



Mentoring programme for people 50+

MODULE 6

Safe use of digital technologies

**Strengthening Capacities to Support Active Ageing in the Conditions of the
21st Century - Peer Mentoring Programme for People 50+**

PEER-TRAIN



**Co-funded by
the European Union**

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.

6. Safe use of digital technologies

6.1 Introduction



The Safe Use of Digital Technologies refers to the responsible and secure use of electronic devices, applications, and online services. As technology has become increasingly ubiquitous in our daily lives, it is important to use digital technologies safely and effectively, particularly for elderly users who may be more vulnerable to digital threats.

Statistics indicate that the use of the internet by elderly users has been steadily increasing in recent years. According to the Pew Research Center, as of 2021, 73% of adults aged 65 and older use the internet. However, many elderly users may not be aware of the risks associated with using digital technologies, such as phishing scams, identity theft, and cyberbullying.

To help ensure the safe use of digital technologies, it is important to take steps to protect personal information and devices. This may include using strong passwords, avoiding clicking on suspicious links or emails, regularly updating software and security settings, and being cautious when sharing personal information online.

Additionally, it can be helpful for elderly users to receive education and training on safe technology use, particularly if they are not familiar with the latest security measures and best practices. This may involve seeking guidance from family members or friends, or attending workshops or classes designed specifically for seniors.

Overall, the safe use of digital technologies is essential for elderly users to fully participate in today's digital world while protecting themselves from potential threats.

Here are 10 important issues to consider for the safe use of digital technologies by elderly users:

Online scams and frauds: Elderly users can be targeted by online scams and frauds, such as phishing emails, fake websites, and identity theft. They should be cautious when sharing personal and financial information online.

Cyberbullying: Elderly users can be vulnerable to cyberbullying and online harassment, especially on social media platforms. They should be aware of the risks and take appropriate measures to protect themselves.

Online privacy: Elderly users should be aware of their online privacy and take steps to protect their personal information. This includes using strong passwords, avoiding public Wi-Fi networks, and being cautious about sharing personal information online.

Technology literacy: Elderly users may lack the necessary skills and knowledge to use digital technologies safely and effectively. They should receive training and support to improve their technology literacy.

Physical safety: Elderly users should be aware of the risks of using technology, such as eye strain, back pain, and falls, and take steps to prevent these risks.

Social isolation: Elderly users may experience social isolation due to the use of digital technologies, such as social media platforms. They should be encouraged to use technology as a means of staying connected with family and friends.

Accessibility: Elderly users may have physical and cognitive impairments that affect their ability to use digital technologies. They should have access to assistive technologies and accommodations to support their use.

Cybersecurity: Elderly users may be more vulnerable to cyber attacks due to their lack of familiarity with digital technologies. They should use antivirus software and be cautious about downloading attachments and clicking on links.

Scam calls: Elderly users can receive scam calls that try to extract money or information from them. They should be aware of such calls and take necessary precautions.

Ageism: Elderly users may be subjected to ageism in the digital world, such as being excluded from online communities or services. They should be empowered to challenge such practices and advocate for their rights.

6.2. Light on Artificial Intelligence



Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. AI has become increasingly important in many industries, including healthcare, finance, and transportation, due to its ability to analyse large amounts of data and make predictions based on that data.

One of the best examples of AI application is in the field of healthcare. AI can be used to analyse patient data, identify patterns, and make predictions about potential health risks. For

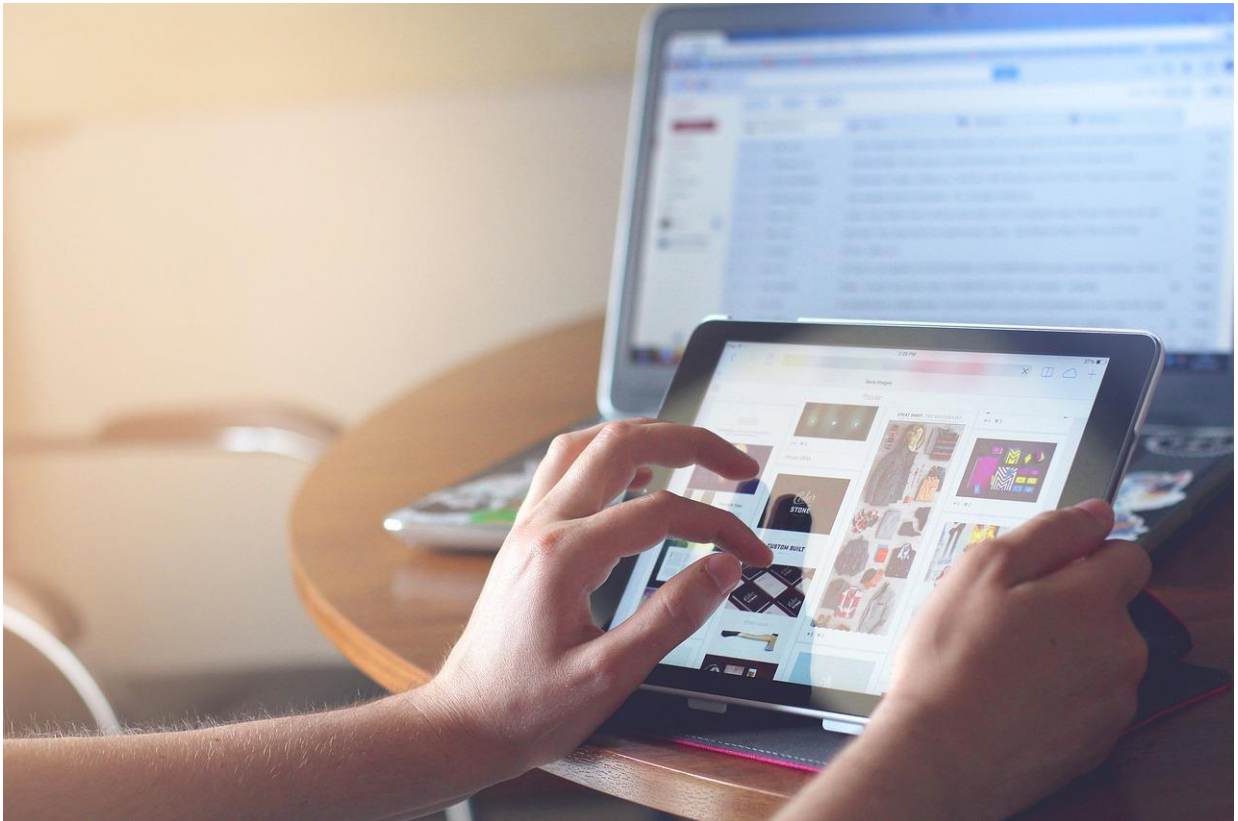
instance, AI algorithms can analyse medical images such as X-rays or MRIs to identify abnormalities that might be difficult for human doctors to spot. AI can also be used to personalize treatment plans based on individual patient data, which can improve patient outcomes and reduce healthcare costs.

Another example of AI application is in the field of finance. AI can be used to analyse large amounts of financial data, such as stock prices and economic indicators, and make predictions about future market trends. This can help financial institutions make more informed investment decisions and reduce the risks associated with market volatility.

In transportation, AI is being used to develop self-driving cars and improve traffic management systems. Self-driving cars rely on AI algorithms to interpret real-time traffic data, navigate roads, and make decisions about speed and direction. AI can also be used to optimize traffic flow by analysing data from sensors and cameras on roads and highways.

Overall, AI has the potential to transform many industries and improve our daily lives in countless ways. However, it is important to consider the ethical implications of AI development and ensure that it is being used responsibly and for the benefit of society as a whole.

6.3. Benefits and Threats of Digital Technologies



Digital technologies have revolutionized the way we live and work, providing many benefits such as increased efficiency, convenience, and connectivity. However, along with these benefits, there are also threats associated with the use of digital technologies that we must be aware of.

One of the main benefits of digital technologies is increased efficiency. Tasks that once took hours or even days to complete can now be done in a matter of minutes, thanks to digital tools and automation. This increased efficiency can help individuals and organizations save time and money, and also allow them to focus on more creative or strategic tasks.

Another benefit of digital technologies is convenience. Online shopping, mobile banking, and video conferencing are just a few examples of how digital technologies have made our lives more convenient. We can now access information and services from anywhere at any time, making our lives more flexible and adaptable.

Digital technologies have also increased connectivity, allowing us to communicate with people all over the world in real-time. Social media, messaging apps, and online communities have

made it easier to connect with like-minded individuals and build relationships, regardless of geographic location. This increased connectivity can help foster collaboration and innovation, leading to new ideas and solutions.

However, with these benefits come threats that we must be aware of. Cybersecurity threats such as hacking, phishing, and identity theft are becoming more common and sophisticated, putting individuals and organizations at risk. Digital technologies can also lead to privacy concerns, as our personal data is often stored and shared online without our consent or knowledge. Furthermore, the overreliance on digital technologies can lead to a lack of social interaction and a decrease in physical activity, which can have negative effects on our mental and physical health.

In conclusion, digital technologies have many benefits that have transformed the way we live and work. However, we must also be aware of the threats associated with their use and take steps to mitigate these risks. This includes being vigilant about cybersecurity, protecting our personal data, and finding a balance between digital connectivity and real-world interactions. By doing so, we can continue to reap the benefits of digital technologies while also staying safe and secure in an increasingly digital world.

6.4. Summary and Frequently Asked Questions



The resources below can be helpful for individuals, parents, educators, and businesses who want to learn more about safe use of digital technologies and how to protect themselves and their personal information online:

- [StaySafeOnline.org](https://www.staysafeonline.org/) - This website is run by the National Cyber Security Alliance and provides resources and tips for staying safe online, including information on how to protect your devices and personal information.
- [Cybersecurity & Infrastructure Security Agency \(CISA\)](https://www.cisa.gov/) - CISA is a government agency that provides resources and guidance on cybersecurity best practices, including tips for individuals and businesses to protect against cyber threats.
- [Common Sense Media](https://www.commonsensemedia.org/) - This website provides resources and advice for parents, educators, and kids about safe and responsible use of digital technologies, including information on privacy, cyberbullying, and screen time.

- NetSmartz - NetSmartz is an interactive website that provides resources and activities for kids and teens to learn about internet safety and cyberbullying.
- Federal Trade Commission (FTC) - The FTC provides information on consumer protection, including resources on online security, identity theft, and scams.
- Online Safety Foundation - This non-profit organization provides resources and tools for safe online behaviour, including tips for parents, educators, and seniors on how to stay safe online.
- Privacy Rights Clearinghouse - This organization provides resources and advice on protecting personal information and privacy, including information on data breaches, identity theft, and online tracking.

Here are example Frequently Asked Questions:

Q: What are some common cybersecurity threats I should be aware of?

A: Common cybersecurity threats include phishing scams, malware, identity theft, and hacking. It is important to be vigilant about suspicious emails, links, and downloads, and to use strong passwords and security software to protect your devices.

Q: How can I protect my personal data online?

A: To protect your personal data online, use strong and unique passwords for all of your accounts, avoid sharing personal information on social media or other online platforms, and be cautious when sharing information with unknown parties. You should also regularly update your privacy settings on social media and other online platforms to ensure that your information is not being shared without your consent.

Q: How can I ensure that my devices are secure?

A: To ensure that your devices are secure, regularly update your software and security settings, use antivirus and anti-malware software, and avoid downloading or installing software from unknown sources. You should also use two-factor authentication whenever possible, which requires a password and a secondary method of verification such as a fingerprint or text message.

Q: How can I avoid becoming a victim of cyberbullying?

A: To avoid becoming a victim of cyberbullying, be cautious about what you share online, and avoid engaging with individuals who are behaving aggressively or inappropriately online. You should also be aware of the resources available for reporting cyberbullying and seeking support, such as your school, workplace, or local law enforcement.

Q: How can I ensure that my children are safe online?

A: To ensure that your children are safe online, monitor their online activity and use parental controls and filtering software to limit access to inappropriate content. You should also teach your children about safe online behaviour, such as avoiding sharing personal information online and being cautious about meeting strangers in person.

Q: What should I do if I suspect that my personal information has been compromised?

A: If you suspect that your personal information has been compromised, contact your financial institution, credit card company, or other relevant organizations immediately to report the issue and take steps to protect your accounts. You should also consider placing a fraud alert or security freeze on your credit report to prevent further unauthorized activity.

Q: What is AI?

A: AI, or artificial intelligence, refers to the ability of machines or computers to perform tasks that would typically require human intelligence, such as recognizing patterns, learning, and problem-solving.

Q: How does AI work?

A: AI works by using algorithms and data to learn and make predictions or decisions. It uses machine learning, natural language processing, and other technologies to simulate human intelligence.

Q: What are some examples of AI applications?

A: AI is used in a wide range of applications, including virtual assistants, image recognition, predictive analytics, autonomous vehicles, and smart homes.

Q: Is AI replacing jobs?

A: AI has the potential to automate certain tasks and jobs, but it can also create new jobs and opportunities. While some jobs may be replaced by AI, others will require human skills such as creativity, problem-solving, and emotional intelligence.

Q: How is AI being regulated?

A: AI is a rapidly evolving field, and regulations are still being developed to address its ethical, legal, and societal implications. Some countries have established AI policies and guidelines, and international organizations such as the OECD and EU are working on developing AI principles.

Q: What are some ethical concerns surrounding AI?

A: Ethical concerns around AI include issues of bias, transparency, privacy, accountability, and the potential misuse of AI technologies for surveillance or harm.

Q: Can AI be biased?

A: AI can be biased if it is trained on biased data or algorithms. This can lead to discriminatory outcomes in areas such as hiring, lending, and criminal justice.

Q: Is AI dangerous?

A: AI can be dangerous if it is not developed and used responsibly. There are concerns about the potential misuse of AI technologies, such as autonomous weapons or surveillance systems.

Q: How can I learn more about AI?

A: There are many resources available to learn more about AI, including online courses, books, and conferences. Some popular resources include Coursera, Udemy, and MIT OpenCourseWare.

Take the poster!

5 Internet Safety Tips



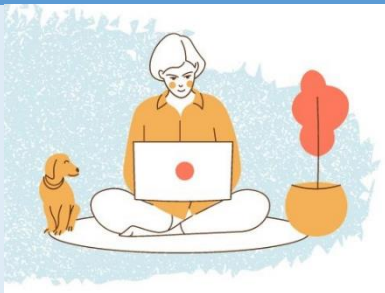
Don't Give Out Personal Information

Keep your personal information private and use it on safe sites only.



Create complex passwords

Create passwords with combination of letters, numbers and symbols



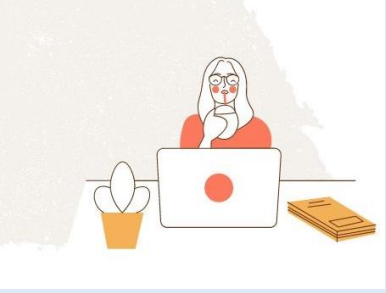
Keep your computer updated

Keep your device software up to date so it is not vulnerable to malware.



Avoid suspicious Online Links

Some websites may steal your personal information by asking you to take a quiz. Be careful!

	<h2 style="text-align: center;">Check website reliability</h2> <p style="text-align: center;">Before purchasing anything on a website ensure that it's safe.</p>
---	--

6.5. Questions

6.5.1 Quiz

1. Is the statement true or false?

It is safe to click on any link or download any attachment that comes through an email, regardless of the sender. (False)

- a) True
- b) False

2. Is the statement true or false?

Using strong passwords, changing them frequently, and not sharing them with others is important for online security. (True)

- a) True
- b) False

3. Is the statement true or false?

It is safe to give out personal information such as your full name, address, and social security number online. (False)

- a) True
- b) False

4. Is the statement true or false?

Public Wi-Fi networks, such as those found at cafes and airports, are typically secure and safe to use. (False)

- a) True
- b) False

5. Is the statement true or false?

Pop-up ads that claim you have won a prize or need to update your computer software are usually legitimate. (False)

- a) True
- b) False

6. Is the statement true or false?

Installing and regularly updating antivirus software on your computer is an effective way to protect against malware and other online threats. (True)

- a) True
- b) False

7. Is the statement true or false?

It is safe to trust every online review and testimonial when making a purchase. (False)

- a) True
- b) False

8. Is the statement true or false?

Social media platforms are a safe place to share personal information and pictures with friends and family. (False)

- a) True
- b) False

9. Is the statement true or false?

Phishing scams, where someone poses as a legitimate entity to trick you into giving them sensitive information, are not very common. (False)

- a) True
- b) False

10. Is the statement true or false?

Online scams and frauds only happen to people who are not tech-savvy. (False)

- a) True
- b) False

6.5.2. Preparation for group session

Online Scavenger Hunt: Create a list of internet safety tips and AI-related terms or concepts, and ask seniors to find and learn more about them online. For example, they can search for "how to create a strong password," "what is two-factor authentication," "what is machine learning," or "what are chatbots."

Using Two-Factor Authentication: Explain the concept of two-factor authentication and how it can help protect online accounts. Have seniors practise setting up two-factor authentication on their email or social media accounts, and explain how this extra layer of security can help prevent hacking attempts.

Spotting Fake News: Share a few articles with seniors and ask them to identify which ones are fake news. Explain how to identify trustworthy sources, how to fact-check information, and how to recognize clickbait headlines. This exercise will help seniors become more critical consumers of online content.

Identify Phishing Emails: Provide seniors with sample emails and ask them to identify which ones are phishing emails. Explain what clues they should look for, such as suspicious links, grammatical errors, or requests for personal information. This exercise will help seniors become more aware of common phishing tactics and avoid falling victim to them.

Spot the Scam: Show seniors examples of online scams and ask them to identify the red flags that suggest they're not legitimate. For example, you can show them a phishing email, a pop-up ad that claims they've won a prize, or a message that asks for their personal information.

AI Applications Brainstorm: Ask seniors to brainstorm practical applications of AI that they'd find helpful or interesting in their daily lives. For example, they can come up with ideas for an AI-powered personal assistant, an app that uses AI to help with grocery shopping or medication management, or a device that uses AI to monitor their health.

Understanding AI Bias: Explain how artificial intelligence can sometimes perpetuate biases and stereotypes, and provide examples of this phenomenon. Ask seniors to think critically about the ways that AI is used in their everyday lives, and how they can identify and address instances of bias.

Practise Strong Passwords: Instruct seniors to create strong passwords using a combination of uppercase and lowercase letters, numbers, and symbols. Have them practise creating and memorising several passwords, and explain why this is important for online security.

Password Management: Provide seniors with examples of weak passwords and ask them to create strong ones that follow best practices. You can also show them how to use a password manager to store and manage their passwords securely.

Building Internet Safety Quiz: Create a quiz on internet safety and AI-related topics and ask seniors to prepare questions. Suggest preparing questions about safe browsing habits, phishing scams, social media privacy settings, and AI ethics. Review the answers together and discuss any areas where they might need more guidance.

Attachment: Quiz answers

Question	Right answer
1.	False
2.	True
3.	False
4.	False
5.	False
6.	True
7.	False
8.	False
9.	False
10.	False

6.6. Literature

1. ChatGPT Feb 13 Version, <https://chat.openai.com/chat>, last opened 2023.02.25
2. BLOG Sektor 3.0 <https://sektor3-0.pl/blog/chatgpt-jak-korzystac/>, last opened 2023.02.25
3. DeepL Translator, <https://www.deepl.com/en/translator>, last opened 2023.02.25
4. YouTube playlist, Light on AI, Światło na Sztuczną Inteligencję, <https://youtube.com/playlist?list=PLeOe3daa0qUxPcl2YaC04pF9Zljr1lleE>, last opened 2023.02.25
5. AI for the Common Good, <https://www.semanticscholar.org/about>, last opened 2023.02.25
6. Future IT Professionals Education in Artificial Intelligence (FITPED-AI), <https://fitped.eu/fitped-ai/>, last opened 2023.02.25
7. ABC Cyberbezpieczeństwa, <https://www.gov.pl/web/baza-wiedzy/abc-cyberbezpieczenstwa---nowy-poradnik-przygotowany-przez-nask-pib>, last opened 2023.02.25
8. ABC Cyberbezpieczeństwa, <https://www.nask.pl/pl/aktualnosci/5123,ABC-cyberbezpieczenstwa-od-NASK.html>, last opened 2023.02.25
9. ACE IT Scotland, Keeping safe on the Internet, <https://youtube.com/playlist?list=PLJQ1e8zJE5Gwo3XpT8OFpyK1qJdIUHrB5>, last opened 2023.02.25
10. ACE IT Scotland, Online Basics, <https://youtube.com/playlist?list=PLJQ1e8zJE5GxvegbjgJAAOfVYt95R4Ogm>, last opened 2023.02.25
11. Grabowska A., Konferencja MoodleMoot PL 2022, MoodleCloud & PEER-TRAIN na Festiwalu Światta <http://utwpg.gda.pl/2023FS/MoodleMoot%202022%20-%20MoodleCloud%20%26%20PEER-TRAIN%20na%20Festiwalu%20%C5%9Awiat%C5%82a.pdf>