Training fiche

Title	Online safety: Do’s and don’ts
Keywords	Internet, safety, online, offline, passwords, privacy
Provided by	Internet Web Solutions
Language	English

Training area (X where applicable)

	Information Literacy
	Communication & Collaboration
X	Safety
	Problem Solving

Objectives / Learning outcomes

At the end of this module, you will:

- Understand the importance of responsible online behaviour
- Identify common online risks
- Recognize the benefits of the internet
- Learn online safety best practices
- Develop digital literacy skills

Description

This course offers a comprehensive overview of how to stay safe while using the internet, providing practical advice on online do’s and don’ts, including tips on secure connections, password management, privacy settings for social media, safe online shopping practices, and recognizing and avoiding frauds and scams. By following these guidelines, you will be able to navigate the online world safely and protect yourself from potential threats.

Content index (3 levels)

Module: Online safety: Do’s and don’ts
Unit 1: Introduction to online safety
1.1. What does it mean to be safe online?
1.2. What are the risks of insecure Internet navigation?
1.3. Why shouldn’t you stop navigating the Internet even with these risks?

Unit 2: Online do’s and don’ts
2.1. Secure connections
2.2. Passwords

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.

2.3. Privacy and social media
2.4. Online shopping
2.5. Frauds and scams

Unit 3: Bonus track: Offline do's and don'ts
3.1. Digital devices

Content developed

Module: Online safety: Do's and don't's

Unit 1: Introduction to online safety

Section 1.1: What does it mean to be safe online?

Being safe online means taking precautions and adopting responsible behaviors while using the internet. It involves understanding and managing the **potential risks and threats** associated with online activities to protect personal information, financial resources, and overall well-being.

The cyberspace is like a freeway: you have to navigate it safely to avoid accidents. Just like fastening your seatbelt, some basic internet safety practices can help ensure that your online experience is safe and enjoyable.

Being safe online is important for several reasons. It helps **protect your personal information** from falling into the wrong hands. Personal details such as your name, address, phone number, and financial information can be used for identity theft, fraud, or other malicious activities if accessed by cybercriminals. Your online presence contributes to your reputation, both personally and professionally.

By being safe online, you can **prevent the dissemination of inappropriate or damaging content** that may negatively impact your image and relationships. Safeguarding your online safety ensures the **protection of your privacy** and **protect you from financial frauds and scams**.

Being safe online also helps in **avoiding instances of cyberbullying and harassment**. By implementing safety measures, you can reduce the risk of encountering harmful individuals or situations that may lead to emotional distress or harm. Online safety is also crucial for **protecting children** and ensuring their well-being in the digital world.

Section 1.2: What are the risks of insecure internet navigation?

Insecure internet navigation poses risks for elderly individuals. They may be less familiar with online platforms and threats, so understanding the specific risks they face is important.

Some common risks are:

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.

- **Phishing and Scams**: Elderly individuals are more susceptible to phishing emails, fraudulent websites, and phone scams, where scammers deceive them into revealing sensitive information.
- **Identity Theft**: Insecure internet navigation increases the risk of personal information and identity theft, leading to financial loss and disruption in their lives.
- **Financial Fraud**: Elderly individuals are targeted with fake investment schemes, lottery scams, or fraudulent purchases, exploiting their trust and vulnerability.
- **Malware and Viruses**: Insecure internet navigation can lead to unintentional downloads of harmful software compromising device security and personal information.
- **Online Harassment and Cyberbullying**: Elderly individuals may suffer emotional distress and mental well-being issues due to online harassment.
- **Privacy Breaches**: Inadequate privacy practices can expose personal information, resulting in identity theft or unwanted solicitations.
- **Tech Support Scams**: Elderly individuals are more susceptible to scams where fraudsters pose as technical support representatives.
- **Lack of Digital Literacy**: Insecure internet navigation is worsened by a lack of digital literacy among elderly individuals, making them more vulnerable to threats and scams.

Elderly individuals should be aware of these risks and take proactive measures to prevent them, for example by seeking help and support from trusted individuals or report concerns to relevant authorities or platforms.

Section 1.3: Why shouldn't you stop navigating the Internet even with these risks?

Internet safety is important, but it doesn’t have to be stressful. Awareness is a powerful first step in protecting yourself together with a trusted antivirus software (lots of them are free!).

You should not completely stop navigating the internet despite the online risks as the net can have enormous advantages for your wellbeing and social inclusion. The internet offers a vast amount of **information and resources** that can greatly benefit you. It provides access to news, educational materials, healthcare resources, communication tools, and various online services.

In terms of **social connection**, the internet enables to stay connected with family, friends, and communities, especially when physical mobility or distance is a barrier. Social media platforms, video calls, and online forums allow to maintain relationships, share experiences, and combat isolation or loneliness. Online platforms offer convenience and **independence** for all people in various aspects of daily life. You can s**hop online, access online banking services, schedule**

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.

appointments, and order medications, providing greater convenience and **reducing the need for physical travel or assistance**.

Navigating is also a source of **cognitive stimulation and mental engagement** as it offers opportunities for learning, playing games, participating in virtual hobbies or communities, and staying mentally active, which can contribute to overall well-being.

By navigating the internet and adopting safe online practices, you can **develop digital literacy skills**, enhance your confidence, and maintain a sense of **empowerment**. The internet provides a wealth of **learning resources**, including online courses, tutorials, and educational platforms. You can explore new interests, learn new skills, and engage in lifelong learning opportunities, promoting personal growth and intellectual stimulation.

While it is important to be aware of online risks and take precautions, **completely avoiding the internet can lead to isolation, limited access to resources, and missed opportunities**.

Unit 2: Online do’s and don’ts

Section 2.1: Secure connections

Do's:

Use Secure Wi-Fi Networks: Connect to secure and trusted Wi-Fi networks whenever possible. These networks usually require a password and encryption, providing a safer browsing environment. Avoid accessing sensitive accounts or conducting financial transactions on public Wi-Fi.

Verify Website Security: Before entering sensitive information or making online transactions, ensure that the website has a secure connection. Look for "https://" in the website address and a padlock symbol in the browser's address bar.

Keep Software Updated: Regularly update your device's operating system, web browsers, and security software. Software updates often include security patches that help protect against known vulnerabilities.

Use Firewall Protection: Enable and maintain a firewall on your computer or router to act as a barrier against unauthorized access and potential threats from the internet.

Don'ts:

Don't Share Sensitive Information: Avoid entering sensitive information, such as passwords, credit card details, or Social Security numbers.

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.

Avoid Suspicious Websites: Avoid visiting suspicious or unfamiliar websites. Stick to reputable and trusted websites for online activities.

Don't Ignore Browser Warnings: Pay attention to browser warnings and alerts about potential security risks or untrusted websites.

Don't Auto-Connect to Networks: Disable the auto-connect feature on your devices, as it may automatically connect to unsecured networks without your knowledge.

Section 2.2: Passwords

Do's:

Create Strong and Unique Passwords: Use strong and unique passwords for each online account. It should include a combination of upper and lowercase letters, numbers, and special characters. Avoid using guessable information such as birthdays or names.

Make Passwords Long: Opt for longer passwords, as they are generally more secure. Aim for a minimum of 12 characters. Consider using passphrases: series of words or a sentence that is easier to remember but difficult for others to guess. For example, "MyFavoriteColorIsBlue!".

Enable Two-Factor Authentication (2FA): Whenever possible, enable two-factor authentication for your online accounts. This adds an extra layer of security by requiring a second verification step, such as a unique code sent to your mobile device.

Regularly Update Passwords: Change your passwords periodically, preferably every few months.

Don'ts:

Don't Reuse Passwords: Never reuse the same password across multiple accounts. If one account is compromised, it could potentially grant access to other accounts as well. Use unique passwords for each online service or platform.

Avoid Common Passwords: Avoid common or easy passwords, such as "123456," "password," or "qwerty." These passwords are often targeted by hackers and can be easily cracked.

Don't Share or Write Down Passwords: Avoid sharing your passwords with others, including family or friends. Additionally, avoid writing down passwords on physical notes or storing them in easily accessible digital files.

Don't Save Passwords in Browsers: Refrain from saving passwords in web browsers or using the "Remember Me" feature. While it may provide convenience, it poses a

Co-funded by the European Union

security risk if someone gains unauthorized access to your device.

Section 2.3: Privacy and social media

Do's:

Review Privacy Settings: Familiarize yourself with the privacy settings of the social media platforms you use. Adjust the settings to control who can view your profile, posts, and personal information. Consider limiting access to trusted friends and family members.

Be Selective with Friend Requests: Be cautious when accepting friend requests or connection requests from unknown individuals. Verify the person's identity before accepting their request.

Think Before You Share: Exercise caution when sharing personal information, photos, or updates on social media platforms. Avoid sharing sensitive details such as your full address, phone number, or financial information publicly.

Regularly Review and Update Friends List: Periodically review your friends or connections list on social media platforms. Remove or unfriend individuals whom you no longer trust or recognize.

Don'ts:

Don't Click on Suspicious Links: Be wary of clicking on links shared on social media, especially those from unknown or suspicious sources. These links may lead to phishing websites or malware downloads. Verify the source before clicking.

Be Cautious with Third-Party Apps: Be selective when granting permissions to third-party applications that request access to your social media accounts. Review the permissions requested and consider the credibility of the application before granting access.

Avoid Publicizing Personal Events: Avoid announcing upcoming vacations or extended periods away from home on social media platforms. Doing so may alert potential burglars or criminals that your home is unoccupied.

Section 2.4: Online shopping

Do's:

Shop from Trusted Websites: Stick to reputable and well-known online retailers when making purchases. Look for websites that have positive customer reviews and secure payment options such as credit cards or reputable payment platforms.

Verify Website Security: Before entering payment or personal information, ensure that the website has a secure connection. Look for "https://" in the website address and a padlock symbol in the browser's address bar.

Keep Track of Transactions: Maintain a record of your online shopping transactions, including order confirmations, receipts, and tracking numbers. This allows you to track deliveries and resolve any issues that may arise.

Don'ts:

Don't Share Unnecessary Information: Be cautious about sharing unnecessary personal information during the checkout process. Retailers typically require basic details like shipping address and payment information.

Beware of Phishing Emails or Links: Be wary of emails or messages claiming to be from online retailers, especially if they ask for personal information or prompt you to click on suspicious links.

Avoid Unsecured Wi-Fi for Transactions: When making online purchases, avoid using unsecured or public Wi-Fi networks. These networks can be vulnerable to hackers who may intercept your personal and financial information.

Don't Fall for Impersonation Scams: Be cautious of online sellers impersonating reputable brands or using deceptive tactics to obtain your personal or financial information. Verify the authenticity of the seller and their website before making a purchase.

Section 2.5: Frauds and scams

Do's:

Be Skeptical and Vigilant: Maintain a healthy skepticism when encountering unsolicited emails, phone calls, or messages asking for personal information or offering strange deals. Verify the legitimacy of the source before providing any information or making any financial commitments.

Educate Yourself: Stay informed about common online scams and fraud tactics targeting elderly individuals. Familiarize yourself with the signs of scams, such as requests for payment through unconventional methods or pressure to act quickly.

Verify the Identity of the Contact: When individuals claim to represent organizations, ask for official contact information and confirm their authenticity by reaching out to the organization directly using verified contact details.

Consult with Trusted Individuals: If you receive a suspicious request or encounter an unfamiliar situation online, seek advice from a trusted family member, friend, or professional.

Co-funded by the European Union

Ignore unsolicited phone calls and "robocalls." Treat any unsolicited phone calls with skepticism. A live person or recorded voice gives you false information that sounds important and time-sensitive. They may claim to be a relative in trouble, that your car's warranty is expiring and payment is required, they might introduce themselves as "tech support" and tell you that your PC need to get it repaired for a fee.

Don'ts:

Don't Rush or Feel Pressured: Scammers often use tactics to create a sense of urgency or pressure, coercing victims into making quick decisions without proper consideration. Take your time, conduct research, and be cautious before making any financial commitments.

Don't Send Money to Unknown Individuals: Be wary of requests for money or wire transfers from individuals you do not know personally. Verify the identity and legitimacy of the individual before engaging in any financial transactions.

Don't click on links in emails from unfamiliar senders. Be wary of strange or unexpected messages, even if they're from people you know. They could contain malicious or phishing links. If a message looks suspicious but appears to be from someone you know and trust, check with them before clicking.

Don't open any attachments. Don't open any attachments you aren't expecting or that are from an unknown contact—especially if they have the extension .exe or .zip. If the file(s) appears to be from a friend or family member, ask them to make sure they have sent you something. This safety rule also applies to attachments sent via text messages and social media.

Don't click on pop-up windows on your phone or computer. A common pop-up ploy is scareware that uses pop-up security alerts to frighten you into downloading or paying for fake software disguised as real cybersecurity protection. For example, an alert will appear telling you that your device is compromised and needs repairing. When you call the support, scammers may ask for remote access to your computer and request a fee. Another malware technique is to use deceptive "Close" or "X" buttons, which automatically install a virus when clicking on them.

Unit 3: Bonus track: Offline do's and don'ts

Section 3.1: Digital devices

Do's:

Lock your devices. Ensure that devices with access to sensitive information automatically lock and require a password to reactivate. Make sure to configure the home Wi-Fi router and access points with unique usernames and passwords that are

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.

not the default ones.

Keep Devices Secure: Ensure that your digital devices, such as smartphones, tablets, or laptops, are physically secure. Store them in a safe and protected place when not in use.

Regularly Update Software: Keep the operating system and applications on your devices up to date. Software updates often include important security patches that help protect against vulnerabilities and ensure optimal performance.

Enable Remote Tracking and Locking: Activate the remote tracking and locking features on your devices, if available. This allows you to locate your device or remotely lock it in case of loss or theft.

Safely Dispose of Old Devices: When disposing of old digital devices, ensure that all personal data is completely wiped from the device. Perform a factory reset or use specialized software to erase your data securely.

Don'ts:

Don't Leave Devices Unattended: Avoid leaving your digital devices unattended in public places, such as cafes or public transportation. Always keep them within your sight or securely stored.

Don't Install Unauthorized Apps: Avoid downloading and installing applications from untrusted sources. Stick to official app stores, such as Google Play Store or Apple App Store, to reduce the risk of downloading malicious or counterfeit apps.

5 Glossary entries

Password. A password is a secret combination of characters used to authenticate and gain access to a device or an account. It is recommended to set a strong password to protect sensitive information.

Social media. Social media refers to online platforms and technologies that enable users to create, share, and exchange information, ideas, and content with others. These platforms typically involve user-generated content and facilitate communication, networking, and interaction among individuals or groups.

Online safety. Online safety refers to the measures and precautions taken to protect individuals and their personal information while using the internet and engaging in online activities. It encompasses practices and guidelines that aim to prevent various online risks such as cyberbullying, identity theft, fraud, hacking, and exposure to inappropriate content. Online safety involves understanding and implementing strategies to safeguard privacy, security, and well-being while using digital

Co-funded by the European Union

platforms.

Malicious Apps. Malicious apps are applications that are designed to harm or compromise the security of a device or user's data. Installing apps from untrusted sources increases the risk of downloading malicious apps that can steal personal information or perform unauthorized actions.

Sensitive information. Sensitive information refers to any data or details that, if disclosed or accessed by unauthorized individuals, could pose a risk to an individual's privacy, security, or well-being. It includes personally identifiable information (PII) such as full names, addresses, phone numbers, social security numbers, financial information, login credentials, and medical records. Sensitive information requires special protection and handling to prevent misuse, identity theft, fraud, or other harmful consequences.

5 multiple-choice self-assessment questions

Question 1. What does a Wi-Fi connection require to be secure?
Option a: Requires it to be private, with use of password and encryption.
Option b: Requires unlimited data usage.
Option c: Requires high internet speed.
Option d: Requires the Wi-Fi connection to be public.
Correct option: a

Question 2. Why is it important to regularly update your device's software?
Option a: Because it increases the storage space of the device.
Option b: Because it makes the device interface look nice.
Option c: Because it protects you against known vulnerabilities and security threats.
Option d: Because it increases the battery life of the device.
Correct option: c

Question 3. How can you identify potential frauds or scams?
Option a: By ignoring security alerts.
Option b: By sharing personal and financial information anywhere.
Option c: Rushing into financial commitments quickly.
Option d: Learning about common online scams and staying alert.
Correct option: d

Question 4. How can you create a strong password?
Option a: Using a single word in lowercase, without numbers or special characters.
Option b: Including uppercase and lowercase letters, numbers, and special characters.
Option c: Reusing the same password for multiple accounts.
Option d: Choosing an easy-to-guess password and sharing it with friends so you don’t lose it.
Correct option: b

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.

Question 5: When shopping online, what should you do if a website doesn't have a secure connection?

Option a: Proceed with the purchase anyway.

Option b: It is best to avoid entering personal or payment details on that website, and make the purchase on a more reliable website with a secure connection.

Option c: I should ask someone else to use their details and make the purchase for me on that website.

Option d: If I make the purchase using a public Wi-Fi network, there will be no problem in sharing my data with that website.

Correct option: b

Bibliography and further references

https://www.enisa.europa.eu/
http://www.eun.org/
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
https://www.microfocus.com/en-us/what-is/cyber-security
https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html
https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/
https://www.europol.europa.eu/wannacry-ransomware

Related material	BOOMER_OnlineSafety_IWS_EN
Reference link	
Video in Powtoon format	https://youtu.be/PYixkF0A34c

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.