Training fiche

Title	Cyber security for seniors: Tools for Safe Navigation
Keywords	Cyber security, online safety, digital dependency, secure browsing, health technology
Provided by	Croatian Telecom Inc.
Language	English

Training area (X where applicable)	
	Information Literacy
	Communication & Collaboration
x	Safety
	Problem Solving

Objectives / Learning outcomes

Objective: The objective of this training is to educate seniors about cyber security and provide them with the necessary tools and knowledge to navigate the online world safely.

Learning Outcomes- by the end of this training, participants will be able to:

- Understand the importance of cyber security
- Recognize common cyber threats
- Practice safe internet browsing
- Safeguard personal information
- Respond to cyber incidents
- Utilize digital technologies for health and well-being

Description

This training equips seniors with the essential knowledge and tools to navigate the online world safely. Participants will learn about cyber security risks and recognize common threats. They will understand safe internet browsing and email security, secure personal devices, safeguard personal information, and stay safe. The training also covers incident response and the importance of staying updated on emerging cyber threats. They will also be able to navigate digital technologies safely in relation to their health and well-being, making informed decisions and leveraging the opportunities they provide. By the end, you will be empowered to protect yourselves and your personal information online.

Content index (3 levels)

Module: Cyber security tools for safe navigation
Unit 1: Introduction to Cyber security
1.1. Understanding Cyber security risks
1.2. Common types of Cyber threats

Co-funded by the European Union

1.3. Importance of Cyber security for seniors

Unit 2: Safe Internet Browsing
2.1. Best practices to keep yourself safe in the digital environment
2.2. Enhancing online safety with secure browsing tools

Unit 3: Health and Well-being in the Digital Age
3.1. Risks of excessive screen time and digital dependency
3.2. Health and digital tools

Content developed

Module: Cyber security tools for safe navigation

Unit 1: Introduction to Cyber Security
Section 1.1.: Understanding Cyber security risks
Think of cyber security risks as potential hazards when you go online. Just like you take precautions to stay safe in the physical world, such as locking your doors, being aware of cyber risks helps you stay safe in the digital world. These risks can include things like hackers trying to steal your personal information, scams that trick you into giving away your money, or viruses that can harm your computer. Moreover, cyber security emphasizes the cultivation of a security-conscious culture by promoting awareness and education about safe online practices.
By learning about these risks, you can better protect yourself. It's like knowing the signs of a slippery floor so you can walk carefully and avoid falling. We will discuss common cyber risks and how to recognize them, so you can navigate the online world with confidence and make informed choices to keep yourself and your information secure. Remember, knowledge is power, and by understanding cyber security risks, you are taking an important step towards protecting yourself online.

1.2. Common Types of Cyber Threats
In this unit, we will explore the common types of cyber threats, which are different ways that bad actors try to harm you or your computer when you are using the internet. Understanding these threats helps you stay safe and avoid potential harm. Let's break it down in simple terms.

Think of cyber threats as sneaky tricks or traps that bad people use online. They want to steal your personal information, infect your computer with harmful software, or trick you into giving them your money. Some common types of cyber threats include things like phishing, malware, and identity theft.

Phishing is like a fake email or message that pretends to be from someone you trust, but it's trying to trick you into giving away your personal information. It's like someone pretending to be a friend to get access to your secrets. Common phishing messages are: fake emails from the bank, false reports of winnings from gambling or games of chance or free prizes, fake accounts of providers of IT or payment services or Internet

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

stores, false confirmations of purported orders or false payment reminders, false messages about personal data privacy policies or terms that should be accepted.
The phishing e-mail message may say: Your credit card has expired, your account has expired, temporarily blocked, or confirm your login information. Layout (corporate design), sender address or directly greeting the user can create the impression that it is an e-mail sent by a bank or other provider service. E-mail messages in HTML format display a "legal" link to the recipient, which contains a hidden link in the background, which leads directly to fraudulent or malicious content.
Malware is like a virus that can infect your computer and cause damage. It can make your computer slow down or even steal your personal information.
Identity theft is when someone steals your personal information, like your name, address, or credit card details, and uses it without your permission. It's like someone pretending to be you and using your money or buying things on your behalf.
Identity thieves can also in their e-mail messages integrate malware such as viruses or Trojan software as a link, attachment, or source code in an email message in HTML format. Just clicking on the image in the phishing message can have serious consequences. Fraudsters who steal identities often use addresses that differ only slightly from the original ones. An identity thief can replace characters to create fake URLs. For example, instead of the original addresses such as http://www.onlinebank.com.hr can be a fake representation use an address such as http://www.on1inebank.com.hr.
How to be aware if something is malicious?

- FAKE SENDER ADDRESS

Hover your mouse over the sender's address. Does the email address contain suspicious elements? Are there spelling mistakes in the address, even if they were insignificant?

- REQUEST FOR CONFIDENTIAL DATA

Does the link contained in the e-mail ask you to enter personal information’s? Are you required to provide confidential information such as PINs or passwords?
URGENCY

- Does the e-mail request that you act immediately or urgent? Does the message contain a threat or a warning?
- LINKS TO FAKE WEBSITES

What URL appears when you mouse over a link? Is it secure page (URL should start with “https://”) and encrypted (lock symbol in front of the URL)?

- STRANGE FORMULATIONS AND SPELLING ERRORS

Is the email greeting generic? Does it contain spelling errors, incorrect punctuation, or special signs?
By learning about these common types of cyber threats, you can recognize them and take steps to protect yourself. We will discuss strategies to stay safe and avoid falling victim to these threats, empowering you to enjoy the online world with confidence and peace of mind.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.3. Importance of Cyber Security for Seniors

Think of cyber security as your personal bodyguard in the digital world, looking out for your well-being. It's like having someone watching over you, making sure your personal information stays safe and your devices remain secure. To ensure cyber security, we need to practice safe online habits, such as creating strong and unique passwords, being cautious about clicking on suspicious links or downloading files from unknown sources, and keeping our devices and software up to date.

- Never confirm your account number, password, or other secret information if requested in an email message. Real banks and companies would never use such for security reasons.
- Check the security status of websites before you enter your personal data. HTTPS does not guarantee that a website is real. Click on the padlock symbol displayed next to the URL in your browser to check the security certificate of the website.
- Belief in the infallibility of technology can leave room for Phishing attacks. A healthy level of mistrust prevents attackers from stealing your identity and access to your accounts and information systems.

Unit 2: Safe Internet Browsing

2.1. Best practices to keep yourself safe in the digital environment

- Practice Safe Browsing Habits: Stick to trusted websites when shopping, banking, or sharing personal information online. Look for the padlock symbol and "https://" in the website address, indicating a secure connection.
- Be Wary of Social Engineering: Beware of unsolicited calls, messages, or emails requesting personal information or financial details. Legitimate organizations will not ask for such information through unsolicited means
- Backup Your Data Regularly: Create backups of your important files and data on a separate storage device or cloud service. This helps protect against data loss due to hardware failure, theft, or ransomware attacks.
- Enable Two-Factor Authentication (2FA): Activate 2FA whenever available. This adds an extra layer of security by requiring a secondary verification step, such as a unique code sent to your mobile device, in addition to your password.
- Be Mindful of Social Media Sharing: Exercise caution when sharing personal information, location details, or vacation plans on social media platforms. Oversharing can provide valuable information to cyber criminals or potential burglars.
- Secure Your Mobile Devices: Apply security features, such as passcodes, fingerprint, or facial recognition, to lock your smartphones and tablets. Install reputable security apps that offer features like remote tracking and wiping in case of loss or theft.
- Trust Your Instincts: If something seems too good to be true or feels suspicious, trust your instincts. Be skeptical of unexpected offers, requests for money, or urgent appeals for personal information.

Co-funded by the European Union

- Clear Browsing Data Regularly: Clear your browsing history, cookies, and cached data on a regular basis. This helps protect your privacy by removing stored information that could potentially be accessed by unauthorized individuals.

2.2. Enhancing Online Safety with Secure Browsing Tools

Enhancing online safety with secure browsing tools is an important aspect of cyber security. By utilizing these tools, you can protect your privacy, secure your personal information, and reduce the risk of online threats. Here are some essential tips to enhance your online safety with secure browsing tools:

- Install and Use a Trusted Web Browser: Choose a reputable web browser, such as Google Chrome, Mozilla Firefox, or Microsoft Edge. These browsers prioritize security and regularly release updates to address vulnerabilities.
- Activate the Browser's Security Features: Familiarize yourself with the security features offered by your web browser. Enable features such as pop-up blockers, safe browsing mode, and privacy settings to enhance your online safety.
- Enable Phishing and Malware Protection: Activate the built-in phishing and malware protection features offered by your web browser. These features can warn you about suspicious websites and prevent you from visiting known malicious sites.
- Stay Educated and Updated: Stay informed about the latest online threats and best practices for secure browsing. Regularly read reliable sources, such as reputable cybersecurity websites or blogs, to stay up to date with the evolving landscape of online security.

Unit 3: Health and Well-being in the Digital Age

3.1. Risks of Excessive Screen Time and Digital Dependency

To mitigate the risks of excessive screen time and digital dependency, here are some strategies and practices to consider:

- Set Screen Time Limits: Establish specific time limits for using screens, both for leisure activities and work-related tasks. This helps create a healthy balance between screen time and other activities.
- Take Regular Breaks: Incorporate regular breaks from screens into your daily routine. Stand up, stretch, and engage in physical activities or hobbies that don't involve digital devices.
- Practice Digital Detox: Dedicate specific periods, such as weekends or evenings, to disconnect from digital devices entirely. Use this time to engage in offline activities, spend time with loved ones, or pursue hobbies.
- Practice Mindful Technology Use: Be mindful of how you use technology and the impact it has on your well-being. Reflect on your digital habits, assess their effects on your life, and make conscious choices to minimize negative consequences.
- Seek Support and Accountability: Share your concerns with trusted family members, friends, or support groups. Establish mutual accountability to encourage responsible technology use and provide support in maintaining healthy habits.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- Set Digital Boundaries: Define clear boundaries for technology use, such as turning off notifications during specific times, avoiding screen time before bed, or setting guidelines for device use during family meals.

Remember, the goal is to develop a healthy relationship with technology and ensure that it enriches your life rather than becoming a source of excessive dependence. By implementing these strategies, you can mitigate the risks associated with excessive screen time and promote a more balanced and fulfilling lifestyle.

3.2. Health and digital tools

Technology can offer numerous ways to support and improve your health. Here are some ways in which technology can help you with your health:

- Access to Information: The internet provides a wealth of health-related information, allowing you to research symptoms, conditions, treatments, and preventive measures. Reliable websites, health apps, and online communities can empower you to make informed decisions about your health.
- Health Monitoring: Wearable devices, such as fitness trackers and smartwatches, can monitor various aspects of your health, including heart rate, sleep patterns, physical activity, and calories burned. These devices can provide valuable insights into your overall well-being and help you track progress toward health goals.
- Telehealth and Remote Consultations: Telehealth services allow you to consult healthcare professionals remotely through video calls or online chats. This convenient approach saves time and can be particularly beneficial for follow-up appointments, routine check-ups, or non-emergency medical consultations.
- Medication Management: Mobile apps and smart pill organizers can help you manage medications by providing reminders for taking pills, tracking medication schedules, and providing alerts for prescription refills. This technology can prevent missed doses and promote adherence to medication regimens.
- Mental Health Support: Various mental health apps and online platforms provide resources for managing stress, anxiety, and depression. These tools can include guided meditation, breathing exercises, mood tracking, and therapy sessions conducted through digital platforms.
- Health Record Management: Digital health records and patient portals enable you to access and manage your medical history, test results, and appointment schedules. This streamlines communication with healthcare providers and ensures continuity of care.
- Support and Motivation: Online communities and social media platforms dedicated to health and wellness can provide support, motivation, and encouragement. Connecting with like-minded individuals can foster a sense of community and help you stay accountable to your health goals.
- Health Tracking and Data Analysis: Technology allows you to track and analyze health data over time, such as blood pressure, blood glucose levels, or weight. By monitoring trends and patterns, you can identify areas for improvement and make necessary adjustments to optimize your health.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Remember, while technology can be a valuable tool in supporting your health, it's important to use it wisely and in conjunction with professional medical advice. Always consult healthcare professionals for accurate diagnosis, treatment recommendations, and personalized guidance.

5 Glossary entries

Cyber security refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, and damage. It involves implementing measures to prevent cyber threats, such as hacking, data breaches, and malware attacks. The goal of cybersecurity is to ensure the confidentiality, integrity, and availability of digital assets, safeguarding individuals and organizations against potential risks and vulnerabilities in the interconnected digital world.

Identify theft refers to the fraudulent acquisition and use of someone's personal information, such as their name, social security number, or financial details, without their consent. It involves impersonating the victim to carry out various illegal activities, including financial fraud, making unauthorized purchases, or committing other forms of identity-related crimes.

Social engineering is a manipulative technique used by cybercriminals to deceive individuals and exploit their trust and emotions. It involves psychological manipulation rather than technical methods to trick people into revealing sensitive information or performing actions that may compromise their security. Examples of social engineering techniques include phishing emails, phone scams, pretexting, and impersonation. The goal of social engineering is to manipulate human behavior to gain unauthorized access to systems, networks, or personal information.

5 multiple-choice self-assessment questions

1. In cyber security, risks refer to:
a) Potential hazards when going online.
b) Physical security measures.
c) Precautions against slippery floors.
d) Safe online practices.
Correct option: a

2. What are some common types of cyber threats?
a) Physical attacks on computers.
b) Tricks or traps used by bad people online.
c) Safety measures for online shopping.
d) Strategies to protect personal information.

Co-funded by the European Union

Correct option: b

3. What is social engineering?
a) A technique used by cybercriminals.
b) The study of human behavior.
c) A secure browsing tool.
d) A type of computer virus.
Correct option: a

4. How can you enhance online safety with secure browsing tools?
a) By using reputable web browsers and activating security features.
b) By increasing screen time and digital dependency.
c) By sharing personal information on social media.
d) By ignoring phishing emails and malware warnings.
Correct option: a

5. What are some strategies to mitigate the risks of excessive screen time?
a) Setting screen time limits and taking regular breaks.
b) Increasing technology use for better health.
c) Disconnecting from digital devices entirely.
d) Seeking support and accountability.
Correct option: a

Bibliography and further references

- https://staysafeonline.org/
- https://www.consumer.ftc.gov/topics/online-security
- https://www.cisa.gov/cybersecurity
- https://www.getsafeonline.org/
- https://us.norton.com/internetsecurity
- https://www.staysmartonline.gov.au/
- https://www.commonsense.org/education/digital-citizenship/privacy-and-security

Related material	BOOMER_Cyber_security_HT
Reference link	
Video in Powtoon format	https://www.youtube.com/watch?v=lvLhhqDhZJY

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.