

Media literacy program and material for adult educators

THEME 5: SAFETY AND PRIVACY



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

This intellectual output has been conceived and developed by the Strategic Partnership in APRICOT project under the coordination and responsibility of *Šiuolaikinių didaktikų centras/ Modern Didactics Centre* (LT).

Thanks to all partners for their precious contributes:

Apricot Training Management Ltd. (UK)

ItF Institut Kassel e.V. – Frauencomputerschule (DE)

Planeta Ciencias (ES)

Editorial coordinator: Daiva Penkauskienė

Authors: Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė

Editorial Board: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė



This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Month/ Year: November 2021

Chapter 6: Theme 5: Safety & privacy

6.1 Introduction into the theme

Security & privacy on the web

The aim of this module is to discuss the topic of security and privacy on the Internet, to know the dangers and how they can be avoided or reduced. In order to do this, the technical measures that should be taken are shown and the critical handling of private data and data protection on the Internet is explained.

Become an adult educator/ trainer:

- know the difference between security and privacy;
- get to know the most important issues and apply them in practical tasks;
- know how to better protect their security and privacy on the internet;
- learn how to search the internet safely;
- learn to recognise and avoid dangers on the Internet;
- learn to navigate social media and protect their private data;
- learn how to deal with personal attacks and cyberbullying.

How it works

- The learning is based on CEA approach and ERR framework (evocation/realization of meaning/reflection);
- The learning employs interactive lecture, individual, pair and group work, variety of strategies and methods;
- The duration of delivery of this theme is 6 hours.

Table 8. Overview of the theme

Learning objectives	Content	Activities / Methods	Material	Duration	Learning outcomes
To present & discuss main concepts of the theme	Introduction to the theme: Understanding protecting security and privacy	Lecture through presentation, "Introduction to the theme Safety and Privacy.pptx" clear the head 6-3-5-method,	Multimedia, Flipchart, markers	1,5 hour	Difference between security and privacy; Overview of the sub-theme

Learning objectives	Content	Activities / Methods	Material	Duration	Learning outcomes
		group discussion			
	Sub-theme 1 Overview of current antivirus programs, tasks of antivirus-program, security settings in browsers	Lecture through presentation "Technical possibilities.pptx" refresh body and mind, K-W-L, joint analysis, online research	Multimedia Flipchart, markers	1,5 hours	critical review of antivirus software; important security settings in the Browser
	Sub-theme 2 Recognize reputable websites, recognizing and avoiding dangers	Lecture through presentation "Serious surfing behavior.pptx" exchange market; joint analysis and group discussions	Multimedia (Projector) Handout, Worksheets, Flipchart, markers	1,5 hours	critical review of websites; recognize characteristics of trustworthy websites
	Sub-theme 3 personal attacks; cyberbullying; Protection in online social networks; protecting own data; protecting emails;	Lecture through presentation "Protection on internet.pptx" atom-molecule-discussion	Multimedia (Projector) Handout, Worksheets, Flipchart, markers	1,5 hours	Personal safety on the Internet

Understanding protecting security and privacy

No matter whether on the notebook, smartphone or tablet, people surf the internet on a daily basis. Internet World Stats [1] estimates that the number of Internet users in Europe in 2018 was around 727.6 million. A review of data on internet use [1] for project partners gave the following results in percentage of the population:

- United Kingdom 95%
- Germany 92%
- Spain 86%
- Lithuania 80%

But how safe are these users on the internet?

The first issue that must be addressed is the difference between privacy and security.

Privacy is the ability to protect sensitive, personally identifiable information. Your privacy on the Internet depends on how much personal information you publish and who has access to this information.

The first step to protect privacy is security. Every user needs to actively participate in data protection. It includes:

- Read privacy statements before sharing personal information.
- Take proactive security measures against viruses, malware and phishing.

As soon as the user enters the World Wide Web, privacy is too often neglected. Internet security should be taken very seriously these days. Many consumers and companies willingly share their information on social media. The same applies to cell phone data, loyalty retail cards, credit cards, iWallets, transport services and the like. Convenience and consumer behaviour can seem to have far more influence on how we handle our personal data than security concerns.

In the digital age, being online is very important for our children, but when they use the internet they can leave traces and willingly disclose personal data.

Protecting personal information on the web – The Internet never forgets!

Everyone who uses the Internet should protect their privacy and personal data. Every user can fall victim to crime on the Internet. Without exception! There are many measures today that can be easily taken to improve our online privacy and security. The following section sets out these measures.

In the individual topics, we provide links that offer current information on these topics. Due to the fast pace of the Internet, we can only name the technical options that are up to date at the time of this document's creation. You should keep yourself regularly informed on the latest developments on internet safety and security, in order to pass this information on to children / grandchildren.

In this chapter we would like to explain security measures and protection options, e.g.

- What are the technical possibilities?
- How do I surf the internet safely?
- How do I protect my personal data?
- How do I protect myself on social media networks?
- How do I cope with personal attacks and cyberbullying?
- How can I recognise dangers and avoid them?

Part I. Presentation of Model Activity

Step 1. WARM-UP

The workshop participants are involved in 5 minutes warm-up-activity „clear the head“ [2]. After it, the session leader introduces the goal of the session & shortly describes what will happen during it.

The procedure

You can perform this activity indoors or outdoors. It is suitable for an unlimited number of participants. Background music is recommended.

Ask the group to move freely through the room; everyone should speak individually about what has happened in their everyday life since 8 p.m. last night until the start of the seminar.

This exercise can also be a way for you as a moderator/ trainer/ seminar leader to focus on the work ahead.

The method is ideal for warming up in the morning, before the event begins in order to get the head clear.

Step 2

Preparation:

Worksheet: 6-3-5 Method

Theme: Security and privacy on the internet

Create a worksheet in a word processing program according to the picture above. You need one worksheet for each participant.

Task 1: Participants are asked to write down their knowledge or questions about security and privacy on the Internet. The 6-3-5 method [3] is used.

For this task, the participants are divided into groups of 6 people. Each participant receives a sheet with 3 columns and 6 rows.

The procedure

Each participant writes 3 ideas on this subject on the paper in front of them. These should differ from each other and approach the question from as different perspectives as possible.

The notes are passed on five times until each participant has had every list once in front of them.

When the sheets are passed on, everyone receives a list with three different ideas/knowledge. In the next line, these ideas are continued with your own thoughts and knowledge. In this way, the existing ideas are taken up, expanded and refined.

This is repeated until the pieces of paper have been passed on a total of five times and everyone has had the opportunity to give their input on each existing idea.

The task is limited to five minutes.

Task 2: Summary of the ideas / opinions by category in a group discussion. Set the categories according to the entries of the participants. Possible categories are:

- technical possibilities
- internet surfing techniques
- privacy

Part II. Analysis of the Process

1. In the group, summarise the ideas / opinions of the participants on the following questions.
What is security?
What is privacy?
2. Ask the following questions to the group:
How do you protect yourself in the digital world?
Before you enter your personal data, do you think about what private data you are providing?
Are you aware of the possible consequences of this data?

Part III. Planning for Implementation

The trainer divides participants into small groups and asks them to develop an activity that parents/grandparents can do with their children to explain the importance of privacy. The following questions should be considered:

- What kind of website / social network is it?
- Is this a secure site?
- What personal data can I provide on this website?
- Why do I enter personal data? Is this really necessary?
- Which ones should I not disclose under any circumstances?

Possible adaptations

Trainers can also use other methods to collect ideas / ask questions.

The 6-3-5 method described above is well suited if the participants are somewhat closed or reserved.

If the group consists of open-minded participants, brainstorming / mind-mapping is also a very good method. For both methods, it is recommended to note the results on the blackboard or on a flipchart.

Let the group answer the questions that have been recorded by the participants. Join the discussion only if the question is not being discussed by any of the participants.

Additional adaptations for disadvantaged groups

For socially disadvantaged parents/grandparents the 6-3-5 method should be used for a little longer, e.g. 10 minutes.

Adapt your language and explanations as appropriate, to the group of participants you are working with, in order to ensure understanding and engagement with the course. Speak a simple language to socially disadvantaged groups so that everyone has the opportunity to follow the course.

6.2 Technical possibilities

Important general information

Data security includes technical measures that serve to protect all possible data. The following goals are pursued in data security: confidentiality, integrity and availability of the data. In contrast to data protection, data security is not limited to personal data. This section explains the possible technical measures that can be taken to increase data security. These measures are various control mechanisms which are intended to prevent

unauthorized access and thus also knowledge, manipulation or removal of the data. See more in the Annex 4.

Part I. Presentation of Model Activity

Step 1. WARM UP

The goal of this warm-up is to refresh the body and mind.

Procedure:

A person starts to make quiet noises by rubbing their hands together. The next person waits a few seconds and then also begins to rub their hands, then the next person and so on.

When the last person starts rubbing their hands, the first person starts with a new sound, e.g. finger snapping. Again people follow one after the other and the new sound replaces the first one.

The order of sounds:

- Rubbing your hands
- Finger snapping
- Clapping your hands on your thighs
- Clapping your hands
- Clapping your hands on your thighs
- Finger snapping
- Rubbing your hands

The volume of the sounds will become louder and then softer again.

Step 2

Taks 1: The trainer introduces the topic to the participants using a presentation (see Chapter 10 Presentation: Technical possibilities).

Task 2: Participants will be asked which anti-virus programs they use and what experiences they have had with them. The results will be noted and evaluated together.

Task 3: Each participant receives a K-W-L (Know - Would like to know - Learned) sheet (Ogle, 1986). The participants fill in the first and second columns. In the first column, they enter what they know about Parental Control on the Internet and in the second column, what questions they have about the topic.

KNOW	WOULD LIKE TO KNOW	LEARNED

Step 3

Joint analysis of the sheet. If needed, online research can be conducted on the topics in the "would like to know" column.

It is recommended to limit the time of task 2 and task 3.

After filling out the K-W-L sheet, a participant starts with the first point she/he wants to know. The other participants try to answer the question. The trainer will intervene only if no participant can clarify the point. The participants are given 1-3 minutes to update their K-W-L-sheet.

Part II. Analysis of the Process

Analysis of the K-W-L sheets in the group discussion:

- What new information did the participants learn from the presentation?
- Which points do you consider as very important?
- Analysis of the current settings of your hardware and software. For example, the security settings in your browser and on the social networks you use.
- Which changes do you consider important for your system?

Part III. Planning for Implementation

Participants brainstorm in small groups and develop a step-by-step guide to the settings parents/grandparents should make on their systems, both in terms of hardware and software.

Afterwards, the instructions from the entire group are combined into a complete manual.

Possible adaptations

If computers with internet access are allowed to be used during the course, it is also possible to research the questions online. This has the advantage that the participants can learn research techniques and thus in the future quickly get the desired information. This reduces the time spent in front of the screen in the future.

Additional adaptations for disadvantaged groups

For groups of socially disadvantaged parents/grandparents, some of the work should definitely be done with computers. Here they should deal with the possibilities of parental control on computers / smartphones.

6.3 Serious surfing behaviour

Important general information

It is well known that from a little data a lot can be read about Internet users. Information can be obtained from online activity, not just in regards to someone's identity and personal data, but also with regards to online behaviour, physical and psychological conditions and other aspects of people's personalities.

Scientists have shown that insights into personality traits can be gained not only from the use of social networks such as Facebook or Twitter, but also from regular internet use, such as information searches and purchases. Many users think they are anonymous in cyberspace - unfortunately, this is a fallacy. The Internet is a space for seamless surveillance.

It is difficult to examine an internet source for its completeness and credibility. However, there are some clues that you can look out for that quickly point to how trustworthy an Internet source is. See more in Annex 5.

Part I. Presentation of Model Activity

Step 1

The idea for this activity is based on the elaboration of the activity "exchange market" [4] by Manfred Bieschke-Behm.

The exchange market implies that you give away what you have too much of and get from others what you have too little of, or do not have at all.

Preparation: Several small tables, each with a chair in front and a chair behind, mark the market stalls. On a separate table there are presentation cards in two different colours and pens. Decide beforehand which colour is to be used for which theme. The themes are: "How to recognise reputable websites" and "How to recognise dangers on the Internet".

Implementation: Before the swap transactions begin, the participants write on the moderation cards their knowledge on the topic "How to recognise reputable websites" and "How to recognise dangers on the Internet" and their name. One dot is written on each moderation card. Those who have something to "sell" sit down at a table and spread out their "barter objects".

The potential buyers go from table to table and find out what is on offer and if there is something lucrative for them. The "seller" asks the "customer" what they have to offer in return.

Note: In the context of "price negotiations", the question of "quantity" must also be clarified. Prerequisite: it is not a 1:1 swap transaction. For example, the "seller" is only willing to give

the "buyer" 1 card of his "knowledge" about "How do I recognise reputable websites" if he gets 2 cards about "How do I recognise dangers on the Internet" in return. If the "business partners" agree to trade, the labeled moderation cards change hands. Every "buyer" has the possibility to approach other sales stands to increase his demand there.

Note on the procedure: Not every "customer" leaves the exchange market with a "purchase". For some the "price" is too high. Also, the "seller" may refuse a barter trade, e.g. if the responsibility for a decision is to be transferred to them in this way. In all phases of this exercise, previously unknown experiences are identified and insights are gathered.

Note 1: It is possible to switch roles. The "seller" becomes the "buyer" and vice versa.

Note 2: open the exchange market for a limited time only.

Note 3: The exchange market can be used universally. It can take place at the beginning as a "warm-up", at the end of an event, as well as a focus of a meeting.

Step 2

Task 1: The moderation cards to the topic are pinned and it is determined who has what knowledge.

Task 2: The evaluation is used as a basis and the trainers pass on their knowledge to the whole group. For this purpose, a trainer from the group is assigned to moderate the meeting.

Step 3

Discuss with your participants the question: "What do you understand by serious surfing behavior?"

Give your participants the 10 points about the topic "Characteristics of a reputable Internet source" to read through. See the 10 identifying features in Annex 6, "1. Features of a reliable internet source". Ask your participants whether or not they pay attention to these points when using the internet.

Let the participants note down the points in their own words to internalize them.

In the case of socially disadvantaged groups, it is advisable to discuss the points together in the group, possibly showing these characteristics online.

Discuss the concept of media literacy for parents / grandparents.

See for further information chapter 9, appendix 1. "Media Literacy for Clinicians and Parents". You will find three different age groups.

Part I: How young children perceive and use media

Part II: Preschool years

Part III: How school age children and adolescents perceive and use media

Part II. Analysis of the Process

- What do you think about the activity "exchange market"?
- Can this activity be done with parents / grandparents?
- Can parents / grandparents carry out this activity in the same or a similar way with their children / grandchildren?

Part III. Planning for Implementation

The participants work in small groups on an activity for parents/grandparents, discussing appropriate suggestions for and answers to the following questions:

- How does my child / grandchild recognise a secure site?
- How can I sensitise my child / grandchild to dangers of the Internet?
- How can I show my child / grandchild the dangers of the Internet?

Possible adaptations

Trainers can also use other activities instead of "Exchange market" that they consider useful, such as a questionnaire with click the box questions.

Possible questions and answers are, e.g.:

Question:

When using a search engine, what does the order in which search results appear, suggest about the web pages ? What does the result of a search engine say when searching for a term?

Possible answers:

1. The order has no meaning.
2. The first results are those that had the most visitors.
3. The first results are secure pages.

(correct answer: 2)

Question:

The desired website is open. How can you tell if the site is secure or not?

Possible answers:

1. The address starts with http.
2. A lock is shown in front of the address.
3. There are many advertisements on the website.

(correct answer: 2)

Question:

Are you allowed to download pictures, music, text, movies, etc.?

Possible answers:

1. Yes, I am allowed to download everything without hesitation, as they are accessible to everyone.
 2. No, I am not allowed to do it, because they are all under copyright.
 3. Yes, I may download everything that is released and used for private purposes only.
- (correct answer: 3)

Additional adaptations for disadvantaged groups

With socially disadvantaged groups it is advisable to discuss the points together in the group, possibly show these characteristics online.

6.4 Secure use of social networks

Important general information

Private use of online social networks allows you to talk, share photos and videos with family, friends and colleagues. However, the dangers of social media networks should not be underestimated, such as identity theft or spying on private information. In the following activity, you will get some security tips [5] (see more in Annex 6: Secure use of social networks).

Part I. Presentation of Model Activity

Step 1. WARM UP

Atom-molecule-discussion [6]

This method is designed so that participants write down questions about a previously selected topic, such as rights and responsibilities on the internet or cyberbullying, in groups of increasing size.

At the beginning the whole group is divided into pairs - each pair sits down somewhere in the room and talks for about 5 minutes about the agreed topic. After this time the trainer gives an agreed signal and the pairs find a second pair and talk to each other again for about 5 minutes. Then each group of four looks for another group of four and talks about the topic for another 10 minutes.

Note: This activity is most suitable for larger groups. For smaller groups, you can stop after the second round (group of four).

Step 2

Task 1: Each group of eight (group of four) should then summarise their questions on the topic in 5 minutes and agree on a group speaker.

Task 2: Afterwards the group speakers will present the questions. The questions collected in this way are noted on a flipchart or digitally.

Step 3

The catalog of questions from Step 2 will be answered in a joint group discussion.

The participants report which (negative) experiences they have had and what they have done about it.

Groups will discuss the selected topic. If they chose the topic of cyberbullying participants may not be willing to share their experiences due to the sensitive nature of this issue. In this case, you can also develop an anonymous questionnaire as a basis for discussion. To create a list of questions, you can use the information from Annex 6: Secure use of social network, subchapter "Cyberbullying".

Part II. Analysis of the Process

We ask the participants to sit in a circle and give feedback on the activity performed.

- What did they like about this activity?
- Did this activity make them more aware of the topic?
- What did they not like?
- Would they suggest any other activities?

Part III. Planning for Implementation

We bring the participants together in small groups and ask them to develop other possible activities that are also suitable for parents and grandparents, which they in turn can do with their children / grandchildren.

Possible adaptations

Cyberbullying is a very sensitive topic that many people do not want to talk about. To be able to discuss this topic with parents and grandparents, an anonymous survey would be one possibility.

For this purpose, a questionnaire can be developed in small groups and then an overall questionnaire produced.

Additional adaptations for disadvantaged groups

This questionnaire should be easy to understand for socially disadvantaged people.

Together as a team, the best way to explain the issues raised to socially disadvantaged groups should be considered..

References

- [1] <https://de.statista.com/statistik/daten/studie/39490/umfrage/anzahl-der-internetnutzer-weltweit-nach-regionen/> from 18.05.2020
- [2] Worksheet von Christina Achner
<https://www.beltz.de/fileadmin/beltz/leseproben/9783407364517.pdf> (page 139) from 04.05.20
- [3] 1. 6-3-5 Method developed by Professor Bernd Rohbach, 1968
- [4] compiled and field-tested by Manfred Bieschke-Behm Head and initiator of self-help groups, workshops and seminars Publisher:
https://www.mittelhof.org/static/media/filer_public/5b/ef/5bef0a48-2cd6-4a8b-afd6-19952a80624a/selbsthilfe_reader_2015.pdf from 20.05.2020
- [5] https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/Zehn_Tipps/Zehn_Tipps_node.html from 25.04.2020
- [6] The idea for this activity is based on the publication by Bodo Köster
https://www.schuldekan-ravensburg.de/fileadmin/mediapool/einrichtungen/E_schuldekan_ravensburg/dokumente/Diskussionsmethoden_fuer_grosse_Groupen.pdf am 12.5.2020