Media Literacy in the Digitalised Era: Supporting Teachers through a Whole-School Approach

MODULE 4: E-SAFETY

Developed by: N.C.S.R. “Demokritos”

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

Co-funded by the Erasmus+ Programme of the European Union

Module 4: E-Safety

DESCRIPTION

This module aims to introduce teachers to a range of scenarios and ways to stay safe online. Issues like risks and responsibilities online, protecting personal data, online disinformation and harmful content, digital copyright, and cyberbullying effective and ineffective practice will be discussed.

Co-funded by the Erasmus+ Programme of the European Union

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

Module 4: E-Safety

MeLDE

LIST OF TOPICS

TOPIC 1 RISKS AND RESPONSIBILITIES ONLINE

TOPIC 2 **PROTECTING PERSONAL DATA**

TOPIC 3 DIGITAL COPYRIGHTS

TOPIC 4 ONLINE MISINFORMATION AND HARMFUL CONTENT

TOPIC 5 CYBERBULLYING

Co-funded by the
Erasmus+ Programme
of the European Union

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

Module 4: E-Safety

SYLLABUS

Topic 1: Risks and responsibilities online

- Potential threats to hardware and software
- Threats to Data and Information
- Ways of reporting Internet scammers
- Online rights and responsibilities

Topic 2: Protecting personal data

- Create and Keep Strong Passwords
- Importance of Updated Antimalware Software and Operating System
- Vulnerability of Mobile Devices and Ways to Keep them Secure
- Malicious Emails
- Ways of Protecting Personal Data on Social Networking Sites

Topic 3: Digital Copyrights

- Discuss new legal policy developments in copyright law and understand how copyright law has adapted to the digital age.
- Understand how to protect digital content created and published by you or your students
- Understand plagiarism and how it can be avoided in the age of information overload where the content can be used and reused in a variety of ways by countless sources
- Explore series of open access sources and understand what and when can digital content be used and reused for educational purposes
- Work in groups to produce a digital copyright short, easy-to-read manual for their schools

Co-funded by the Erasmus+ Programme of the European Union

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

MeLDE

SYLLABUS

Topic 4: Online misinformation and harmful content

- The difference between a genuine and a copycat website
- Evaluate and report fake websites
- The concept of ‘fake news’ and how to evaluate and identify them
- Why it is important to report fake websites and their detrimental impact on democracy, society and individuals

Topic 5: Cyberbullying

- What cyberbullying is and why it is important
- Different forms of cyberbullying
- Identify students who are victims of cyberbullying in a variety of ways
- Actions that will help students who are victims of cyberbullying
- The importance of having a cyberbullying intervention and prevention strategy in schools

Co-funded by the
Erasmus+ Programme
of the European Union

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

Topic 2: Protecting personal data

MeLDE

BRIEF DESCRIPTION AND SUB-TOPICS

This topic aims to introduce teachers to the most common security measures, such as strong passwords, Anti-Malware software, data backup, encryption, firewall and shopping securely. The topic will also touch on how to stay safe on social media, how to keep your mobile devices safe, and how to avoid harmful or offensive content on social media.

The following will be discussed:

- Create and Keep Strong Passwords
- Importance of Updated Anti-Malware Software and Operating System
- Vulnerability of Mobile Devices and Ways to Keep them Secure
- Malicious Emails
- Ways of Protecting Personal Data on Social Networking Sites

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

CREATE AND KEEP STRONG PASSWORDS

Creating strong passwords for your online accounts is one of the most effective ways you can protect your personal data and information, and keep yourself safe from cyberattacks.

In order to create strong passwords you will have to do the following:

- Use passphrases rather than passwords
- Use passwords that contain uppercase and lowercase letters, numbers and special characters
- Use passwords more than eight characters in length
- Avoid using easy to guess words or alphanumeric combinations (*e.g. names of children or pets, birth dates, addresses, social security numbers*)
- Use non-dictionary words

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

CREATE AND KEEP STRONG PASSWORDS

In order to keep your passwords safe you will have to do the following:

- Don’t store passwords with your laptop or your mobile device
- Don’t save passwords in your browser
- Don't write your passwords down, try to memorize it instead
- Use a password manager that can share single login credentials with other people without them actually being able to view or interpret the login information
- Don't use the same password for more than one account or service
- Organize your passwords in logical groupings
- Don't send passwords or account login credentials over public or unsecured Wi-Fi networks
- Change your password as soon as a security breach is found and the intruder is blocked

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

IMPORTANCE OF UPDATED ANTI-MALWARE SOFTWARE AND OPERATING SYSTEM

UPDATING THE ANTI-MALWARE SOFTWARE

Cybercrime is increasing, so it is important to download and install the latest updates.

- Most Anti-Malware companies are very quick to add protection for new threats and make that updated protection available to their customers.
- Most companies and individuals have time to protect themselves from new threats, if they keep their Anti-malware software up to date.
- Virus writers and malicious code engineers are constantly finding ways around the new technology features and holes in operating systems only help them in their efforts.
- If you are using security software for a long time and haven’t updated it often since then, it’s almost as good as not having Antivirus and Anti-Malware software installed.
- As long as security software stays outdated, cybercriminals are able to find bugs and issues to exploit.
- If your computer or laptop is infected with a virus or malware, it could affect not only your data or hard-drive, but it could spread itself to other devices via network links or emails.
- The cybercriminals can use your personal information like email address, online accounts to commit cybercrimes in your name.

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

MeLDE

IMPORTANCE OF UPDATING ANTI-MALWARE SOFTWARE AND OPERATING SYSTEM

UPDATING THE OPERATING SYSTEM

Hackers can take advantage of a software vulnerability, that is a security hole/weakness found in a software program/operating system, by writing code to target the vulnerability and use your stolen personal information to commit crimes in your name or sell them on the dark web to enable others to commit crimes.

Additional benefits to regularly updating your operating system:

- Repair security holes, by the software patches and by the fixed or removed security bugs.
- Add new features to your devices.
- Remove outdated features from your devices.
- Not to stay behind from the technology involvement, by using outdated programs and applications, that are vital to your success at school, home, work, etc.
- Fix the bugs discovered after the release of an operating system/program/application.

Co-funded by the
Erasmus+ Programme
of the European Union

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

Topic 2: Protecting personal data

VULNERABILITY OF MOBILE DEVICES AND WAYS TO KEEP THEM SECURE

Hackers nowadays are targeting smartphones and mobile devices alike, to gain access to personal information from text messages, Facebook and other social media applications, banking and shopping data, email messages, etc.

In order to avoid or recover from such an attack the smartphone and mobile device users can take the following steps:

- Lock your phone
  - All smartphones have a password protect capability, so be sure you are using it and change the password every three to six months. An easier alternative to passwords are a lock “pattern”, a face, voice or finger recognition.
- Turn on tracking
  - If your smartphone gets stolen you can check its location by using this feature. In addition, you can lock your phone remotely with a tracker application.
- Update your operating system
  - Make sure to download your smartphone’s latest updates, in order to close down vulnerabilities that hackers may discover.

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

VULNERABILITY OF MOBILE DEVICES AND WAYS TO KEEP THEM SECURE

- Be careful with applications
  - Make sure you are downloading an app from App Store (for iOS) or from Google Play (for Android), which verify the authenticity of the apps they are offering.
- Be cautious about text messages from an unknown source
  - Don’t open any text message from a stranger, an unknown number or a number that seems odd to you and delete them instead.
  - Don’t click on any links in the message.
  - Don’t download any apps from a text message.
- Be mindful of the risks of using free WiFi
  - Be wary of unsecured wireless networks.
  - If you are not using your service provider’s Internet service but a WiFi connection, you run the risk exposing your data to hackers.
  - Ensure that you are connected to a WiFi hotspot that is owned by a business. Be aware that free WiFi hotspot might owned by a hacker who may be able to steal personal data in crowded areas.
- Make sure you always have Antivirus protection
  - Your smartphone has an operating system; it is like a mini-computer, that needs protection from hackers.

Co-funded by the
Erasmus+ Programme
of the European Union

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

Topic 2: Protecting personal data

RECOGNISE MALICIOUS EMAILS

HOW TO RECOGNISE MALICIOUS EMAILS

1. Check if the sender is incorrect
   - Check if the address matches the name of the sender.
   - Check if the domain of the sender's company is correct.

   In order to be able to check the abovementioned, your email client must display the sender's email address and not just their name.
2. Check if the sender is not aware of your identity
   - Check if the sender addresses you in a way you would expect.
   - Check if the sender's signature matches how he/she would usually sign their emails.

   For example, your bank would normally address you with your full name in an email, not just in a generic way ("Dear customer").
3. Check if any embedded links have suspicious URLs
   - Hover over the links in an email before you open them. Check if the destination's URL matches the site that the email refers to.

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

RECOGNISE MALICIOUS EMAILS

4. Check the spelling and grammar
   - Check if the email is full of spelling and grammatical errors, like someone has used an online automatic translator for your language.
5. Check if the content is believable
   - If the email is promising to deliver great gain in return for small investment or for free, it usually is a phishing email.

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

WHAT TO DO IF YOU CLICKED A MALICIOUS LINK

1. Do not enter any personal data if requested.
2. Do not enter any login credentials.
   - ➢ The cybercriminals will use them to log in to the real account.
3. Disconnect from the Internet as soon as possible to contain any malware infection.
   - ➢ By switching off the network connection on your device.
   - ➢ By unplugging the network cable.
4. Scan your device with an antivirus or/and Anti-Malware software with a full scan.
   - ➢ Remain disconnected from the Internet while scanning.
5. Change your passwords on the real site or anywhere you are using your email with the same password.
6. Back up your files in a different device.

Co-funded by the
Erasmus+ Programme
of the European Union

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

Topic 2: Protecting personal data

WAYS OF PROTECTING PERSONAL DATA ON SOCIAL NETWORKS

1. Avoid filling out the ‘about me’ fields.
   - Most social networks, like Facebook, keep their ‘about me’ sections optional. Consider giving only general information or simply leave the field empty.
2. Acquaint yourself with the privacy settings.
   - Explore the privacy settings and try different options to find out what suits your preferences. Try to limit post viewing to specific people that you trust. Bear in mind that even if you set them to “private”, some photos may still be indexed publicly in Google Image Search, so if you don’t want your images found publicly simply do not post them.
3. Be sure to friend people you know and trust.
   - The more people you befriend on social media, the harder it gets to control the information you post. Do not hesitate to use the “block” feature if you are afraid that a person might take advantage of you and your information.
4. Avoid using the “tag into some location” feature.
   - Some criminals might take advantage of you and even do you harm if they know exactly your location.
   - Some criminals might even break into your house if they know you are away from it.

Co-funded by the
Erasmus+ Programme
of the European Union

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

Topic 2: Protecting personal data

WAYS OF PROTECTING PERSONAL DATA ON SOCIAL NETWORKS

5. Log out of a social media site when you are done.
   - If you are using a public device for signing in or even your own device, logging out of a social media site helps to ensure your account won't be hacked by another person having access to the device you were logged in with and verbally attack your friends, post embarrassing content on your behalf or worse change your personal information, your password or even lock you out of your own account.
6. Create strong, private passwords.
   - Strong passwords use a combination of upper and lowercase letters, numbers and special characters, that are easy to remember but tough for other people to guess or crack.
   - Avoid using easy and common passwords like birthdates, anniversaries and names of your pets.
   - Keep your passwords private, and if you have to write them down keep this secure and away from your computer.

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 1: Risks and responsibilities online

MeLDE

SUMMARY

In this topic teachers were introduced to the most common security measures. The topic also touched on how to stay safe on social media, how to keep mobile devices safe, and how to avoid harmful or offensive content on social media.

A few things to remember:

- Creating strong passwords for your online accounts is one of the most effective ways you can protect your personal data and information.
- Virus writers and malicious code engineers are constantly finding ways around the new technology features and holes in operating systems only help them in their efforts.
- If you are using security software for a long time and haven't updated it often since then, it's almost as good as not having Antivirus and Anti-Malware software installed.
- Hackers can take advantage of a software vulnerability by writing code to target the vulnerability and use your stolen personal information to commit crimes in your name or sell them on the dark web to enable others to commit crimes.
- Hackers nowadays are targeting smartphones and mobile devices alike, to gain access to personal information from text messages, Facebook and other social media applications, banking and shopping data, email messages, etc.

Have any questions?

You can find us at http://meldeproject.eu

Co-funded by the Erasmus+ Programme of the European Union

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

Topic 2: Protecting personal data

MeLDE

REFERENCES

- Protection of personal data. Retrieved from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en
- De Groot, J. (2019, December). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020. Retrieved from https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe
- How to create a good password. Retrieved from https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/how-to-create-a-good-password/
- McDonald, J. (2006, October). The Importance of Updating Antivirus Definitions. Retrieved from https://www.symantec.com/connect/blogs/importance-updating-antivirus-definitions
- Graham-Smith, D. (2017, March). 12 ways to hack-proof your smartphone. Retrieved from https://www.theguardian.com/technology/2017/mar/26/12-ways-to-hack-proof-your-smartphone-privacy-data-thieveshttps://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-to-tell-if-your-smartphone-has-been-hacked/

Co-funded by the Erasmus+ Programme of the European Union

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

Module 4: E-Safety

GLOSSARY

Term	Definition
Password	A secret word or expression used to gain entrance, access to a machine, site, etc.
Anti-malware	Anti-Malware is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices.
Antivirus	Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers, etc.
Malicious URL	Malicious URL is a link created with the purpose of promoting scams, attacks and frauds.

Co-funded by the
Erasmus+ Programme
of the European Union

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