every Saturday (reveals: routine, regular location)
- Photo 4: Award certificate with full name and school (reveals: name, school, class)

Ask: “How could you share the same proud moment more safely?” (crop school name, blur background, use private group)

Key point: “Your child may one day be embarrassed by photos you posted when they were little. As they get older, ask their permission.”

Hands-on: The Digital Cleanup (8 min)

Trainer Note

Quick practical session. Participants take action on their phones RIGHT NOW.

1. Go to your social media profile. Use “View As” to see what’s public.
2. Scroll through your old posts from the last 6 months. Anything you want to delete or hide?
3. Check Settings → Apps and Websites. Remove any connected apps you don’t use.
4. Enable “Tag review” so you approve tags before they appear on your profile.
5. Check: is your profile set to Private? If not, consider changing it now.

Handout + Wrap-up (2 min)

Distribute Worksheet 5. Highlight the Family Challenge: “This week, search your child’s name on Google and ask them: Is there anything I posted about you that you’d like me to remove?”

Module 2. Breaking the Scroll (45 min)

Related Chapter	Section 5: Social Media Addiction
Duration	60 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, large paper + markers, timer, small cards
Group Size	10-20 participants
Handouts	Worksheet 6 from the Parent Worksheets Booklet

Objectives

- Understand the psychology behind social media addiction (dopamine, FOMO, variable rewards)
- Honestly assess their own and their children's screen time habits
- Distinguish between a strong habit and a dependency
- Develop a concrete personal action plan for healthier screen use

Session Plan

Time	Activity	Method	Materials
0:00-0:08	Icebreaker: "The Scroll Timer"	Individual + group	Smartphones, timer
0:08-0:20	The Big Reveal + Shocking Math	Individual + flipchart	Smartphones, flipchart
0:20-0:32	Interactive Lesson: "Design an Addictive App"	Small groups	Large paper, markers
0:32-0:42	Self-Assessment: Habit or Addiction?	Individual	Small cards

0:42-0:52	Group Brainstorm: “30 Things to Do Instead”	Full group	Flipchart
0:52-1:00	 Handout + Wrap-up	Individual	Worksheet 6

Detailed Activity Guide

Icebreaker: “The Scroll Timer” (8 min)

Trainer Note

Participants experience how social media distorts time perception.

1. Tell everyone: “Open any social media app and start scrolling. I’ll tell you when to stop.”
2. Start a timer but DON’T show it.
3. After exactly 3 minutes: “STOP!”
4. Ask: “How long was that? Raise hand: 1 minute? 2 minutes? 3? 5?”
5. Reveal: “Exactly 3 minutes. Most of you thought it was shorter. This is how social media distorts time.”

The Big Reveal + Shocking Math (12 min)

Trainer Note

Most impactful moment. Be sensitive - normalize results.

1. Guide to screen time: iPhone: Settings → Screen Time. Android: Settings → Digital Wellbeing.
2. Each person writes: total daily average + #1 app.
3. Go around: share ONLY daily average (keep it comfortable).
4. Calculate group average on flipchart.
5. The math: “ $2.5 \text{ hours/day} \times 365 = 912 \text{ hours/year} = 38 \text{ FULL DAYS}$. More than a month of your life!”

6. Ask: “What could you do with one extra month per year?”

“Design an Addictive App” (12 min)

Trainer Note

Creative and energetic. Once they design it, they’ll never look at their apps the same way.

1. Groups of 3-4, large paper + markers.
2. Brief: “Design an app that keeps people scrolling FOREVER. What features?”
3. 8 minutes to draw and list features.
4. Each group presents their “evil app.”
5. Reveal: “Every feature you designed already exists! Infinite scrolling, notifications, likes, autoplay - all designed to hook you.”

Self-Assessment: Habit or Addiction? (10 min)

Trainer Note

Private exercise. No one shares results unless they want to. The goal is honest self-reflection.

Read 6 statements aloud. Participants write YES/NO on a small card:

1. “I check my phone first thing in the morning, before getting out of bed.”
2. “I feel anxious when I can’t access social media.”
3. “I often spend more time on social media than I intended.”
4. “I’ve neglected something important because of scrolling.”
5. “I use social media to cope when I’m bored, stressed, or lonely.”
6. “I’ve tried to reduce my screen time but couldn’t stick to it.”

Scoring: 0-1 = healthy. 2-3 = strong habit. 4-6 = may be affecting well-being. No judgment - awareness is the first step.

“30 Things to Do Instead” (10 min)

Trainer Note

Positive energy. Shifts from “what to stop” to “what to start.” Go fast - shout out ideas!

Challenge: “Let’s come up with 30 things to do instead of scrolling!” Write on flipchart. Try to hit 30 in 5 minutes. Each person circles their top 3.

Handout + Wrap-up (8 min)

Distribute Worksheet 6. Fill in screen time data, self-assessment score, and 3 alternatives.

Close: “Social media isn’t evil. But it IS designed to take more time than you realize. Now you know the tricks, you’ve seen your numbers, and you have a plan.”

Module 3. The Digital Parent Toolkit (45 min)

Related Chapter	Section 6: Digital Parenting - Guiding Your Child's Online Life
Duration	60 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, smartphones, large paper for Agreement draft, markers, role-play scenario cards
Group Size	10-20 participants
Handouts	Worksheet 7 from the Parent Worksheets Booklet

Objectives

- Understand the key principles of effective digital parenting (communication > control)
- Practice calm, supportive responses to children's online problems
- Set up parental controls on their own devices
- Draft a Family Media Agreement to finalize at home

Session Plan

Time	Activity	Method	Materials
0:00-0:08	Icebreaker: "What Did You Do Online at Age 12?"	Group circle	None
0:08-0:18	Mini-lesson: The 3 Pillars of Digital Parenting	Presentation	Projector
0:18-0:30	Role-play: "Mom/Dad, Something Happened Online"	Pairs	Scenario cards
0:30-0:42	Hands-on: Setting Up Parental Controls	Individual	Smartphones

0:42-0:55	 Handout: Family Media Agreement + Discussion	Individual + group	Worksheet 7
0:55-1:00	Closing: The One Sentence That Matters	Group	None

Detailed Activity Guide

Icebreaker: “What Did You Do Online at Age 12?” (8 min)

Trainer Note

Creates perspective and empathy. Most parents either didn’t have internet at 12 or had very different experiences.

1. Ask: “Think back to age 12. Did you have internet? A phone? What did you do online?”
2. Go around: each person shares in 20-30 seconds.
3. Then: “Now think about YOUR child at 12. What are they doing online?”
4. Bridge: “The world has changed completely. That’s why we’re here.”

Mini-lesson: The 3 Pillars (10 min)

Trainer Note

Draw 3 columns on flipchart. Keep it visual and conversational.

Pillar 1: COMMUNICATE

- Talk regularly about digital life - not just when something goes wrong.
- Be curious, not judgmental. Ask: “What did you see online today?”
- Share your OWN struggles with technology. Model vulnerability.

Pillar 2: COLLABORATE

- Set rules TOGETHER. Children follow rules they helped create.
- Create a Family Media Agreement as a family project.
- Review and adjust rules together every few months.

Pillar 3: PROTECT

- Use parental controls as a safety net, not a substitute for communication.
- Teach the “Tell Me First” rule: if anything scary happens online, come to me. No punishment for telling.
- Know what apps your children use. Ask them to show you.

Role-play: “Mom/Dad, Something Happened” (12 min)

Trainer Note

Most important skill in this workshop: HOW parents react. Practice the LISTEN → THANK → SAVE → SOLVE method.

Scenarios (pairs - one plays child, one parent, then switch):

- A: “Mom, someone in my class group chat is saying mean things about me.”
- B: “Dad, I accidentally clicked a link and weird pop-ups keep appearing.”
- C: “Mom, a person I don’t know sent me a message saying I’m pretty and asking for my photo.”
- D: “Dad, my friend showed me a really scary video and I can’t stop thinking about it.”
- E: “Mom, I created a TikTok account without telling you. I’m sorry.”

After each, debrief:

- How did the “child” feel about the reaction?
- Did the parent stay calm? Listen first?
- Would the child come back next time?

Key: “Your first 10 seconds determine whether your child comes to you next time. Always: LISTEN → THANK → SOLVE.”

Hands-on: Parental Controls (12 min)

Trainer Note

Live demo on projector. Cover the two most common systems.

Android (Google Family Link):

1. Open Google Family Link app.
2. Add child's Google account.
3. Set daily screen time limits.
4. Enable content filters and app approval.
5. Turn on location sharing (discuss with child).

Apple (Screen Time):

1. Settings → Screen Time → Set Up for Family.
2. Set Downtime hours (e.g., 9 PM - 7 AM).
3. Set App Limits for categories (Social, Games).
4. Enable Content & Privacy Restrictions.

Remind: "Parental controls are a safety net, not a cage. Always explain WHY."

Handout + Discussion (13 min)

Distribute Worksheet 7 (Family Media Agreement template). Walk through on projector. Give 8 minutes to fill in draft.

Quick share (5 min): 2-3 volunteers: "What's one rule in your agreement? What was hardest to decide?"

Closing: The One Sentence That Matters (5 min)

Everyone completes: "The most important thing I want my child to know about coming to me with online problems is: _____"

2-3 share aloud. Close: "No filter, no app, no rule will ever be as powerful as your child knowing they can come to you."

Module 4. When the Internet Hurts: Understanding Cyberbullying

(45 min)

Related Chapter	Section 2.4.3: Cyberbullying - Recognition, Response, and Prevention
Duration	60 minutes
Target Group	Parents with low/medium level of education (G2)
Materials	Projector/screen, printed scenario cards, smartphones, flipchart, markers, sticky notes, tissues (for emotional moments)
Group Size	10-20 participants
Handouts	Corresponding worksheet from the Parent Worksheets Booklet (Set 2)

Why This Workshop Matters

Cyberbullying is one of the most serious online risks for children. It can cause lasting psychological harm, and many parents feel helpless when it happens. This workshop equips parents with the knowledge to recognize cyberbullying, the confidence to respond effectively, and the tools to support their child through it.

Objectives

- Understand what cyberbullying is and how it differs from traditional bullying
- Recognize the warning signs that a child is being cyberbullied
- Practice the correct response: Listen → Save evidence → Report → Support
- Know when and how to escalate to schools and authorities
- Learn how to have a conversation with their child about cyberbullying before it happens

Session Plan

Time	Activity	Method	Materials
------	----------	--------	-----------

0:00-0:08	Icebreaker: “Words That Stick”	Individual + group	Sticky notes, pens
0:08-0:20	Interactive Lesson: Cyberbullying 101	Presentation + Q&A	Projector
0:20-0:32	Spot the Signs: “Is My Child Being Cyberbullied?”	Group exercise	Projector/cards
0:32-0:45	Role-play: The Parent Response	Pairs	Scenario cards
0:45-0:52	Hands-on: How to Block, Report, and Save Evidence	Demo on phones	Smartphones, projector
0:52-1:00	 Handout: Family Cyberbullying Action Plan + Wrap-up	Individual	Printed worksheet

Detailed Activity Guide

Icebreaker: “Words That Stick” (8 min)

Trainer Note

Powerful and emotional opener. Sets the tone by showing how hurtful words stay with us - and how much worse it is when those words are online and permanent. Have tissues available. Be prepared for emotional responses.

1. Give everyone a sticky note and a pen.
2. Ask: “Think of a hurtful word or comment someone said to you when you were young. You don’t have to share what it was - just write how OLD you were when you heard it.”
3. Collect the sticky notes on the flipchart. Read the ages aloud: “8... 10... 12... 7... 14...”
4. Say: “You still remember these words, even after all these years. Now imagine your child receiving a hurtful message online - a message that doesn’t go away. That stays on their screen. That can be shared with hundreds of people. That’s cyberbullying.”

Interactive Lesson: Cyberbullying 101 (12 min)

Trainer Note

Keep it conversational. Use the question-answer format to keep parents engaged. Don't lecture - ask them questions and build on their answers.

Key points to cover:

- Definition: Repeated, deliberate use of digital tools to harass, humiliate, or threaten someone.
- Forms: Harassment, public humiliation, exclusion from groups, impersonation, sharing private info, trolling.
- What makes it different from playground bullying: It follows you home. It's 24/7. It can be anonymous. It reaches a huge audience. It's permanent.
- The numbers: Ask "What percentage of teenagers do you think have experienced cyberbullying?" Let them guess. Reveal: roughly 1 in 3 (varies by study/country).
- The silence: Most children don't tell their parents. The #1 reason: they're afraid of losing their phone.

 Spot the Signs: "Is My Child Being Cyberbullied?" (12 min)

 Trainer Note

Show 6 scenarios/descriptions on the projector. For each, parents discuss: could this be cyberbullying? Make it interactive - not a lecture.

Scenarios to discuss (show one at a time):

1. "My 12-year-old suddenly doesn't want to go to school and says she feels sick every morning." - Could it be related to something online? What would you ask?
2. "My son used to love his phone, but now he gets upset every time it buzzes and sometimes hides it under the pillow." - What does this behavior change suggest?
3. "My daughter came home crying after school. Her friends have created a group chat without her and are posting mean comments she can see on other people's phones." - Is this cyberbullying? (Yes: exclusion + visible humiliation)
4. "My child's grades dropped suddenly this semester. They seem distracted and anxious." - Could online issues be a factor?

5. “I noticed my teenager deleted all their social media accounts overnight without explanation.” - What might have happened?
6. “My child tells me everything is fine but seems withdrawn and barely eats dinner.” - Should I push for information or give space?

After all scenarios, summarize the warning signs on the flipchart: behavior changes, mood changes, avoidance of school/friends, secrecy with devices, sleep/appetite changes.

Role-play: The Parent Response (13 min)

Trainer Note

THIS is the most important part of the workshop. Parents practice the response they would give if their child comes to them. The instinctive reaction (anger, panic, taking the phone) is usually wrong. We're training a better reflex.

The method to practice: LISTEN → THANK → SAVE → SOLVE

- LISTEN: Let the child speak. Don't interrupt. Don't react with shock.
- THANK: “Thank you for telling me. I'm proud of you. This is not your fault.”
- SAVE: “Let's take screenshots of everything before we do anything else.”
- SOLVE: “Let's decide together what to do next: block, report, contact school.”

Role-play scenarios (pairs - one plays child, one plays parent, then switch):

- Scenario 1: “Mom, kids in my class are making fun of my photo in a group chat. They added laughing emojis and told everyone not to talk to me.”
- Scenario 2: “Dad, someone created a fake account with my name and is posting embarrassing things. My friends think it's me.”
- Scenario 3: “Mom, a boy in my class keeps sending me mean messages. He says if I tell anyone, it will get worse.”

After each:

Ask the “child”: “How did you feel about the parent's reaction? Would you come back to them next time?”

Hands-on: Block, Report, Save Evidence (7 min)

Trainer Note

Quick practical demo. Show on projector, participants follow on phones. Focus on the TWO most common platforms for children.

Instagram:

1. To block: Go to the person's profile → Tap ... → Block.
2. To report: Tap ... on a post or message → Report → Select reason (Bullying or harassment).
3. To save evidence: Take a screenshot BEFORE blocking (important!).

WhatsApp:

1. To save evidence: Screenshot the messages (including timestamps).
2. To report: Open the contact → Tap the name at top → Scroll down → Report contact.
3. To block: Same screen → Block contact.

Remind: “Always save evidence FIRST, then block and report.”

Handout + Wrap-up (8 min)

Distribute Worksheet 8 (Family Cyberbullying Action Plan). Walk through it briefly. Ask parents to fill in the emergency contact section now.

Closing message:

Say: “Cyberbullying is real, it’s serious, and it can happen to anyone’s child. But now you know how to spot it, how to respond, and most importantly - how to keep the door open so your child will come to you when they need you. That is the most powerful protection any parent can offer.”

Optional: “If your child is currently experiencing cyberbullying and you need support, please speak to me after the session.”

Annex A - Participant Feedback Form

Please complete this brief questionnaire to help us evaluate and improve Workshop 2 (Communication and Collaboration in the Online Environment). Your feedback is anonymous.

Date: _____ **Location:** _____

1. Overall Satisfaction

How would you rate the overall quality of this workshop?

- ☐ Excellent
- ☐ Good
- ☐ Average
- ☐ Poor

2. Relevance of Modules

Please rate how useful you found each module (1 = Not useful, 4 = Very useful):

Module	1	2	3	4
Module 1: Your Digital Shadow (Digital Footprint & Sharenting)	☐	☐	☐	☐
Module 2: Breaking the Scroll (Screen Time & Addiction)	☐	☐	☐	☐
Module 3: The Digital Parent Toolkit (Parental Controls & Agreements)	☐	☐	☐	☐
Module 4: When the Internet Hurts (Cyberbullying & Action Plan)	☐	☐	☐	☐

3. Practical Application

What is the most important change or action you will take at home after today's session?

4. Trainer Assessment

Was the trainer clear, engaging, and supportive during practical activities?

- ☐ Yes, completely
- ☐ Mostly
- ☐ Needs improvement

5. Additional Comments or Suggestions

Annex B - Logistical Checklist for Trainers

This checklist helps trainers prepare all necessary equipment, materials, and digital setups prior to conducting Workshop 2 sessions.

1. Room Setup & AV Equipment

- ☐ Projector and screen with HDMI/USB-C adapters for mobile screen mirroring.
- ☐ Stable Wi-Fi network with credentials clearly displayed on the flipchart.
- ☐ Flipchart stand, 2-3 full pads of flipchart paper, and colorful markers (black, blue, red, green).
- ☐ Flexible seating arrangement (chairs arranged in a semi-circle or small tables for group work).

2. Digital Live Demo Preparation

- ☐ Demonstration smartphone (Android and iOS) prepared with test accounts.
- ☐ Social media apps pre-installed (Instagram, TikTok, WhatsApp) for settings/privacy demos.
- ☐ Screen Time (Apple) and Google Family Link apps configured for live walkthroughs.
- ☐ Sample profile screenshots (5-6 real vs. fake/bot profiles) loaded into the slide deck.

3. Physical Printed Materials & Cards

- ☐ Participant Worksheets Booklet (Worksheets 1 through 8 printed per participant).
- ☐ Printed Role-Play Scenario Cards for Module 3 and Module 4 (cut into sets for pairs).
- ☐ Sticky notes (multiple colors) and ballpoint pens for every participant.
- ☐ Small index cards for the "Habit vs. Addiction" self-assessment exercise.
- ☐ Tissues (placed discretely in the room for emotional moments during cyberbullying discussions).

4. Support & Escalation Information

- ☐ Contact numbers for local child helplines, school counseling services, and cyberbullying reporting centers written on flipchart or printed on handouts.
- ☐ Evaluation / Feedback Forms (Annex A) printed for end-of-workshop distribution.

Annex C - List of Useful Resources for Participants

A curated list of trusted guides, tools, and support services to help parents manage online privacy, screen time, and cyberbullying.

1. Social Media Privacy Guides & Tools

- **Internet Matters Privacy Guides:** Step-by-step guides for setting privacy on Instagram, TikTok, Snapchat, and WhatsApp. (www.internetmatters.org)
- **Family Safety Centers:** Official safety portals for major platforms (meta.com/family, tiktok.com/safety, safety.google/families).
- **Terms of Service; Didn't Read:** Simple summaries of app privacy policies and data sharing practices. (tosdr.org)

2. Digital Footprint & Fact-Checking Resources

- **Google Account Removal Tool:** Request removal of personally identifiable information or photos of minors from Google Search. (support.google.com/websearch/troubleshooting/3111061)
- **TinEye / Google Reverse Image Search:** Tools to verify if photos or profiles are using stolen stock imagery.
- **Snopes & FactCheck.org:** Independent fact-checking websites to verify viral posts, news stories, and online rumors.

3. Screen Time & Digital Wellbeing Apps

- **Google Family Link:** Free parental control tool for managing Android devices, app approvals, and bedtimes.
- **Apple Screen Time:** Built-in iOS feature for setting downtime, app limits, and content restrictions across family devices.
- **Forest / One Sec:** Focus apps designed to break habits of impulse scrolling and reduce screen time.

4. Cyberbullying & Online Safety Helplines

- **Better Internet for Kids (BIK):** Pan-European network of safer internet centers offering helplines and advice. (betterinternetforkids.eu)
- **Cyberbullying Research Center:** Fact sheets, reporting guides, and practical advice for parents and educators. (cyberbullying.org)
- **Take It Down (NCMEC):** Free service to help remove explicit imagery of young people posted online. (takeitdown.ncmec.org)

Annex D - Parent Worksheets for Chapter II

Workshop 1

WORKSHEET 1

My Communication Rules

Name: _____

Date: _____

The communication tools I uses:

App / Tool	I use it for...	How often?

Fix the message!

The trainer showed a “bad” message. Write a better version here:

My email to the school

Write an email asking about the next parent-teacher meeting.

Subject line:

Message:

My 3 personal rules for online communication

Rule 1:

Rule 2:

Rule 3:

 **One thing I learned today:**

WORKSHEET 2

My Social Media Map

Name: _____

Date: _____

My social media apps

App name	Purpose (why I use it)	Hours/day (est.)	Do my children use it?

The Algorithm Experiment

I compared my feed with my partner's feed. What was different?

Feed changes I made today

- ☐ I hid or marked “Not Interested” on unwanted content
- ☐ I muted or unfollowed an account I don’t enjoy
- ☐ I liked/commented on content I genuinely want to see more of
- ☐ I unfollowed accounts I don’t remember following

 **This week, I will replace 15 min of scrolling with:**

WORKSHEET 3

My Online Safety Plan

Name: _____

Date: _____

My Privacy Audit Results

- ☐ Set profile to Private
- ☐ Removed personal info from public view
- ☐ Removed unknown people from friends/followers
- ☐ Removed connected apps I don't recognize
- ☐ Turned off location sharing for social media
- ☐ Enabled tag review
- ☐ Other: _____

Fake Post Detectives – My Results

I got right: _____

The clue that helped me spot fakes:

The 3-Second Rule: Before sharing anything, I will ask:

1. Who wrote this? 2. Can I verify it? 3. Am I sharing because of emotion?

My Feed Detox

Content that makes me feel GOOD (follow MORE):

Content that makes me feel BAD (unfollow/mute):

 **My 3 online safety commitments:**

1.

2.

3.

My Profile Check-Up

Name: _____

Date: _____

My “Who Am I Online?” Drawing

(Stick your drawing here or describe it)

Profile review results

- ☐ Changed profile photo to something more private
- ☐ Removed personal information from bio
- ☐ Set profile to Private
- ☐ Removed unknown people from friends/followers
- ☐ Reviewed posts from last month

Fake Account Detection – What I Learned

Red flags of a fake account:

Two-Factor Authentication

☐ I set up 2FA on my main social media account

☐ I saved my backup codes

The platform I set it up on:

 **My profile is now safer because:**

Workshop 2

WORKSHEET 5

My Digital Footprint Check

Name: _____

Date: _____

Before Googling – My Prediction

I think Google will find about me: ☐ A lot ☐ A little ☐ Nothing

Google Search Results – About Me

What I found:

Was I surprised? ☐ Yes ☐ No

Anything I want to remove? ☐ Yes ☐ No

If yes, what?

Google Search Results – About My Child

What I found:

Was I surprised? ☐ Yes ☐ No

My Sharenting Reflection

How often do I post photos of my children?

☐ Every day ☐ Few times/week ☐ Few times/month ☐ Rarely ☐ Never

Who can see these photos? ☐ Everyone ☐ Friends ☐ Close friends only

Have I asked my child if they're okay with my posts? ☐ Yes ☐ No ☐ Too young to ask

Digital Cleanup – Changes I Made Today

☐ Deleted or hid old posts

☐ Removed connected apps

☐ Enabled tag review

☐ Set profile to Private



Family Challenge (this week!)

☐ Search my child's name on Google

☐ Review photos I posted of my children in the last month

☐ Ask my child: "Is there anything I posted about you that you'd like me to remove?"

My Screen Time Action Plan

Name: _____

Date: _____

My Screen Time Reality

Total daily average: _____

My #1 app: _____

My #2 app: _____

The shocking math:

Daily average	_____ hours
× 365 days =	_____ hours/year
÷ 24 hours =	_____ FULL DAYS/year

If I had those days back, I would:

Self-Assessment: Habit or Addiction?

Statement	Yes / No
-----------	----------

I check my phone first thing in the morning	
I feel anxious when I can't access social media	
I often spend more time than intended	
I've neglected something important because of scrolling	
I use social media to cope with boredom/stress/loneliness	
I've tried to reduce but couldn't stick to it	

My YES count: _____

0–1 = healthy | 2–3 = strong habit | 4–6 = may be affecting well-being

My 3 Alternatives to Scrolling

1.

2.

3.

 **My screen time goal for next week:**

Current average: _____

My goal: _____

Steps I will take:

- ☐ Set daily app limits
- ☐ Turn off non-essential notifications
- ☐ Move social apps off home screen
- ☐ Use a physical alarm clock
- ☐ Create a phone-free zone at: _____

My Digital Parenting Toolkit + Family Media Agreement

Name: _____

Date: _____

The 3 Pillars – My Notes

COMMUNICATE – What I will say to my child this week:

COLLABORATE – One rule I will create TOGETHER with my child:

PROTECT – One technical change I will make on my child's device:

Parental Controls I Set Up

- ☐ Google Family Link (Android)
- ☐ Apple Screen Time (iPhone)
- ☐ Daily screen time limits set
- ☐ Content filters enabled
- ☐ App approval required

- ☐ Downtime hours configured
- ☐ YouTube Restricted Mode on

Our Family Media Agreement

Complete at home with your family. Everyone signs!

Screen-free times:

- ☐ During meals
- ☐ After _____ PM
- ☐ During family activities
- ☐ Other: _____

Screen-free zones:

- ☐ Dining table
- ☐ Bedrooms
- ☐ Other: _____

Daily limits:

Family member	Weekday	Weekend

Our “Tell Me First” Rule:

“If anything scary happens online, my only job is to close the screen and tell a trusted adult. I will NEVER be punished for telling.”

The One Sentence That Matters

The most important thing I want my child to know:

Signatures (complete at home):

Parent:	Date:
Child:	Date:
Child:	Date:

 WORKSHEET 8

Family Cyberbullying Action Plan

Name: _____

Date: _____

What I Learned About Cyberbullying Today

Cyberbullying is different from playground bullying because:

The warning signs I will watch for in my child:

- ☐ Sudden change in mood after using their phone
- ☐ Not wanting to go to school
- ☐ Becoming secretive about online activities
- ☐ Changes in sleep or appetite
- ☐ Withdrawal from friends or family
- ☐ Declining grades
- ☐ Suddenly deleting apps or accounts

My Response Plan: LISTEN → THANK → SAVE → SOLVE

If my child tells me they are being cyberbullied, I will:

LISTEN:

Let them speak without interrupting. Stay calm. Don't show shock or anger.

THANK:

Say: "Thank you for telling me. I'm proud of you. This is NOT your fault."

SAVE:

Take screenshots of ALL messages, posts, and interactions before anything is deleted.

SOLVE:

Together, decide: Block the bully. Report to the platform. Contact school if needed.

Emergency Contacts

Fill these in now so you have them ready if you ever need them:

Contact	Phone / Email
Child's school (main office):	
Class teacher:	
School counselor / psychologist:	
Local police (non-emergency):	
National helpline for children / cyberbullying:	

How to Block and Report

Write down the steps for the apps YOUR child uses:

App 1: _____

To save evidence: _____

To block: _____

To report: _____

App 2: _____

To save evidence: _____

To block: _____

To report: _____

App 3: _____

To save evidence: _____

To block: _____

To report: _____

⚠ Remember: Always SAVE EVIDENCE first (screenshot), THEN block and report.

Conversation Starters

Use these to talk to your child about cyberbullying BEFORE it happens:

“What would you do if someone sent you a mean message online?”

“Do you know how to block someone on [their app]?”

“If something upsetting happened online, would you feel safe telling me? Why or why not?”

“Has anyone in your class ever been bullied online? What happened?”

“What would you do if a friend was being cyberbullied?”

What My Child Said

After using the conversation starters above, write down what you learned:

My child’s biggest concern about online safety:

Does my child know how to block and report?

☐ Yes ☐ No ☐ We practiced it together today

Would my child feel safe telling me about an online problem?

☐ Yes ☐ Not sure ☐ We need to work on this

My Promise to My Child

Write a personal promise about how you will respond if they come to you:

Signed:

Parent:	Date:
----------------	--------------

--	--

This worksheet booklet is part of the DEPART project (Erasmus+)

Keep it and keep your family safe! 

CHAPTER III

WORKSHOP 1

Total duration: 3 hours 45 minutes (225 minutes) | Target group: parents | Break: 15 minutes at mid-point

Covers sections 1–3.2 of Chapter III of the theoretical part.

General Objective

By the end of Workshop 1, parents will be able to protect their devices with antivirus software and regular updates, create strong and unique passwords, activate multi-factor authentication on their key accounts, and recognise the most common types of phishing and online data threats.

Specific Objectives

- They understand why antivirus software and system updates are the first, indispensable layer of digital defence.
- They can create a strong passphrase using the 'Secret Story' technique and understand why password reuse is dangerous.
- They activate MFA on at least one of their main accounts during the session.
- They can distinguish between different types of personal data and apply a simple check before sharing information online.
- They recognise the red flags of a phishing message and know how to apply the 'Go to the Source' rule.
- They leave with 1–3 concrete security actions they will apply during the coming week.

Workshop 1 Agenda

Time	Activity	Description
00:00–00:15	Arrival, introduction, ice-breaker	"My digital home" - what protects a physical home vs. a digital one.
00:15–01:00	M1: Device Protection & Updates	Antivirus, updates, mobile security, scareware vs. real alerts (sec. 1).
01:00–01:45	M2: Strong Passwords & Passphrases	Anatomy of a strong password, passphrase technique, password reuse trap (sec. 2.1–2.2).
01:45–02:00	Coffee break	-
02:00–02:45	M3: 2FA, MFA & Password Managers	Layers of security, enabling MFA, digital vaults and passkeys (sec. 2.3–2.5).
02:45–03:30	M4: Personal Data & Recognising Phishing	What is personal data, cookies, phishing red flags, STOP rule (sec. 3.1–3.2).
03:30–03:45	Summary, personal plan, feedback	"One security habit I start today."

Opening (15 min) - Welcome and Ice-Breaker

Objectives:

- Create a relaxed, non-judgmental atmosphere.
- Introduce the metaphor of the 'digital home' that frames the entire chapter.

Step by step:

- Welcome participants individually; help them write their first name on a name badge (3 min).

- Introduce yourself briefly - your name, role and one sentence about why digital security matters to you personally. Demystify the 'expert' role. (2 min)
- Draw a simple house on the flipchart. Ask: 'What protects your physical home?' Write answers around the house (door, lock, alarm, habits). Then ask: 'What protects your digital home?' Guide participants toward antivirus, passwords, updates, and safe habits. (6 min)
- Briefly announce the workshop agenda and what participants will take home. (1 min)
- Present the group rules: we listen until the end, there are no stupid questions, phones stay on the table - we will use them. (1 min)



Trainer Note

The 'digital home' metaphor is the thread connecting all eight modules - refer back to it whenever useful.

If a participant says 'I am not technical at all', respond: 'Then you are exactly the right person for today's workshop.'

Do not skip the ice-breaker - it builds the trust that will make the hands-on activities work.

Distribute the folders with Chapter III at the beginning, not at the end.

Module 1 - Device Protection & Updates (45 min)

↪ Correspondence with Part I: Sections 1.1–1.5 - 'Antivirus Software - Necessity or Fad'

Related Chapter	Sections 1.1–1.5 - Antivirus Software and Device Protection
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, participants' smartphones, printed scenario cards (Safe or Unsafe?), flipchart, markers
Group Size	8–14 participants
Handouts	Worksheets 1–4 from the Parent Worksheets Booklet (Workshop 1, Module 1): W1 - Real Alert or Scareware? (Ref. 1.1–1.2); W2 - Safe or Unsafe? (Ref. 1.3–1.4); W3 - What Are We Sharing? (Ref. 3.1); W4 - The Permission Check (Ref. 1.3–1.5)

Learning Objectives

- The participant understands that antivirus software is one indispensable layer of a broader defence strategy, not a magic solution.
- The participant distinguishes between real security alerts and scareware (fake, fear-based pop-ups).
- The participant can check whether their device has active protection and pending updates.
- The participant applies basic mobile security practices: reviewing app permissions, downloading only from official stores.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'The Digital House'	Group discussion + flipchart	Flipchart, markers
0:08– 0:20	Activity: Real Alert or Scareware? + Device Check (Worksheet 1)	Group analysis + individual on devices	Projected pop-up examples + smartphones + Worksheet 1
0:20– 0:30	Mini-lesson: What threatens our digital home?	Presentation + Q&A	Projector
0:30– 0:42	Game: Safe or Unsafe? (Worksheet 2)	Small groups	Worksheet 2
0:42– 0:48	Activity: What Are We Sharing? (Worksheet 3)	Individual + pairs	Smartphones + Worksheet 4
0:48– 0:50	 Wrap-up	Individual	Learning box on Worksheet 3

Detailed Activity Guide

Icebreaker: 'The Digital House' (8 min)

Trainer Note

This activity was introduced in the Workshop opening - if time is short, refer back to it briefly rather than repeating the full exercise.

The 'digital home' metaphor will recur throughout all eight modules. Use it consistently.

Avoid technical vocabulary. If a participant says 'antivirus', great - if not, guide them there naturally.

- Draw a simple house outline on the flipchart.
- Ask: 'What protects your physical home?' Write answers: doors, locks, alarm, cameras, good habits.
- Ask: 'What protects your digital home?' Guide toward: antivirus, passwords, updates, screen lock, safe downloading.
- Conclude: 'Just as we would not leave our front door open, we cannot afford gaps in our digital defences. Today we learn the first layer: protecting our devices.'

Activity: Real Alert or Scareware? - The Pop-up Challenge (12 min)

Trainer Note

Prepare two projected examples BEFORE the session: one real OS notification (e.g. Windows Security or iOS update prompt, screenshot) and one scareware pop-up (readily available via a web search for 'scareware example'). The contrast must be visual and immediate.

Project both images side by side if possible. If not, show them sequentially.

Participants work on Worksheet 1 while looking at the projected examples - they circle warning signs and complete the quick device check directly on the worksheet.

This activity intentionally comes BEFORE the mini-lesson on threat types: the emotional reaction to the scareware ('that looks terrifying!') creates the right conditions for the lesson that follows.

Do not reveal the answers immediately - let groups discuss for 2–3 minutes first.

- Project Pop-up A (scareware example) and Pop-up B (genuine OS notification) on screen.
- Participants open Worksheet 1 and circle every suspicious detail on Pop-up A, then note what makes Pop-up B trustworthy (2 min).
- Small group discussion (2 min): 'What differences did you spot?'
- Plenary debrief (3 min): collect answers on the flipchart. Guide toward: official notifications do not use alarming language, do not appear in the browser, do not display countdown timers, and never ask you to call a number or pay immediately.
- Participants complete their 'scareware rule' and quick device check on Worksheet 1 individually (5 min).

Key message: 'Scareware is designed to bypass rational thinking by triggering panic. Recognising it is the first defence. The second defence is the rule: close the window, never click inside it, then verify through your actual security settings.'

Mini-lesson: What threatens our digital home? (10 min)



Trainer Note

Build directly on the scareware activity - participants have already seen one real example.

Use the four threat types as labels, not lecture topics - one sentence each is enough.

The key message is not the taxonomy of threats, but the fact that threats are now automated, invisible, and do not require the user to make an obvious mistake.

Introduce the four main threat categories with a one-sentence definition each:

- Virus - a program that spreads between files and devices, damaging data.
- Malware - any software designed to damage, monitor, or steal information (viruses are one type of malware).
- Spyware - software that secretly collects personal data and transmits it to third parties.
- Ransomware - malware that encrypts files and demands payment to restore access.

Ask: 'Have you ever received a suspicious pop-up or warning on your device? What did you do?'

Allow 2–3 brief responses. Validate any instinct to close, ignore, or verify through settings.

Key message: 'Most cyber threats today do not wait for the user to make an obvious mistake - they actively look for unpatched vulnerabilities. Your behaviour matters, but so does your security software.'

Hands-on: Device Safety Check (12 min)

Trainer Note

This is integrated into Worksheet 1, right after the pop-up challenge. Participants tick off the quick checks while you guide them step by step on the projector.

Walk around the room and support those who need help. Pair more confident participants with those who feel uncertain.

Never ask participants to enter passwords or sensitive data during this exercise.

Have 2–3 spare devices available for those who have forgotten theirs.

Guide through the quick checks on Worksheet 1, step by step:

- Protection status: Android → Play Protect; Windows → Windows Security; iPhone → confirm iOS is up to date.
- Pending updates: 'Updates are security repairs. Every ignored notification is an open door.'
- Screen lock: verify PIN, fingerprint, or Face ID is active on every device. 'A locked device buys time to remotely erase data if lost or stolen.'
- One app permission check: Settings → Apps / Privacy → Permission Manager. Ask participants to check just one app's camera/microphone access - 'Does it make sense for this app to need this?'

Game: Safe or Unsafe? (6 min)

Trainer Note

Participants use Worksheet 2 to record their answers - print physical scenario cards too for tactile group engagement.

After each scenario, ask: 'Why?' - the reasoning matters more than the correct answer.

Keep the pace fast: this is a game, not a test.

Scenario	Expected Answer
Download a free game from an unknown website.	UNSAFE - unofficial sources often bundle malware.
Install an app from the official Google Play or App Store.	GENERALLY SAFE - always check reviews and permissions first.
A pop-up says: 'Your phone has 57 viruses! Click SCAN NOW!'	UNSAFE - classic scareware. Close it; verify through official security settings.
Your operating system prompts you to install a security update.	SAFE - install it. Delays leave known vulnerabilities open.
A calculator app requests access to your contacts and microphone.	UNSAFE - excessive permissions are a warning sign.

Key Messages of the Module

1. An antivirus is one essential layer of protection - not a substitute for safe behaviour, but a safety net for the moments when human eyes cannot detect the threat.
2. Updates are security repairs. Delaying them means leaving known vulnerabilities deliberately open.
3. Scareware is designed to cause panic. A real security alert never demands that you call a number or pay immediately.

Trainer Tips

- Use local, relatable examples: a child downloading a 'free' game, a parent opening an attachment that looked like a school invoice.
- Avoid making participants feel foolish for past mistakes - normalise the problem: 'This catches everyone at some point.'
- Do not recommend specific paid antivirus brands. Mention that built-in protections (Windows Defender, Google Play Protect, iOS security) are a solid starting point when kept updated.

- Final message for participants: 'Digital security does not require expert knowledge - it requires awareness and a few consistent habits. Today you took the first step.'

Module 2 - Strong Passwords & Passphrases (45 min)

↪ *Correspondence with Part I: Sections 2.1–2.2 - 'The Importance of Passwords in Securing Accounts'*

Related Chapter	Sections 2.1–2.2 - Password Anatomy and Password Reuse
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, paper, pens, markers
Group Size	8–14 participants
Handouts	Worksheets 5–6 from the Parent Worksheets Booklet (Workshop 1, Module 2): W5 - Rank the Passwords (Ref. 2.1); W6 - The Password Reuse Trap (Ref. 2.2)

Learning Objectives

- The participant recognises common password mistakes (short, predictable, based on personal data).
- The participant understands why a long passphrase is often stronger than a short complex password.
- The participant creates their own 'Secret Story' passphrase - a memorable phrase that is hard for machines to guess.
- The participant understands the chain-reaction risk of password reuse through the 'credential stuffing' concept.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'The Secret Code'	Group discussion	Flipchart
0:08– 0:18	Mini-lesson: Why passwords matter - and how they fail	Presentation + discussion	Projector
0:18– 0:30	Game: Rank the Passwords	Small groups	Worksheet 4
0:30– 0:42	Hands-on: Build a 'Secret Story' Passphrase	Individual + pairs	Paper, pens
0:42– 0:48	Discussion: The Password Reuse Trap	Group discussion	Flipchart
0:48– 0:50	 Handout + Wrap-up	Individual	Worksheets 5–6

Detailed Activity Guide

Icebreaker: 'The Secret Code' (8 min)

Trainer Note

This activity connects the abstract concept of passwords to a childhood experience everyone has had.

Keep it light and fast - 30 seconds per person maximum.

The goal is to surface the emotional logic behind passwords: they protect what matters to us.

- Ask: 'When you were a child, did you ever have a secret code or hiding place with friends or family?'
- Invite 3–4 volunteers to share briefly.

- Ask: 'Why did you use a secret code? - To keep others out. To identify trusted people. To protect something.'
- Connect: 'Passwords serve exactly the same purpose. They are the keys to our digital lives - and like physical keys, some are much stronger than others.'

Mini-lesson: Why passwords matter - and how they fail (10 min)

Trainer Note

Start with the 'email as master key' insight - it tends to generate a strong 'aha' moment.

Do not go into technical details about hashing algorithms. Focus on the human behaviour that makes passwords weak.

The most common reaction is: 'I never thought about how many accounts my email can reset.' Build on this.

Ask participants: 'How many online accounts do you think you have?' Write a few answers on the flipchart. (Most people underestimate significantly - research suggests the average is 80–100.)

Ask: 'Which account would be most damaging to lose?' Guide toward: email - because it can be used to reset passwords for almost every other service.

Introduce common password mistakes:

- Using personal information: names, birthdays, pet names, birth year.
- Using predictable patterns: 'Password1!', sequences like '12345678', keyboard walks like 'qwerty'.
- Using short passwords - modern computers can test millions of combinations per second.
- Sharing passwords or writing them in visible places.

Introduce the concept of entropy: what makes a password genuinely hard to guess is unpredictability, not just complexity symbols. A 20-character passphrase built from unrelated

words is exponentially harder to crack than an 8-character password with symbols, because its unpredictability comes from human memory rather than predictable rules.

Game: Rank the Passwords (12 min)

Trainer Note

Teams of 3–4 receive worksheet 4. They rank from weakest to strongest before the reveal.

The goal is not the correct ranking - it is the discussion. Why did they choose this order?

Make it slightly competitive: 'Which group got the ranking exactly right?'

Card	Password	Strength & Reason
A	123456	Very weak - the single most common password globally.
B	Maria1980	Weak - personal information, predictable pattern.
C	Football22!	Weak-medium - common word, predictable substitution.
D	P@ssw0rd!	Weak despite 'complexity' - follows predictable rules that hacking software knows.
E	BlueTrainRiverMoon	Strong - long, four unrelated words, no personal data.
F	i-PlaYeD-bAll-on-SundaY-26-vito!	Very strong - a personal story with irregular capitalisation, a random number, and a name only the creator would use.

After the reveal, explain the key insight: length and unpredictability beat complexity. Card F is stronger not because of its symbols, but because a machine cannot guess the story behind it.

Hands-on: Build a 'Secret Story' Passphrase (12 min)

Trainer Note

Do NOT ask participants to reveal real passwords. Ask only: 'How many words did you use?' and 'Was it easier to remember?'

Walk around the room and offer help. Some participants will find the creative step difficult - suggest starting with a funny family memory.

This activity connects directly to Chapter III's 'Secret Story' activity and the 'Leo and the blue squirrel' example.

Guide participants through the following steps on paper:

- Think of a funny or unusual memory that only your family would know (e.g., a squirrel eating a blue popsicle at the park).
- Turn it into a short sentence: 'BlueSquirrelAteIt!'
- Now strengthen it: add a random number in a non-obvious place, mix one word from another language, or use irregular capitalisation that is meaningful to you: 'blu3-Squirrel-mangiò-IT!'
- Practice typing it twice. If you can type it from memory, it works.

Debrief in pairs: 'Is it easier to remember than a string of random characters? Why?'

Discussion: The Password Reuse Trap (6 min)

Trainer Note

Draw several houses on the flipchart - this is the 'neighbourhood key' analogy from Chapter III.

The 'credential stuffing' concept does not need to be named - just explain the mechanism.

Draw 5 houses on the flipchart and ask: 'Imagine every house in this street used exactly the same front door key. What would happen if one key were stolen?'

Participants immediately see the problem. Connect: 'Using the same password across multiple accounts creates exactly this risk. One breach in one website - even a small one you have almost forgotten - can cascade into every account you own.'

Ask: 'Which accounts should absolutely have unique passwords?' Guide toward: email, banking, government services, social media.

Key Messages of the Module

1. The strength of a password comes from unpredictability, not just complexity. A long passphrase built from a personal story is much harder for a machine to guess than a short password with symbols.
2. Your email account is the master key to your digital life - it deserves a unique, strong passphrase above all others.
3. Reusing passwords creates a chain reaction: one breach can compromise every account that shares the same key.

Trainer Tips

- Avoid jargon: say 'a sequence of words' rather than 'passphrase' until participants are comfortable with the concept.
- The 'child creating a magic spell' framing (from sec. 2.5) works well even with adult participants - it makes the creative step feel playful rather than technical.
- If a participant says 'I have too many accounts to use different passwords everywhere', transition naturally to the next module (password managers).
- Final message for participants: 'A strong password does not need to be complicated - it needs to be unique, long, and meaningful to you. Start with your email account.'

Module 3 - 2FA, MFA & Password Managers (45 min)

↔ Correspondence with Part I: Sections 2.3–2.5 - '2FA and MFA: The Essential Layers of Security' and 'Digital Vaults and Passkeys'

Related Chapter	Sections 2.3–2.5 - Multi-Factor Authentication, Password Managers, Passkeys
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, smartphones, Worksheet 7 (The Unexpected Notification), flipchart, markers
Group Size	8–14 participants
Handouts	Worksheets 7–8 from the Parent Worksheets Booklet (Workshop 1, Module 3): W7 - Activating 2FA (Ref. 2.3); W8 - My Digital Vault (Ref. 2.4–2.5)

Learning Objectives

- The participant understands why even a strong password can be stolen and why MFA is the essential safety net.
- The participant can enable Two-Factor Authentication on at least one of their key accounts during the session.
- The participant recognises an unsolicited MFA prompt as a sign that someone is actively trying to break into their account.
- The participant understands the concept and benefit of a password manager (Digital Vault) without feeling technically overwhelmed.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'One Lock or Two?'	Group discussion + flipchart	Flipchart, markers
0:08– 0:18	Mini-lesson: Why passwords are sometimes not enough	Presentation + discussion	Projector
0:18– 0:33	Hands-on: Enable MFA - The Master Account Upgrade	Individual on devices	Smartphones
0:33– 0:43	Group Exercise: The Stolen Password Scenario	Small groups	Scenario cards
0:43– 0:48	Mini-lesson: Password Managers Made Simple	Short presentation + Q&A	Projector
0:48– 0:50	 Handout + Wrap-up	Individual	Worksheets 7–8

Detailed Activity Guide

Icebreaker: 'One Lock or Two?' (8 min)

Trainer Note

Draw two simple doors on the flipchart. This is a quick visual exercise, not a long discussion.

The analogy 'password = first lock, MFA = second lock' is the key message to establish here.

If someone has already heard of 2FA, let them explain it briefly - it validates their knowledge and speeds up the lesson.

- Draw Door A (one lock) and Door B (lock + security alarm code).

- Ask: 'Which door would you choose to protect something valuable?' (Door B - everyone agrees.)
- Ask: 'Why do we often protect our online accounts with only one lock?' Allow brief answers.
- Conclude: 'A password is the first lock. 2FA adds a second lock - and we are going to activate it today.'

Mini-lesson: Why passwords are sometimes not enough (10 min)

Trainer Note

Build directly on Module 2. Do not re-explain passwords from scratch.

The three scenarios are the core of this section - take 2 minutes each.

The Unexpected Notification - what would you do?

Project or hand out the simulated notification: "🔔 Sign-in request - Someone is trying to access your email from a device you don't recognise. [Approve] [Deny]"

Ask participants: "You didn't try to log into anything. What do you do?" Let them answer on Worksheet 6.

Guide toward: Deny first - that blocks the immediate attempt. Then explain the critical second step: changing the password, because a request you didn't trigger means someone already has it. Denying alone doesn't close the door for the future.

Ask: 'Can even a strong passphrase be stolen?' Let participants think. Guide toward: phishing sites, data breaches in third-party services, shared devices.

Present three real scenarios:

- Scenario 1: A website you use suffers a data breach. Your email and password are published on the dark web - even though you did nothing wrong.
- Scenario 2: You receive a convincing email from what appears to be your bank. You enter your credentials on a fake page.

- Scenario 3: You previously saved your password on a shared family device that another person can access.

Key message: 'MFA does not prevent password theft. It prevents unauthorized access even after the password has been stolen. A hacker with your password but without your phone is locked out of your account.'

Briefly introduce the MFA Fatigue concept: attackers sometimes flood a phone with rapid MFA approval requests, hoping the user will accidentally tap 'Approve' to clear the screen. Rule: 'If you did not start the login, never approve the request.'

Hands-on: Enable 2FA - The Master Account Upgrade (15 min)

Trainer Note

This is the core practical activity of the module. Every participant should leave having activated MFA on at least one account.

Demonstrate live on a platform shown on the projector (Google or email account recommended). Participants follow on their own devices.

Walk around the room and provide individual support. Pair confident participants with those who struggle.

Never ask participants to enter their password in front of others - they should work on their own device privately.

Guide participants through the following steps:

- Open account settings on your primary email account.
- Navigate to: Security → Two-Step Verification (or Two-Factor Authentication / MFA).
- Choose a verification method. Explain the options:
- SMS code - quick to set up, but can be intercepted via SIM-swapping. Good starting point.

- Authenticator App (Google Authenticator, Microsoft Authenticator) - generates a time-limited code locally, more secure than SMS.
- Passkey / biometric - the most advanced option; uses fingerprint or Face ID. Explore this if participants are comfortable.
- Complete the activation and store recovery codes in a safe physical location (e.g., printed and kept with important documents at home).

Important reminder: 'If you receive an MFA approval request that you did not initiate, deny it immediately. It means someone has your password and is actively trying to get in. After denying, change your password right away.'

Group Exercise: The Stolen Password Scenario (10 min)

Trainer Note

Groups of 3 discuss each card for 2 minutes, then share with the room.

The goal is to show that the same event (password stolen) has completely different outcomes depending on whether MFA is active.

Card	Scenario	Discussion Questions
1	A hacker finds your Facebook password from a data breach. MFA is disabled.	What can the hacker do? What information do they now have access to? What can they do with it?
2	A hacker finds your Facebook password from a data breach. MFA is enabled.	What happens when they try to log in? What wall do they hit? What do you see on your phone?
3	Someone learns your primary email password. MFA is enabled.	Why is the email account particularly critical? What additional barrier does MFA create here?

After discussion, summarise: 'Passwords protect accounts from people who do not know the password. MFA protects access even from people who do.'

Mini-lesson: Password Managers Made Simple (5 min)

Trainer Note

Many participants will react with 'But if someone hacks the manager, they have everything!' - address this proactively.

Keep it short. The goal is awareness and a first step, not a full tutorial.

Use the 'key cabinet' analogy from Chapter III section 2.4.

Ask: 'How do you currently manage your passwords?' (Show of hands: I remember them / I write them on paper / I use the browser / I use a manager.)

Introduce the concept: 'A password manager - or Digital Vault - is like a secure key cabinet. It stores all your passwords in an encrypted safe. You only need to remember one Master Passphrase to open it.'

Benefits: generates unique strong passwords for every account, autofills them for you, alerts you if any of your passwords have been leaked in known data breaches.

Examples to mention: Bitwarden (free, open-source), 1Password, or the built-in password manager in iPhone (Passwords app) or Google Chrome.

Key reassurance: 'The manager encrypts everything. Even the service provider cannot see your passwords. If you lose your Master Passphrase, there is no backup - so write it down and keep it safe at home.'

Key Messages of the Module

1. MFA is the essential safety net that protects your account even after your password has been stolen.
2. If you receive an MFA request you did not initiate - deny it and change your password immediately.

3. A password manager removes the impossible task of memorising dozens of unique passwords. You only need to remember one.

Trainer Tips

- Test the MFA activation flow on the platform you plan to demo BEFORE the workshop. Interfaces change frequently.
- If a participant's device does not support authenticator apps, SMS-based 2FA is still much better than no MFA at all.
- Do not go into the technical details of public-key cryptography or passkeys unless participants specifically ask. Focus on the practical outcome: 'You log in with your face - there is no password to steal.'
- Final message for participants: 'A strong password is an excellent start. MFA is the alarm system behind the lock. Together they make your digital home genuinely secure.'

Module 4 - Personal Data & Recognising Phishing (45 min)

↔ *Correspondence with Part I: Sections 3.1–3.2 - 'Protecting Your Family's Online Data', 'Personal Data' and 'Phishing and Social Engineering'*

Related Chapter	Sections 3.1–3.2 - What is Personal Data and Phishing / Social Engineering
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, Worksheet 8 (data sorting), Worksheet 9 (phishing examples), flipchart, markers
Group Size	8–14 participants

Handouts	Worksheets 9–10 from the Parent Worksheets Booklet (Workshop 1, Module 4): W9 - Spot the Fake (Ref. 3.2); W10 - My Workshop 1 Action Plan
-----------------	--

Learning Objectives

- The participant understands that personal data extends far beyond names and ID numbers - it includes browsing habits, photos, location, and daily routines.
- The participant understands what website cookies are and can make a conscious choice when encountering a cookie consent banner.
- The participant recognises the red flags of a phishing message: urgency, generic greeting, suspicious sender address, link mismatch.
- The participant applies the 'Go to the Source' rule: never use a link from an alarming message - always navigate directly to the official website.

Session Plan

Time	Activity	Method	Materials
0:00–0:08	Icebreaker: 'What Would a Stranger Know?'	Group discussion + flipchart	Flipchart, markers
0:08–0:18	Mini-lesson: What is Personal Data - and Why It Has Value	Presentation + Q&A	Projector
0:18–0:30	Activity: Data Sorting Challenge + Cookie Moment	Small groups + discussion	Data-sorting cards
0:30–0:43	Activity: Phishing Detective	Small groups	Worksheet

Time	Activity	Method	Materials
0:43– 0:48	Discussion: The 'Go to the Source' Rule	Group discussion	Flipchart
0:48– 0:50	 Handout + Wrap-up	Individual	Worksheets 9–10

Detailed Activity Guide

Icebreaker: 'What Would a Stranger Know?' (8 min)

Trainer Note

This is a powerful opening exercise - participants often surprise themselves.

Focus on what can be inferred, not just what is directly stated. A photo with a school uniform and a visible street sign reveals school, neighbourhood, and routine.

Keep it non-judgmental - the goal is reflection, not shame.

- Ask: 'Imagine a stranger could see your last month of social media posts. What could they learn about you and your family?' Write answers on the flipchart.
- Guide toward: name, family members, home area, school name and schedule, daily routines, workplace, places visited, income indicators, children's physical appearance.
- Ask: 'Would you feel comfortable if a stranger knew all of this?' Allow brief discussion.
- Conclude: 'Personal information is valuable. Once shared online, it is very difficult to control where it goes or who uses it.'

Mini-lesson: What is Personal Data - and Why It Has Value (10 min)

Trainer Note

The key insight to land here: personal data is not just formal identifiers - it is the invisible trail of daily digital life.

The GDPR reference is important for European audiences - it reframes privacy as a legal right, not just a good habit.

The child identity-theft angle (synthetic identity fraud) tends to generate strong emotional engagement among parents.

Explain: 'Personal data is any information that can identify a person - directly or indirectly.'

Direct identifiers: name, address, phone number, email, national ID number.

Indirect identifiers: location history, browsing habits, photos (including metadata), school name, daily routines, device fingerprint.

Invisible data: cookie tracking across websites, app permissions, smart-device usage patterns.

Introduce the concept of cookies briefly: small text files that websites store on a device to remember preferences, keep users logged in, or track browsing behaviour across different sites. When a cookie banner appears, participants now have the context to make a meaningful choice - not just click 'Accept All' to make it disappear.

Key message: 'When an app or website is free, we are often paying with data. Recognising this allows us to make conscious choices about what we share.'

Mention child data specifically: children's data is particularly sensitive because their records are clean, unmonitored, and can be exploited for identity fraud for years before it is discovered.

Activity: Data Sorting Challenge (12 min)

Trainer Note

Groups use Worksheet 8 and sort the listed information into three columns.

The 'share carefully' column generates the most discussion - context always matters.

The Cookie Moment takes only 3 minutes at the end - show a real cookie banner on the projector and walk through the options together.

Groups of 3–4 sort cards into three categories:

Safe to Share Publicly	Share Carefully	Keep Private
First name only	Full name	National ID / tax number
General interest (e.g., 'I love hiking')	Workplace name	Home address and postcode
Holiday photos (after returning home)	Children's school name	Children's full names + school + photo together
-	Holiday photos (while still away)	Banking or payment details

After sorting, discuss: 'Did any card surprise you? Which ones were hardest to categorise?'

Note: cookies are covered in depth in Workshop 2, Module 5, Worksheet 13. Mention briefly here that cookie banners are part of how personal data is collected online - 'when a site is free, you often pay with your data' - then refer participants to the dedicated worksheet in Workshop 2.

Activity: Phishing Detective (13 min)

Trainer Note

Print three example messages in advance. Groups analyse each one and circle every warning sign they can find.

The best examples use real-looking logos (delivery companies, banks) to show how convincing modern phishing has become.

Avoid examples from local politics or religion - use universal contexts: delivery, banking, streaming services, schools.

Groups receive three printed examples (email, SMS, WhatsApp message). For each, they circle every warning sign they notice.

Example	Scenario	Red Flags to Find
A	Email: 'URGENT - Your bank account will be suspended today! Click here to verify.'	Generic greeting ('Dear Customer'), alarming subject, suspicious link (hover reveals: mybank.account-verify.net), pressure to act immediately, no account details.
B	SMS: 'Your package is waiting. Pay €2.50 delivery fee: [link]'	Unknown sender number, unexpected request, suspicious URL, no tracking number, no sender identification.
C	WhatsApp: 'Hi, I'm from [School Name] IT support. We need your login to update your account.'	Legitimate organisations never ask for credentials via message, no official school channel, urgency tactic.

After reviewing together, ask: 'What made these messages convincing despite the warning signs?'
Guide toward: familiar branding, emotional urgency, appearing to come from a trusted institution.

Discussion: The 'Go to the Source' Rule (5 min)

Introduce the rule: 'If you receive an alarming message from a bank, school, delivery company, or government agency - never use the link or phone number provided in that message. Open a new

browser tab and navigate directly to the official website you already know. If the problem is real, you will see it there. If it is not, you have just avoided a trap.'

Ask: 'Has anyone here already done something like this without knowing it had a name?' Often participants have.

Key Messages of the Module

1. Personal data is your family's digital identity - it extends far beyond names and includes the invisible trail of everyday digital life.
2. When something online is free, you are often paying with your data. Recognising this is the first step to managing it.
3. The most effective protection against phishing is the 'Go to the Source' rule: never follow a link from an alarming message - always navigate independently.

Trainer Tips

- Use local examples for phishing: mention that Italian families frequently receive SMS scams impersonating the Poste Italiane, courier companies (SDA, BRT), or INPS.
- Normalise falling for scams: 'Scammers today use AI to create flawless, personalised messages. Being deceived does not mean being careless.'
- Avoid using political figures or controversial brands as examples - keep it universally relatable.
- Final message for participants: 'Your personal data is one of your family's most valuable assets. Protecting it does not require technical expertise - it requires the habit of pausing and thinking before sharing or clicking.'

Workshop 1 Closing (15 min)

Objectives:

- Summarise the four modules in four simple messages.

- Personal plan: 1–3 concrete actions for the coming week.
- Collect feedback.

Step by step:

- Visual summary on the flipchart (3 min): recap the four key messages in one sentence each. 'Update your devices. Create a strong passphrase. Activate MFA on your email. Pause before clicking.'
- 'One habit I start today' circle (5 min): each participant says in one sentence the single security action they will take this week.
- Referral to Chapter III (2 min): 'At home, re-read Chapter III of your guide - everything we discussed today is there, with additional examples and step-by-step guides.'
- Feedback form - Annex A (3 min).
- Announcing Workshop 2: date, location, topics. (2 min)

Final message for participants - Workshop 1: 'Protecting your digital home does not require expert knowledge. It requires four habits: keep your devices updated, use strong and unique passwords, add a second lock with MFA, and pause before sharing or clicking. You have taken all four steps today. Thank you.'

WORKSHOP 2

Protecting Your Family Online

Total duration: 3 hours 45 minutes (225 minutes) | Target group: parents | Break: 15 minutes at mid-point

Covers sections 3.3–5.5 of Chapter III of the theoretical part.

General Objective

By the end of Workshop 2, parents will be able to use public Wi-Fi networks safely, manage privacy settings on smart home devices and cloud accounts, establish a Family Digital Understanding, configure parental controls appropriate to their children's ages, and respond effectively when their child encounters an online risk.

Specific Objectives

- They understand the risks of public Wi-Fi and know how a VPN provides a practical layer of protection.
- They can identify what data their smart TV, voice assistant, or connected toy may be collecting and know how to audit privacy settings.
- They can draft a simple, co-designed Family Digital Understanding with clear rules, responsibilities, and consequences.
- They can configure at least one parental control feature on a family device during the session.
- They recognise the warning signs of cyberbullying, grooming, harmful content exposure, and gaming scams.
- They know how to respond when a child discloses an online incident: listen, reassure, document, act.

- They leave with 1–3 concrete family safety actions to implement before the next week.

Workshop 2 Agenda

Time	Activity	Description
00:00–00:15	Recap + ice-breaker	What did we apply from Workshop 1? + Opinion Barometer.
00:15–01:00	M5: Public Wi-Fi, VPNs & Secure Websites	Risks of open networks, VPN basics, HTTPS vs. HTTP (sec. 3.3–3.5).
01:00–01:45	M6: Smart Devices, Cloud & Family Digital Contract	Privacy on connected home devices, cloud settings, drafting the Understanding (sec. 3.4 + 4.1–4.2).
01:45–02:00	Coffee break	-
02:00–02:45	M7: Parental Controls, Screen Time & Leading by Example	Hands-on with tools, age-appropriate limits, adult digital behaviour (sec. 4.3–4.5).
02:45–03:30	M8: Online Risks - Cyberbullying to Digital Resilience	Threats, warning signs, communication, LISTEN-REASSURE-DOCUMENT-ACT (sec. 5).
03:30–03:45	Final summary, personal plan, feedback	"One thing I will do for my family this week."

Opening (15 min) - Recap and Ice-Breaker

Objectives:

- Reactivate the connections established in Workshop 1.
- Identify what participants actually applied during the week.

Step by step:

- Welcome participants, name badges (2 min).
- Quick circle: 'My name is... and since the last workshop I tried / I noticed / I changed...' (5 min).
- Opinion Barometer (6 min): Three corners of the room - YES / NO / NOT SURE. Read statements; participants move physically: 'I know if my Smart TV has a microphone' • 'I have a rule at home about phone use at dinner' • 'I know what my child does online after school' • 'I would feel confident responding if my child reported an online problem.'
- Announce the agenda for Workshop 2. (2 min)



Trainer Note

The Barometer is especially powerful here because it surfaces the gap between intention (Workshop 1) and action - without any judgment.

Validate all changes made during the week, however small. 'You checked your app permissions? That is exactly what we hoped for.'

Do not comment on Barometer positions - simply ask 'Why did you choose here?' and listen.

Module 5 - Public Wi-Fi, VPNs & Secure Websites (45 min)

↔ *Correspondence with Part I: Sections 3.3–3.5 - 'Public Wi-Fi Risks and VPNs', 'Recognising Secure Websites'*

Related Chapter	Sections 3.3–3.5 - Public Wi-Fi, VPNs, HTTPS vs. HTTP
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, smartphones, Worksheet 11 (Wi-Fi Risk Map), flipchart, markers
Group Size	8–14 participants
Handouts	Worksheets 11–13 from the Parent Worksheets Booklet (Workshop 2, Module 5): W11 - Public Wi-Fi Risks (Ref. 3.3); W12 - The Padlock Inspection (Ref. 3.5); W13 - Cookies: Our Digital Footprints (Ref. 3.1)

Learning Objectives

- The participant understands why public Wi-Fi networks are inherently risky and can identify the most dangerous situations.
- The participant understands what a VPN does in practical terms - it encrypts the connection so that intercepted data is unreadable - and knows how to activate one.
- The participant recognises the HTTPS padlock and understands both what it guarantees (encrypted connection) and what it does not guarantee (the site itself is trustworthy).
- The participant knows the 'Forget This Network' habit and can apply it after leaving a public place.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'The Glass Room'	Group discussion	Flipchart
0:08– 0:18	Mini-lesson: Why public Wi-Fi is a risk - and what attackers do	Presentation + discussion	Projector
0:18– 0:30	Activity: The Wi-Fi Risk Map	Small groups	Worksheet 11
0:30– 0:40	Mini-lesson: VPNs and HTTPS - two practical shields	Presentation + live demo	Projector + smartphones
0:40– 0:48	Hands-on: The Hotspot Check	Individual on devices	Smartphones
0:48– 0:50	 Handout + Wrap-up	Individual	Worksheets 11–13

Detailed Activity Guide

Icebreaker: 'The Glass Room' (8 min)

Trainer Note

This analogy comes directly from Chapter III section 3.3. Use the exact image: 'a room with glass walls where anyone can see what you are doing.'

The goal is to create an immediate, visceral understanding of what 'open network' means - no technical explanation needed yet.

- Ask: 'Have you ever connected to a free Wi-Fi network in a café, airport, or hotel?' (Almost everyone raises their hand.)
- Ask: 'What did you use it for?' Write answers: email, social media, banking, shopping, watching videos.
- Introduce the metaphor: 'Imagine that room had glass walls and everyone could watch exactly what you were doing on your device. That is essentially what an open public Wi-Fi network is from a security perspective.'
- Pause. Let the image land. Then: 'Today we learn how to draw the curtains.'

Mini-lesson: Why public Wi-Fi is a risk - and what attackers do (10 min)

Trainer Note

Introduce Man-in-the-Middle and Evil Twin attacks using simple language, not technical names.

The 'Free_Airport_WiFi' Evil Twin example resonates strongly with families who travel.

Keep this conceptual - the practical defence comes in the next activities.

- Explain: 'When you connect to a public Wi-Fi, your device joins a shared space with everyone else at that location. If the network is not encrypted, someone with the right tools can see the data flowing between your device and the internet.'
- Introduce the interception concept simply: 'An attacker can position themselves between your phone and the network router, capturing everything that passes through.'
- Introduce the Evil Twin concept: 'Attackers sometimes create a fake Wi-Fi network with a legitimate-sounding name - Free_Airport_WiFi, Hotel_Guest, CafeInternet. Once you connect, they can redirect you to fake login pages or capture your data.'
- Ask: 'Which of the things you said you use public Wi-Fi for would be most dangerous if someone could read them?' Guide toward: banking, email login, entering passwords, shopping.

Activity: The Wi-Fi Risk Map (12 min)

Trainer Note

Prepare scenario cards. Groups discuss and rank each situation from LOW to HIGH risk.

The goal is not a perfect risk taxonomy - it is helping participants build intuition about when to be careful.

Scenario	Risk Level	Why
Watching a YouTube video on café Wi-Fi	Low-Medium	Data is not sensitive; no login credentials entered.
Checking your bank balance on airport Wi-Fi	HIGH	Bank login credentials and account details at risk.
Entering a password on a hotel Wi-Fi network	HIGH	Password could be intercepted.
Letting children play a downloaded game on public Wi-Fi	Medium	Lower direct risk if no login or in-app purchase involved.
Accessing your work email on a library Wi-Fi	HIGH	Professional credentials and potentially sensitive data at risk.

Mini-lesson: VPNs and HTTPS - two practical shields (10 min)

Trainer Note

A VPN should be explained functionally, not technically. The 'encrypted tunnel' metaphor is enough.

The HTTPS section must include the critical caveat: HTTPS means the connection is encrypted, NOT that the website is trustworthy.

Show a real browser padlock on the projector. Let participants find it on a website they use.

VPN - the encrypted tunnel:

- 'A VPN is software that wraps your internet connection in an encrypted layer. Even if someone intercepts it, all they see is scrambled, unreadable data.'
- 'For families, the most important use case is protecting sensitive activities - banking, emails, passwords - when using public Wi-Fi.'
- Examples of reputable VPNs to mention (without recommending): ProtonVPN (free tier available), NordVPN, the VPN built into some routers.
- Important caveat: 'A VPN protects your connection - it does not protect you from phishing, malicious apps, or clicking on suspicious links.'

HTTPS - the padlock:

- 'A website starting with HTTPS encrypts the communication between your browser and the site. Look for the padlock icon in the address bar.'
- Critical distinction: 'The padlock means the connection is secure. It does not mean the website itself is honest. A scam site can have HTTPS too - it just means the scam is delivered securely to you.'
- 'Always check the full address. A single changed letter - paypal.com instead of paypal.com - is enough to send you to a fake site.'

Hands-on: The Hotspot Check (8 min)

Trainer Note

This is a direct application of the 'Forget the Network' tip from Chapter III section 3.3.

Walk through the steps on the projector. Participants follow on their own phones.

- Ask participants to open their Wi-Fi settings. Count how many open networks (no padlock) are visible.

- Guide: 'Find a network you have connected to before in a public place. Use the Forget option.' (iPhone: tap ⓘ → Forget This Network. Android: long-press network name → Forget.)
- Explain: 'This prevents your phone from automatically connecting to that network - or a fake network with the same name - next time you are nearby.'
- Remind: 'Enable the setting that requires permission before joining new networks, rather than connecting automatically.'

Key Messages of the Module

1. Public Wi-Fi is a shared space - treat it like a public conversation that others can hear. Never use it for sensitive tasks without a VPN.
2. A VPN encrypts your connection so that intercepted data is unreadable. It is a practical, easy-to-use tool - not just for tech experts.
3. HTTPS means the connection is encrypted. It does not mean the website is trustworthy. Always check the full address carefully.

Trainer Tips

- Use the Marco example from Chapter III section 3.3 - he activates the family VPN before checking his bank balance at a bus station. It is concrete and relatable.
- Do not recommend any specific VPN brand, but acknowledge that the built-in VPN on some routers and in Apple's iCloud Private Relay offer convenient starting points.
- For the HTTPS section, show both a padlock and a 'Not Secure' warning in Chrome/Safari. The visual contrast is very effective.
- Final message for participants: 'You cannot always control which networks are available. But you can always control whether you activate your VPN before opening your bank app - and that choice protects your family's money.'

Module 6 - Smart Devices, Cloud Privacy & Family Digital Contract (45 min)

↔ *Correspondence with Part I: Section 3.4 - 'Privacy on the Internet, in the Cloud and on Connected Home Devices' and Section 4.1 - 'Establishing a Family Digital Understanding'*

Related Chapter	Section 3.4 - Smart Devices and Cloud Privacy; Section 4.1 - Family Digital Understanding
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, smartphones, 'Device Mute Walk' list, Family Agreement template (flipchart or printed), markers
Group Size	8–14 participants
Handouts	Worksheets 14–16 from the Parent Worksheets Booklet (Workshop 2, Module 6): W14 - The 'Device Mute' Walk (Ref. 3.4) - completed during session; W15 - The 'Device Basket' Challenge (Ref. 4.4–4.5) - completed during session; W16 - Our Family Digital Understanding (Ref. 4.1) - distributed at end of module, to be completed at home with the whole family

Learning Objectives

- The participant understands that Smart TVs, voice assistants, and connected toys collect data passively and knows how to audit their privacy settings.
- The participant understands that cloud backups exist and are running on their device - and knows how to review what is being backed up and who has access.
- The participant drafts the basic structure of a Family Digital Understanding - a written, co-designed agreement covering screen-free zones, reporting of problems, and basic security commitments.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'Does Your TV Listen?'	Group discussion	Flipchart
0:08– 0:18	Mini-lesson: The Connected Home - what is watching and listening	Presentation + discussion	Projector
0:18– 0:28	Hands-on: Cloud & Smart Device Privacy Audit	Individual on devices	Smartphones
0:28– 0:40	Activity: Draft a Family Digital Understanding	Individual + pairs	Agreement template
0:40– 0:48	Discussion: What Makes a Digital Agreement Work?	Group discussion	Flipchart
0:48– 0:50	 Handout + Wrap-up	Individual	W14–W15 (completed during session); W16 (take-home)

Detailed Activity Guide

Icebreaker: 'Does Your TV Listen?' (8 min)

Trainer Note

Many parents have never thought of a Smart TV as a data-collecting device. The initial reaction is often disbelief.

Keep the opening question light and curious, not alarmist.

The goal is not to create fear about smart devices - it is to create awareness that they require privacy management, just like smartphones.

- Ask: 'How many of you have a Smart TV at home? A voice assistant like Alexa or Google Home? Any connected toys for your children?'
- Ask: 'Do you think your Smart TV knows what you watch? Could it know when you are at home?'
- Allow reactions. Many participants will be surprised. Validate: 'You are not wrong to be surprised - most people set up smart devices and never look at the privacy settings again.'
- Conclude: 'Today we look at the invisible side of the connected home - and we take control of it.'

Mini-lesson: The Connected Home - what is watching and listening (10 min)

Trainer Note

Reference the European research findings from Chapter III section 3.4 briefly - it adds authority without being academic.

The key message is not 'throw away your smart devices' but 'manage them actively, just as you manage your phone.'

Mention the GDPR right to be forgotten and data minimisation - participants have legal tools available to them.

- Smart TVs: often collect viewing habits through Automatic Content Recognition (ACR), which identifies what you watch even from external devices. Many have integrated microphones for voice control that remain active unless manually disabled.
- Voice assistants: record short audio clips when they detect a wake word - and sometimes when they do not. These recordings are stored on remote servers and reviewed by human contractors in quality-improvement programmes.

- Connected toys and baby monitors: many use weak security (default passwords, unencrypted connections), meaning they can be accessed remotely if not properly secured.
- Cloud storage: most families have automatic cloud backup running on their phones without realising it. Photos, contacts, documents, and device settings are copied to remote servers linked to their Google or Apple account.

Key message: 'Under GDPR, you have the right to know what data your devices collect, the right to limit it, and the right to demand it be deleted. These are legal rights - not favours.'

Hands-on: Cloud & Smart Device Privacy Audit (10 min)

Trainer Note

This connects directly to the 'Device Mute Walk' and 'Invisible Audit' activities from Chapter III.

Focus on the two most universally owned devices: their smartphone and (if applicable) Smart TV.

Never ask participants to change settings they are not comfortable with. The goal is awareness.

On smartphones:

- Open Settings → Privacy → Location Services: identify which apps have 'Always On' location access and change to 'While Using' or 'Off' where appropriate.
- Open Settings → Privacy → Microphone: check which apps have microphone access and remove it from any app that does not need it.
- Check cloud backup status (iPhone: Settings → [Name] → iCloud; Android: Settings → Google → Backup). Are you aware of what is being backed up?

For Smart TVs (general guidance - no device required):

- Most Smart TVs have a Privacy or Data Sharing menu in Settings. Look for: Automatic Content Recognition (ACR), Voice Data Collection, Data Sharing with Third Parties.

- Disable ACR if found. Disable voice control microphone unless actively using it.
- Recommend running a brief check at home using the TV remote.

Activity: Draft a Family Digital Understanding (12 min)

Trainer Note

Use the Family Digital Understanding template on the flipchart or a printed sheet.

Emphasise that this is a collaborative document - children should be involved in writing it at home.

The parental clauses (rules that also apply to adults) are the most important element - they transform the contract from a list of restrictions into a family commitment.

Connect this to section 4.1 in Chapter III - the 'Family Drafting Session' activity.

Guide participants to complete the following four sections:

Section	Example Content
Screen-free times and zones	No devices at family meals. All devices charged outside bedrooms by 9:30 PM.
Security commitments	Always ask before downloading an app. Never share passwords outside the family. Report suspicious messages.
Reporting clause	If something uncomfortable, confusing or worrying happens online, we talk about it together - without punishment.
Parental clauses	Parents will not use phones during family time without explaining why. We apply the same rules to ourselves.

Invite 2–3 participants to share one item from their draft. Discuss: 'What makes this item realistic and enforceable?'

Discussion: What Makes a Digital Agreement Work? (8 min)

- Ask: 'What is the difference between rules imposed from above and rules drafted together?'
- Key insight from Chapter III: children are significantly more likely to respect boundaries they helped design. The agreement should be printed, signed by every family member, and displayed somewhere visible.
- Ask: 'What is the most important single rule you wrote today?' Let participants share. Note the variety - there is no single right answer.

Key Messages of the Module

1. Smart devices collect data passively and silently - managing their privacy settings is as important as managing your phone.
2. Cloud storage means your family's photos, contacts, and documents exist on remote servers. Review what is being backed up and who has access.
3. A Family Digital Understanding works best when children help design it. Rules built together are respected more than rules imposed alone.

Trainer Tips

- Do not frame this module as a reason to distrust technology - frame it as an invitation to manage it actively.
- The connected toy and baby monitor security issues can be raised briefly, but do not dwell on them - they risk creating disproportionate anxiety.
- Remind participants that GDPR gives them actionable rights: they can contact any service to request data deletion.
- Final message for participants: 'Your home is the safest place in the world for your family. Taking ten minutes to review your Smart TV's privacy settings and drafting a simple digital agreement today extends that safety to the digital dimension of your home.'

Module 7 - Parental Controls, Screen Time & Leading by Example (45 min)

↪ Correspondence with Part I: Sections 4.2–4.5 - 'Parental Controls within the European Regulatory Landscape', 'Monitoring vs. Spying', 'Managing Screen Time', 'Leading by Example'

Related Chapter	Sections 4.2–4.5 - Parental Controls, Monitoring vs. Spying, Screen Time, Adult Modelling
Duration	45 minutes
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, smartphones, Worksheet 15 (Monitoring or Spying?), flipchart, markers
Group Size	8–14 participants
Handouts	Worksheet 17 from the Parent Worksheets Booklet (Workshop 2, Module 7): W17 - Parental Controls: Monitoring, Not Spying (Ref. 4.2–4.3)

Learning Objectives

- The participant can configure at least one parental control feature on a family device during the session (Screen Time on iPhone or Digital Wellbeing on Android).
- The participant understands the operational and ethical distinction between transparent monitoring and covert spying, and can explain why covert surveillance is counterproductive.
- The participant applies age-appropriate screen time guidance and understands why blanket rules designed for young children do not work for teenagers.
- The participant recognises the concept of 'technoference' and identifies at least one concrete change in their own digital habits.

Session Plan

Time	Activity	Method	Materials
0:00– 0:08	Icebreaker: 'What Rules Exist at Home?'	Group discussion + flipchart	Flipchart, markers
0:08– 0:18	Hands-on: Configure a Parental Control Feature	Individual on devices	Smartphones
0:18– 0:28	Activity: Monitoring or Spying?	Small groups	Scenario cards
0:28– 0:38	Mini-lesson: Screen Time by Age + Leading by Example	Presentation + discussion	Projector
0:38– 0:48	Activity: The 'Device Basket' Challenge Planning	Individual reflection	Flipchart
0:48– 0:50	 Handout + Wrap-up	Individual	Worksheet 17

Detailed Activity Guide

Icebreaker: 'What Rules Exist at Home?' (8 min)

Trainer Note

Begin with offline rules - homework before TV, bedtime, family meals - before moving to digital rules.

The goal is to surface the gap: most families have clear offline rules and much vaguer digital ones.

Avoid framing this as a judgement. Many parents feel guilty about screen time - normalise the challenge.

- Ask: 'What rules already exist in your home?' Write answers on the flipchart. Expect: bedtime, homework first, family meals, chores.
- Ask: 'Do you have equally clear rules for smartphones, tablets, gaming, and social media?' Expect a much less confident response.
- Key insight: 'Most families have very clear offline rules and much vaguer digital ones. That is completely normal - digital devices are new, and the rules are still being worked out. Today we build them together.'

Hands-on: Configure a Parental Control Feature (10 min)



Trainer Note

Demonstrate live on a device shown on the projector. Keep the demo to one specific feature - Screen Time App Limits is the most universally accessible.

Participants follow on their own devices. Walk around and support those who need help.

Emphasise: the goal is not maximum restriction - it is informed, age-appropriate management.

iPhone - Screen Time:

- Settings → Screen Time → Turn On Screen Time.
- App Limits → Add Limit → select a category (e.g., Social Networking or Games) → set a daily limit (e.g., 1 hour).
- Create a Screen Time Passcode - different from the device passcode - so the child cannot change the settings.
- Downtime → set overnight hours (e.g., 9:30 PM to 7:00 AM) during which most apps are blocked.
- For full remote management: enable Family Sharing and link the child's Apple ID - settings can then be managed remotely from the parent's own device.

Android - Digital Wellbeing:

- Settings → Digital Wellbeing & Parental Controls.
- Tap an app → set a daily timer.
- For cross-device management: link to Google Family Link (families.google.com/familylink).

Remind participants: for the most robust setup, use Family Sharing (iPhone) or Google Family Link (Android) - this allows the parent to manage all settings remotely from their own device and covers all linked devices simultaneously.

Activity: Monitoring or Spying? (10 min)

Trainer Note

This is the most ethically charged activity of Workshop 2. Handle it with sensitivity.

The goal is not to make parents feel judged - it is to help them understand that transparency is both more ethical and more effective.

Reference the UCL research finding from Chapter III section 4.3: hidden monitoring apps often have worse security than transparent ones, ironically exposing the child's data to external hackers.

Groups receive scenario cards and must decide: is this Monitoring or Spying?

Scenario	Answer	Why
A parent installs Screen Time and shows their teenager exactly what data it records.	Monitoring	Transparent, educational, and the child is aware.
A parent installs a hidden app that logs all keystrokes and messages without telling the child.	Spying	Covert, excessive, damages trust - and often legally ambiguous.

Scenario	Answer	Why
Parents and child review the Screen Time weekly report together.	Monitoring	Collaborative, uses data as an educational tool, not a surveillance weapon.
A parent reads all of a teenager's private messages regularly without their knowledge.	Spying	Covert and disproportionate. Undermines the child's developing autonomy and trust.

Key message from Chapter III: 'Monitoring and spying differ not by the data they collect, but by the transparency of their application. A monitoring tool that the child knows about is a safety net. A hidden surveillance app is a trap - for trust, for the relationship, and often for the child's own data security.'

Mini-lesson: Screen Time by Age + Leading by Example (10 min)

Trainer Note

Keep the age guidance very brief - one sentence per age group. The detail is in Chapter III section 4.4.

The Leading by Example section tends to generate the most personal reflection. Give it space.

The 'technoference' concept does not need its name - describe the behaviour and let parents recognise it.

Screen time guidance by age (from Chapter III section 4.4):

- Under 2: avoid screens except video calling.
- 2–5 years: up to 1 hour of high-quality, co-viewed content per day.
- 6–12 years: balance digital use with offline responsibilities - impact on sleep, homework, and exercise matters more than a fixed limit.
- Teenagers: focus on self-regulation and habit formation, not hard limits. Protect sleep and discourage compulsive use patterns.

Leading by example - ask participants:

- 'When was the last time you checked your phone during a family meal or a conversation with your child?'
- 'How do you think your child interprets that?' - Guide toward: 'If adults can look at their phones whenever they want, why can't I?'

Key insight from Chapter III: 'Children do not learn digital discipline from rules. They learn it from what they observe at home every day. A parent who models healthy digital habits makes every other rule more believable.'

Activity: The 'Device Basket' Challenge Planning (10 min)

Trainer Note

This is a commitment-building exercise - participants plan to implement the 'Device Basket' activity from Chapter III section 4.5.

The key is that it applies to everyone - parents included. Emphasise this.

Ask participants to choose a specific, upcoming family moment to try it.

Ask participants to complete on paper:

- 'When will I try the Device Basket this week?' (e.g., Sunday dinner, Saturday afternoon activity.)
- 'Who will be involved?' (All family members, including parents.)
- 'What offline activity will we do during that time?' (Board game, cooking together, walk, reading.)
- 'What is the single rule I will commit to modelling myself?'

Invite 2–3 participants to share their plan. Ask: 'What do you expect the hardest part to be?' (Usually: their own phone habits, not the children's.)

Key Messages of the Module

1. Parental controls are a useful structural guardrail - but they work best when paired with open communication and transparency, not as hidden surveillance.
2. Screen time rules must evolve as children grow. Rules designed for a seven-year-old will not work - and may backfire - with a fifteen-year-old.
3. The most powerful parental control tool is adult behaviour. Children do not follow rules - they follow examples.

Trainer Tips

- Avoid recommending specific third-party parental control apps unless participants ask. Mention that Google Family Link and Apple Screen Time are built-in, free, and sufficient for most families.
- If a participant mentions wanting to spy on their teenager, respond gently: 'Many parents feel that way, and the worry is completely understandable. Research shows that transparent monitoring - where the teenager knows what is being tracked - is actually more effective at keeping them safe, because it preserves the trust that makes them come to you when something goes wrong.'
- Final message for participants: 'The most secure digital home is not the one with the most restrictions - it is the one where children feel safe to talk to their parents about anything that happens online.'

Module 8 - Online Risks for Children: from Cyberbullying to Digital Resilience (60 min)

↔ Correspondence with Part I: Section 5 - 'Risks to Which Children May Be Exposed Online'

Related Chapter	Section 5 - Cyberbullying, Grooming, Inappropriate Content, Gaming Scams, Digital Resilience
Duration	60 minutes (extended module)
Target Group	Parents with low/medium level of digital literacy (G2)
Materials	Projector/screen, Worksheet 17 (Warning Signs), Worksheet 19 (Role-Play scenario), flipchart, markers
Group Size	8–14 participants
Handouts	Worksheets 18–20 from the Parent Worksheets Booklet (Workshop 2, Module 8): W18 - Would You Notice the Warning Signs? (Ref. 5.1–5.2); W19 - Rabbit Holes & Gaming Scams; W20 - LISTEN–REASSURE–DOCUMENT–ACT (Ref. 5.5); W21 - My Family Digital Resilience Plan (Ref. 5.5)

Learning Objectives

- The participant recognises the four main online risk categories affecting children and their behavioural warning signs.
- The participant understands why children often do not disclose online problems - and what makes disclosure more likely.
- The participant practises the LISTEN - REASSURE - DOCUMENT - ACT response framework using realistic scenarios.

- The participant understands what digital resilience means: not the absence of online risk, but the confidence, knowledge, and family support to respond effectively when something goes wrong.

Session Plan

Time	Activity	Method	Materials
0:00–0:08	Icebreaker: 'Would You Notice?'	Group discussion + flipchart	Flipchart, markers
0:08–0:22	Activity: Risk Category Overview + Warning Signs Detective	Small groups + plenary	Scenario cards
0:22–0:30	Discussion: Why Don't Children Always Tell Us?	Guided discussion	Flipchart
0:30–0:47	Role-Play: The Parent Response (LISTEN–REASSURE–DOCUMENT–ACT)	Pairs	Role-play cards
0:47–0:55	Mini-lesson: Building Digital Resilience	Short presentation + discussion	Projector
0:55–1:00	 Handout + Wrap-up	Individual	Worksheets 18–20

Detailed Activity Guide

Icebreaker: 'Would You Notice?' (8 min)

Trainer Note

The goal is to surface the uncomfortable truth that online problems rarely announce themselves directly - they appear as behavioural changes.

Keep it empathetic. Many parents feel guilty about not having noticed warning signs sooner.

This exercise primes participants to think about behaviour rather than devices.

- Ask: 'If your child was experiencing a serious online problem right now, how would you know?' Write answers on the flipchart.
- Guide toward: mood changes, withdrawal, sudden anxiety around devices, avoiding school, changes in sleep, loss of interest in usual activities, secretiveness.
- Ask: 'Have you ever noticed a change in your child's behaviour that you could not explain at the time?' Allow brief, voluntary sharing.
- Conclude: 'Children do not usually say I am being bullied online. They show it in other ways. Recognising those signs is our first protective tool.'

Activity: Risk Category Overview + Warning Signs Detective (14 min)

Trainer Note

Present the four risk categories in two minutes total - this is an overview, not a lecture.

The Warning Signs Detective is the main activity: groups receive one scenario each and identify warning signs.

Avoid sensationalist language, especially for grooming. Focus on observable behaviours, not graphic scenarios.

Brief overview of the four main risk categories (2 min each):

Risk	Core Mechanism	Key Warning Signs
Cyberbullying	Peer harassment that follows the child into the home through their devices, 24/7.	Emotional volatility around notifications; reluctance to attend school; sudden withdrawal from activities; device shielding.
Grooming	An adult builds gradual trust with a child online, migrating them to private, unmonitored channels.	Secretive about a new 'online friend'; anxiety when device is away; adult vocabulary; unexplained gifts.
Inappropriate Content / Algorithmic Rabbit Holes	Recommendation algorithms progressively push extreme content.	Sudden shifts in language, views, or values; withdrawal from real-world relationships; changes in eating or appearance.
Gaming Scams & Dark Patterns	Predatory monetisation design and social manipulation inside games.	Rage or anxiety about missing limited-time events; requesting money urgently; treating gaming as a stressful obligation.

Warning Signs Detective (12 min):

Assign one scenario per group. Groups read it and identify: (1) which risk category this might be; (2) what specific warning signs are present; (3) what the parent should NOT do first.

Scenario	Details
A	A thirteen-year-old who used to love gaming with friends now panics every time his phone shows a notification and becomes furious when his parents touch his device.
B	A fifteen-year-old girl has started using adult terminology, become secretive about an online friend 'who really understands her', and has stopped spending time with her school friends.
C	A twelve-year-old who was calm and sociable has begun making comments at dinner about how 'certain people' are responsible for society's problems, using language his parents do not recognise.

Scenario	Details
D	A ten-year-old had a meltdown when a limited-time game character was taken down and has been asking to use a parent's credit card for 'just a small purchase' every few days.

Groups share findings. Summarise on the flipchart: one warning sign per scenario.

Discussion: Why Don't Children Always Tell Us? (8 min)

Trainer Note

This is the most emotionally sensitive discussion of the entire guide. Handle with care.

Do not ask participants to share specific incidents unless they volunteer.

The key insight - 'children come to us when they believe they will be heard, not judged' - should feel like a revelation, not a lecture.

- Ask: 'Why might a child hide an online problem from their parents?' Write all answers without comment.
- Common responses: fear of punishment, embarrassment, fear of losing device access, worry that parents will not understand, belief that it will get worse if they tell.
- Ask: 'Looking at this list - how many of these fears could we address by changing how we respond?'
- Key insight from Chapter III section 5.5: 'The first condition of resilience is trust. If a child knows that disclosure will be met with emotional support - not panic, not device confiscation - they are much more likely to come to us when something goes wrong.'
- Challenge: 'What is one thing you could say to your child today that would make them feel safer asking for help?' Invite a few volunteers.

Role-Play: The Parent Response - LISTEN–REASSURE–DOCUMENT–ACT (17 min)

Trainer Note

This is the most important practical activity of Workshop 2. Every participant should practise all four steps.

Pairs rotate: one plays the parent, one plays the child disclosing the problem.

After each scenario, ask the 'child' role: 'How did you feel during that conversation? Would you come back to that parent with another problem?'

Use the 'wrong version' and 'right version' contrast - this is very effective and used in Chapter 1 as well.

Introduce the four-step framework:

Step	What to do	What NOT to do
LISTEN	Allow the child to explain fully without interruption. Ask open questions: 'Can you show me?', 'When did this start?'	Do not interrupt, minimise, or immediately jump to solutions.
REASSURE	Show support and thank them for telling you. 'Thank you for coming to me. We will deal with this together. You did the right thing.'	Do not say: 'Why didn't you tell me sooner?', 'What did you do to provoke this?'
DOCUMENT	Save screenshots, preserve evidence. Do not delete harmful messages - they are legal evidence.	Do not immediately delete or report before preserving evidence.
ACT	Decide on next steps together: blocking the account, reporting to the platform, contacting the school, or involving authorities if necessary.	Do not act unilaterally without explaining to the child what you are doing and why.

Role-play scenarios (pairs choose one):

- 'Someone keeps sending me insulting messages in the class group chat and other people are laughing along.'

- 'A person I met in an online game says we are best friends and wants to move to a private app where we can talk just us two.'
- 'I clicked on a link that promised free game credits and now my account is acting strangely.'

After each role-play, ask the 'child' role: 'How did that conversation feel? Would you come back with another problem?' Then ask the 'parent' role: 'Which step was hardest?'

Mini-lesson: Building Digital Resilience (8 min)

Trainer Note

This is the closing mini-lesson of the entire guide. It should feel like an arrival, not a beginning.

Resilience is the key shift from this chapter: from passive protection (filters, rules) to active competence (knowing what to do when something goes wrong).

The three-layer model - Prevention, Response, Recovery - is the takeaway structure.

Introduce the concept from Chapter III section 5.5: 'Digital resilience is not the absence of online risk. No technical guardrail is foolproof. Resilience means knowing what to do next when something goes wrong - and having the confidence and family support to do it.'

The three-layer model:

- Prevention: age-appropriate settings, parental guidance, digital literacy. Reduces initial exposure.
- Response: clear reporting and support procedures. What to do when something happens.
- Recovery: discussion, reassurance, and practical lessons. Helps the child rebuild confidence and learn without shame.

A resilient child is one who:

- Knows exactly which adult to tell and how to save evidence.
- Understands that coming to a parent with an online problem will result in support, not punishment.
- Can identify when an online space is becoming emotionally unhealthy and knows how to step away.

Final insight: 'Technical controls matter - but they are only part of the solution. Children need the confidence, knowledge, and family support to act when those controls are not enough. That is what we have been building today.'

Key Messages of the Module

1. Online risks rarely announce themselves. They appear as changes in behaviour - and a parent who recognises those changes is the most effective safeguard.
2. Children come to us when they believe they will be heard, not judged. LISTEN - REASSURE - DOCUMENT - ACT.
3. Digital resilience means not the absence of risk, but the confidence and family support to respond effectively when something goes wrong.

Trainer Tips

- Avoid a 'specialist' tone in this module. You are not a psychologist or a law enforcement officer - you are a trainer presenting a framework that empowers parents.
- If a participant reveals a serious situation during the discussion, do not attempt to counsel them. Acknowledge it warmly and invite them to a private conversation after the workshop.
- Have the Safer Internet Centre helpline for your country ready to share: in Italy, it is Telefono Azzurro (19696) and the European Children's Helpline (116 111).
- Never delete harassment evidence before preserving screenshots. Remind this clearly.

- Final message for participants - Workshop 2: 'Technology changes constantly. But what children need has not changed: a trusted adult who listens, does not judge, and helps them move forward. That adult is you. Thank you for being here today.'

Workshop 2 Closing (15 min)

Objectives:

- Summarise both workshops with four key ideas.
- Final personal plan: 1–3 concrete actions for the coming month.
- Feedback and thanks.

Step by step:

- 'Four ideas I take home' (3 min): write on the flipchart: Update & Protect. Strong Keys. MFA. Pause & Think. Trusted Adult.
- 'One thing I will do for my family this week' (5 min): each participant shares one sentence.
- 30-day personal plan worksheet (3 min): 'What will I do in the next 30 days? (maximum 3 things).'
- Feedback form - Annex A (3 min).
- Thanks and Annex C (useful resources) printed for each person. (1 min)

Final message for participants - Workshop 2: 'Protecting your family online does not require technical expertise. It requires awareness, a few consistent habits, and - above all - a home where children feel safe to talk to you. You have all of those. Thank you for taking these steps with us.'

Annex A - Participant Feedback Form

Distribute at the end of each workshop. Anonymous. Maximum 5 minutes to complete.

1. How useful was this session for your everyday life?

1 2 3 4 5 (1 = not very useful; 5 = very useful)

2. What did you like most?

.....

.....

3. What would you have liked to discuss more?

.....

.....

4. One single security change you will make at home:

.....

5. Would you recommend this workshop to another parent?

☐ Yes ☐ No Why?

.....

6. Other comment or suggestion:

.....

.....

Annex B - Logistical Checklist for Trainers

One Week Before

- I have read the methodological guide and Chapter III in full.
- I have prepared 2–3 local examples for each module (local scam types, familiar platforms).
- I have reserved the room (with written confirmation) and checked seating arrangement.
- I have sent a reminder message to participants asking them to bring their smartphone and/or tablet.

48 Hours Before

- I have tested the Wi-Fi connection in the room.
- I have verified that the Parent Worksheets booklet has enough printed copies for every participant (Worksheets 1–21). All scenario activities are already included in the worksheets - no separate printed cards needed. For Module 5, I have the Cookie Banner slides ready (DEPART_Cookies_Slides.pptx).
- I have tested activating MFA on the platform I plan to demonstrate live.
- I have printed all worksheets (1 complete set per participant + 2 spare sets).
- I have printed Annex A (feedback) and Annex C (resources) for each participant.

On the Day of the Workshop

- I arrive 45 minutes early.
- I arrange the room in a U-shape or in groups of 3–4. Never in rows.
- I put on the tables: pens, name badges, folders with worksheets and Chapter III.
- I check projector, sound, and lighting.
- I prepare the flipchart pages that are pre-written (cover them until the right moment).
- I put out water and a small welcome platter.
- I check the internet connection.

After the Workshop

- I collect the feedback forms (anonymous).
- I note 3 things that worked well and 1 thing to improve.
- I send a short report (1 page) to the project coordinator within 48 hours.

Annex C - List of Useful Resources for Participants

Distribute at the end of Workshop 2. Maximum 1 A4 page, clearly printed.

Note: this list does not need to be memorised. Keep it at home and refer to it when a question arises.

Topic	Resources
Antivirus and device protection	Windows Security (built-in): open Settings → Windows Security. Google Play Protect (Android): open Play Store → Profile → Play Protect. Apple iOS: keep iOS updated – built-in protections are strong when current.
Passwords and MFA	Have I Been Pwned? (haveibeenpwned.com) - check if your email has been in a data breach. Bitwarden (bitwarden.com) - free, open-source password manager. Google Authenticator or Microsoft Authenticator - free authenticator apps.
Public Wi-Fi and VPNs	ProtonVPN (protonvpn.com) - free tier available. Always look for HTTPS (padlock) in the browser address bar before entering any personal information.
Smart home privacy	Your Smart TV Settings → Privacy or Data Sharing menu. Disable Automatic Content Recognition (ACR) and voice control microphone when not in use. Under GDPR, you have the right to request data deletion from any company: check the company's privacy policy for contact details.
Parental controls	Apple Screen Time: Settings → Screen Time. Google Family Link (families.google.com/familylink). Qustodio (qustodio.com) - third-party option for multi-device families.
Children's online safety helplines	Italy: Telefono Azzurro - 19696 (free, 24/7). European Children's Helpline - 116 111 (free). Save the Children online reporting: savethechildren.it. Cyberbullying report (Italy): Polizia Postale - commissariatodips.it.

Topic	Resources
Reporting cybercrime	Polizia Postale (Italy): commissariatodips.it . Your national cybercrime unit: check your country's police website. Platform reporting tools: use the 'Report' button within each app or website.

Annex D - Notes for Translators and National Adaptors

This guide was developed within the DEPART Erasmus+ project and is designed for use across six partner countries: Romania, Italy, Slovenia, Belgium, and Poland. When adapting for national delivery, please note the following:

- Replace country-specific examples where indicated: public service platforms (e.g., PagoPA for Italy, obywatel.gov.pl for Poland, eUprava for Slovenia), local scam types, and specific phishing scenarios should reflect the national context.
- The Parental Controls section (Module 7) references the European Digital Identity Wallet and the European Commission's age-verification prototype. Update the rollout status as the EUDI Wallet becomes operational in your country during 2026–2027.
- The legal references in Module 8 (cyberbullying legislation) should be reviewed against national law: France, Italy, and Ireland have specific cyberbullying legislation mentioned in Chapter III; verify whether equivalent provisions exist in your country.
- The helpline numbers in Annex C must be replaced with national equivalents. Italy-specific numbers are provided as the default.

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

Annex E - Parent Worksheets for Chapter III

21 Worksheets for Workshop 1 & Workshop 2

WORKSHOP 1

WORKSHEET 1

Antivirus: Real Alert or Scareware?

Ref. 1.1–1.2

Name: _____

Date: _____

Spot the difference

Your trainer is showing two pop-ups on screen. Circle what's suspicious.

CRITICAL SECURITY ALERT

Your device has been infected with 14 viruses! Click SCAN NOW or call: +1-800-FIX-VIRUS

 **This warning will expire in: 02:37**

Windows Security

Virus & threat protection update available. Your definitions are 3 days old. We recommend running a quick update.

[Update now](#) [Remind me later](#)

What seems wrong?

My scareware rule

If I see a scary pop-up, the FIRST thing I do is:

Quick device check

Open your phone now and tick what's true:

- ☐ My antivirus / Play Protect / Windows Security is active
- ☐ My device has no pending updates
- ☐ My screen lock (PIN, fingerprint, Face ID) is active
- ☐ I checked one app's camera/microphone permissions - and they made sense

 **One security habit I will start this week:**

WORKSHEET 2

Digital habits: Safe or Unsafe?

Ref. 1.3–1.4

Name: _____

Date: _____

The game - your group's answers

Decide together: safe or unsafe?

Scenario	Safe / Unsafe?
Download a free game from an unknown website	
Install an app from the official App Store or Play Store	
Pop-up: '57 viruses found! Click SCAN NOW!'	
The OS asks you to install a security update	
A calculator app requests access to contacts and microphone	

Built-in or extra protection?

Do you think we need to download extra "cleaner" or "antivirus" apps from internet pop-ups?

☐ Yes, to be safer ☐ No, built-in phone security is enough

Verifying Before Downloading

Looking at the table above, what is your family's number one golden rule to make sure a new download is official and safe?

Our download rule:

Talking to my child

If your child gets a frightening message saying their device is broken or infected:

Our family rule for scary messages will be:

 **One thing I learned today:**

WORKSHEET 3

Data Online: What Are We Sharing?

Ref. 3.1

Name: _____

Date: _____

'What would a stranger know?'

If a stranger saw your last month of social posts, what could they learn about your family?

Data sorting

Sort each type of information:

Information	Share publicly	Share carefully	Keep private
Full name + city	☐	☐	☐
Children's school name	☐	☐	☐
Holiday photos (while still away)	☐	☐	☐
Home address and postcode	☐	☐	☐
Professional job title or field of work	☐	☐	☐

The item that surprised me most:

 **One piece of information I will protect more carefully from now on:**



WORKSHEET 4

The Permission Check

Ref. 1.3–1.5

Name: _____

Date: _____

Right now, on your phone

Settings → Apps / Privacy → Permission Manager.

☐ Apps with Camera access: _____ Apps with Microphone access: _____

☐ I found at least one app I no longer use - I removed its permissions or deleted it.

☐ 'Find My Device' (or equivalent) is activated.

Tip: Group your apps into folders (e.g., by category) so it's easier to see what you actually use and delete what you don't need.

The app that surprised me most:

'Free' apps - the real cost

'When an app costs nothing, your children are not the customers - they are the product.'

One 'free' app my family uses, and what it might be collecting:

 **One thing I will change about how my family uses devices:**

Rank the Passwords

Ref. 2.1

Name: _____

Date: _____

Rank the passwords

Before seeing the answers, rank these from weakest (1) to strongest (4):

Password	My ranking	Why?
123456		
P@ssw0rd!		
Football22!		
BlueTrainRiverM0on.		

What makes a long passphrase stronger than a short one with symbols?

Build your 'Secret Story' passphrase

Leo (age 11) used a memory - a squirrel eating a blue popsicle - to build: BlueSquirrel8It!

My funny family memory:

My passphrase from it (add a number or irregular capitalisation to strengthen it):

 **My password rule from today onwards:**

The Password Reuse Trap

Ref. 2.2

Name: _____

Date: _____

The 'neighbourhood key'

Imagine every house on a street uses the exact same key. What happens if one is stolen?

How does this connect to using the same password on multiple accounts?

My account check

Do you reuse the same password anywhere? ☐ Yes ☐ No ☐ Not sure

Account	Unique password?	Update this week?
Primary email	☐ Yes ☐ No	☐
Banking	☐ Yes ☐ No	☐
Social media	☐ Yes ☐ No	☐
Google/ Iphone Account	☐ Yes ☐ No	☐

The account I will update FIRST:



One thing I understood about password reuse today:

WORKSHEET 7

Activating 2FA

Ref. 2.3

Name: _____

Date: _____

Why 2FA matters

If a password is like the key to your front door, 2FA acts as:

☐ A second deadbolt ☐ A security guard checking IDs ☐ A security camera.

The Master Account Upgrade

On your primary email: Security Settings → Two-Step Verification / 2FA. Tick as you go:

- ☐ I found the 2FA / Two-Step Verification section.
- ☐ I chose a method: ☐ SMS ☐ Authenticator App ☐ Passkey / biometric
- ☐ I completed activation and saved my recovery codes at home.

Unexpected Alert!



Sign-in

request

Someone is trying to access your email from a device you don't recognise.

[Approve] [Deny]

You safely tapped **Deny** and blocked the access. However, your account is still at risk until you do one more essential thing.

What is your immediate next step?



One thing I learned today:

WORKSHEET 8

Password Managers: My Digital Vault

Ref. 2.4–2.5

Name: _____

Date: _____

Starting my Digital Vault

Have you ever heard of a password manager?

☐ Yes, I use one ☐ Yes, but I've never used one ☐ No, never heard of it

☐ I set a Master Passphrase using the 'Secret Story' method.

☐ I saved at least one account into the vault.

Now let's set one up, step by step:

☐ Step 1 - Choose one: Bitwarden / your phone's built-in manager (Passwords app / Google) /

Other: _____

☐ Step 2 - Download it, if you don't have it yet.

☐ Step 3 - Open it and create your Master Passphrase using the 'Secret Story' method.

☐ Step 4 - Save at least one account into the vault.

The ONE thing I must never forget when using it:

Teaching my child their 'Secret Key'

Like Leo's 'BlueSquirrel8It!' - what memory could my child use for their first passphrase?



The digital security habit I will teach my child first:

WORKSHEET 9

Phishing: Spot the Fake

Ref. 3.2

Name: _____

Date: _____

Phishing - your group's answers

For each message, find the warning signs:

Message	Red flags I found
Email: bank suspension warning Your bank account has been suspended due to suspicious activity. Verify your access immediately: <i>secure-bank-login-update.com</i>	
SMS: delivery fee request Your package is held at the depot due to an unpaid €1.99 delivery fee. Click here to clear it: <i>bit.ly/post-delivery-update</i>	
WhatsApp: IT support login request	

Message	Red flags I found
Hello, this is IT Support. We detected a security breach on your account. To secure it, reply with the 6-digit verification code you just received.	

The 'Go to the Source' rule

Instead of clicking a link in an alarming message, what do I do?

 **One thing I learned today:**

 WORKSHEET 10

My Workshop 1 Action Plan

Name: _____

Date: _____

What I commit to this week

- ☐ Update all devices and verify antivirus / Play Protect is active.
- ☐ Create a unique 'Secret Story' passphrase for my email.
- ☐ Activate 2FA on at least one key account.
- ☐ Check what I share publicly on social media.
- ☐ Teach my child the 'Secret Story' game.

One conversation I will have at home

The one security tip I want to pass on:

Looking back at today

Which of the four modules will be hardest to actually put into practice - and why?

 **My single most important security commitment from Workshop 1:**

WORKSHOP 2

WORKSHEET 11

Public Wi-Fi and VPNs

Name: _____

Date: _____

The Wi-Fi Twin Trap

Look at the networks visible at the airport. Which one looks like an "Evil Twin" trap?

 Airport_Official_Gate4

 FREE_HIGH_SPEED_AIRPORT_WIFI

 Free_Airport_WiFi

The Real Risk Check:

You click to connect and you are asked to: *"Log in with your Google Account to verify your identity"*. What just happened there?

☐ It's a standard security check by the airport provider.

☐ It's a Phishing Trap.

Wi-Fi Risk Map - my group's answers

Scenario	Risk level
Watching YouTube on café Wi-Fi	☐ Low ☐ Medium ☐ High
Checking bank balance on airport Wi-Fi	☐ Low ☐ Medium ☐ High
Leaving AirDrop (Apple) or Quick Share (Android) set to "Everyone" while waiting at the hotel lobby.	☐ Low ☐ Medium ☐ High

The Hotspot Check

Open your Wi-Fi settings now:

- ☐ I found and removed at least one old public network ('Forget This Network').
- ☐ My phone does not auto-connect to unknown networks.
- ☐ I will change my phone's Personal Hotspot password to a strong, custom one.
- ☐ I will update my home Wi-Fi password.

WORKSHEET 12

HTTPS: The Padlock Inspection

Ref. 3.5

Name: _____

Date: _____

HTTP vs. HTTPS

HTTPS means the connection is encrypted. Does it also mean the website is trustworthy?

Check three websites you use

Website	Has padlock + HTTPS?	URL looks correct?
	☐ Yes ☐ No	☐ Yes ☐ No
	☐ Yes ☐ No	☐ Yes ☐ No
	☐ Yes ☐ No	☐ Yes ☐ No

Before entering personal data on any website, I will always:

 **One thing I learned today about website safety:**

WORKSHEET 13

Cookies: Our Digital Footprints

Ref. 3.1

Name: _____

Date: _____

The Cookie Banner

You visit a website for the first time. Before you can continue, a message appears on the screen.

This website uses cookies

We use cookies to improve your browsing experience, personalise content and analyse website traffic.

what do you usually click?

☐ Accept All (Fast, but shares everything) ☐ Reject All / Manage Preferences

Have you ever clicked "**Accept All**" without reading the message?

☐ Yes

☐ No

If yes, why?

The Hidden Trap: Think About It!

Scenario: To watch the video, a website asks to install a cookie.

- If you **block** it, the video won't play.
- If you **accept** it, you are being tracked even after you leave the website.

What is the real risk here?

What would you do?

- ☐ Block it. My privacy is worth more than a video.
- ☐ Accept it. I just want to watch the video, even if they track me.

Which cookies would you keep?

Read the list below and tick only the cookies you think are necessary.

- ☐ Remember my shopping cart
- ☐ Save my language preferences
- ☐ Measure website visits

☐ Personalised advertising

☐ Keep me logged in during this session

 **One thing I will pay attention to:**

 WORKSHEET 14

Smart Device: The 'Device Mute' Walk

Ref. 3.4

Name: _____

Date: _____

Walk around your home

Identify every device with a microphone or camera, and check it:

Device	Has mic/camera?	Privacy checked?
Smart TV	☐	☐ Yes ☐ No

Device	Has mic/camera?	Privacy checked?
Voice assistant	☐	☐ Yes ☐ No
Baby monitor / cam	☐	☐ Yes ☐ No
Laptop webcam	☐	☐ Yes ☐ No

Cloud backup - what's being saved?

Open your phone's cloud settings

(iPhone: Settings → [Name] → iCloud; Android: Settings → Google → Backup). Look at what's listed.

One thing you didn't know was being backed up:

One thing you would want to delete from the back up?



The smart device setting I will review this week:

The 'Device Basket' Challenge

Ref. 4.4–4.5

Name: _____

Date: _____

My honest check

Do I check my phone during family meals or while my child is talking to me?

☐ Often ☐ Sometimes ☐ Rarely

The Device Basket Challenge

Every family member - parents included - puts their device in a basket for 2 hours.

When will I try this?

What offline activity will we do instead?

 **The digital habit I will change first - and why:**

WORKSHEET 16

Ref. 4.1

Our Family Digital Understanding

Name: _____

Date: _____

Complete this together with your family.

- | Where | We | Keep | Devices |
|--|-----------------------|-------------------|----------------|
| ☐ Phones | charge in the kitchen | overnight, not in | bedrooms. |
| ☐ No | devices at the table | when we eat | together. |
| ☐ Tablets and laptops stay in shared spaces, not behind closed doors. | | | |

Our security commitments

- ☐ We always ask a parent before downloading an app or game or browser extension.
- ☐ We never share passwords or 2FA recovery codes outside the family.
- ☐ We report suspicious messages before clicking.
- ☐ We only make purchases with a parent's knowledge and consent.
- ☐ We never share home address or school name online with strangers.

Parental commitments - rules that apply to adults too

- ☐ We will not use phones during family time without explaining why.
- ☐ We apply the same screen time rules to ourselves.
- ☐ Our rule for us: _____

Proposed by our child: _____



The most important rule in our Family Digital Understanding:

Parental Controls: Monitoring, Invasion of Privacy

Ref. 4.2–4.3

Name: _____

Date: _____

What I set up today

Talk to your children and tell them *before* you install any parental controls.

iPhone: Screen Time → App Limits → Passcode → Downtime.

Android: Digital Wellbeing → daily timer.

Feature I configured: _____

Monitoring or Invasion?

Scenario	Monitoring or Spying?
Parent installs Screen Time and shows the teenager exactly what it records	
Parent installs a hidden app that logs all keystrokes without telling the child	

Scenario	Monitoring or Spying?
Parent reads their 12-year-old's private WhatsApp chats because they noticed a sudden change in their mood	
Parent takes the child's phone while they are asleep and scrolls through everything just to check.	
Parent uses location tracking to check if their teenager actually went to the library after school.	
Parent sits with their 10-year-old once a week to review together the new apps or games downloaded	

What I will tell my child about the tools I use on their device:

 **The parental control feature that will make the most difference in my home:**

Cyberbullying: Would You Notice the Warning Signs?

Ref. 5.1–5.2

Name: _____

Date: _____

Imagine that your child is facing a serious problem online (like cyberbullying or grooming) but is too afraid or ashamed to tell you. They are trying to hide it. How would you notice?

Warning signs

Look at their mood, sleep, or school attitude. What changes would alarm you first?

Look at how they interact with their screen. What strange device habits might jump out?

Scenario analysis

Scenario my group analysed:

Warning signs present - and what a parent should do FIRST:

 **The warning sign I had never thought about before today:**

Gaming Scams and Rabbit Holes

Ref. 5.3–5.4

Name: _____

Date: _____

The algorithmic rabbit hole

A teenager searched for home workouts; autoplay pushed him into increasingly extreme content over weeks. Warning signs of this drift:

The '5-Minute Game & Store Check'

Step 1: Explore without judgment.

Sit with your child, open their favourite game, and ask them to show you around. Let them explain how it works, what they love about it, and who they play with. Just listen and learn!

Step 2: Check the shop together.

Go to the in-game store. Most expensive item: _____ Price in real money: _____

How many hours of real-world work does this represent?

What I will tell my child if a player offers a free in-game gift:

 **One thing I will discuss with my child about gaming this week:**

LISTEN - REASSURE - DOCUMENT - ACT

Ref. 5.5

Name: _____

Date: _____

My role-play notes

Scenario: "My child comes to me looking upset and says: 'Something happened online and I don't know what to do' They haven't told me what yet"

Step	What I said / did
 LISTEN	
 REASSURE	
 DOCUMENT	
 ACT	

Which step do you think is the hardest - and why?

Why don't children always tell us?

What emerged in discussion - and one thing I could say to make my child feel safer asking for help:

 **The sentence I will say to my child to make them feel safe telling me:**

My Family Digital Resilience Plan

Ref. 5.5

Name: _____

Date: _____

Phase	What I will actually do
Prevention - reduce initial exposure	
Response - what to do when something happens	
Recovery - rebuild trust after an incident	

Conversation starters for this week

- ☐ 'What would you do if someone sent you a mean message online?'
- ☐ 'Do you know how to block someone on the apps you use?'
- ☐ 'If something worrying happened online, would you feel safe telling me?'
- ☐ 'If you saw someone being cyberbullied or sharing something inappropriate online, how would that make you feel?'

Use at the end of Workshop 2 or distribute as a take-home evaluation. Not part of the standard workshop flow.

WORKSHEET 22

(optional)

How Digitally Safe Is My Family? - Self-Assessment

Name: _____

Date: _____

Part 1 - Device Security (from Chapter III, section 7)

Tick every statement that is true for your family today:

- ☐ All devices in our home have up-to-date antivirus protection or built-in security software active.
- ☐ All devices are set to receive automatic system updates.
- ☐ All devices have a screen lock (PIN, password, fingerprint, or Face ID) activated.
- ☐ I know the difference between a real security alert and a scareware pop-up.
- ☐ I only download apps from official stores (Google Play, App Store).
- ☐ I regularly review and remove app permissions that are no longer necessary.

Part 2 - Passwords and Authentication

- ☐ I use a strong, unique passphrase for my primary email account.
- ☐ I do not reuse the same password across multiple accounts.
- ☐ I have activated Multi-Factor Authentication (2FA) on at least one key account.

- ☐ I know what to do if I receive an unexpected 2FA request I did not initiate.
- ☐ I have explored or set up a password manager.

Part 3 - Data and Network Safety

- ☐ I know which types of personal data to keep private and which are safer to share.
- ☐ I read cookie consent banners before accepting - I do not just click 'Accept All'.
- ☐ I can recognise the warning signs of a phishing message.
- ☐ I apply the 'Go to the Source' rule when I receive alarming messages.
- ☐ I understand the risks of public Wi-Fi and protect myself with a VPN when needed.
- ☐ I check the HTTPS padlock and the full URL before entering personal data on a website.

Part 4 - Protecting My Family

- ☐ I have reviewed the privacy settings on our Smart TV and voice assistants.
- ☐ I know what our cloud backup contains and who has access to it.
- ☐ My family has a written digital agreement with clear rules everyone knows.
- ☐ I have configured parental controls on my child's device.
- ☐ I know the warning signs that a child may be experiencing an online problem.
- ☐ My child knows they can come to me with any online problem without fear of punishment.
- ☐ I know the LISTEN–REASSURE–DOCUMENT–ACT response framework.

My score

Total ticked:	/ 23	
---------------	------	--

19–23 	Your family is well protected. Focus on maintaining and updating your habits.	
13–18 	Good progress! Choose 3 gaps from above and address them this month.	
Under 13 	You have taken important first steps. Go back through the workshop materials and set a 30-day plan.	

The 3 areas where I will focus my energy over the next 30 days:

1. _____
2. _____
3. _____

 **The single most important change I have made for my family's digital safety:**
