Erasmus+

GoDIGITAL

Internet Safety

SPOŁECZNA AKADEMIA NAUK
UNIVERSITY OF SOCIAL SCIENCES
EUnipartners
PUBLICA FIDES
Emphasys CENTRE

2.2.1 TOPIC 1: INTERNET SAFETY

Internet could be compared to the ocean. The ocean can be a very dangerous place: people can be lost or drowned by trying to enjoy the sea or explore its enchanting immensity. But the mother in the photograph does not forbid her children's contact with the sea. Instead, she keeps them in touch with her and teaches them to enjoy it by explaining some rules for safe "use" of the sea. In the beginning she stands next to them and advises them so they gradually acquire autonomy and can themselves enjoy the sea later on.

This is how we should think about the use of the Internet. We need to identify the potential dangers of widespread Internet and acquire knowledge and ways to avoid all possible risks. It is then necessary to introduce young students to the adoption of good practices in relation to the safe use of the Internet.

Risks on the Internet are of many kinds. We outline ten (10) of the most important risks:

1. Internet addiction and alienation of users from the real world
2. Inappropriate and offensive website content

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

3. Unwanted messages (spam)
4. Internet bullying
5. Electronic seduction of users - Reporting on child pornography, online gambling, violent games and other harmful behaviors
6. Violation of user privacy
7. Misinformation disseminated on the Internet (false news, urban myths, digital pranks)
8. Interception of personal data through "phishing" and "pharming"
9. Malicious software that infects PCs
10. Physical conditions resulting from prolonged use of computers

We consider that nowdays, the theoretical knowledge of the above is not enough for a teacher. It requires familiarity and practical knowledge. For this reason, some technical issues will be developed in the following paragraphs, so that users and teachers in particular can be susceptible to, but also react to, possible online risks being able to protect and educate their students accordingly from an early age.

2.2.1.1 How to avoid bad sites

Before we begin to introduce ways to avoid “bad” web sites, we have to answer the question: what is considered as a “bad” site? A “bad” site is generally considered to be any website containing material that falls under categories 1 to 8 presented in the introduction above.

Some of the ways to avoid these kinds of websites are the following:

- **Use Internet filters**
  There are many Internet filters that someone can buy or download that will prohibit him/her or members of his/her family from opening any questionable sites. These filters work by preventing user access to sites that are deemed questionable safety-wise, or that present inappropriate or NSFW (not safe for work) content. Many parents use these filters to make sure that their kids are only using sites that are age-

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

appropriate, but people of all ages, as well as teachers, can use them to make sure that their web searches are always safe.

- **Take advantage of search engines' built-in filters**
  Many search engines give Internet users the option of choosing a "safer" search when using their services. For example, Google offers “safe search filtering”. This goes for all image and video searches, as well as news and general search content.

- **Don't guess the address of a Web site**
  This is probably the number one way that people get into trouble. There are many sites that use similar Web addresses as legitimately safe websites so that when people try to remember which site to go to, they end up visiting the wrong site accidentally.

- **Never click on sites that seem questionable**
  When someone is in doubt, he may not click. If the site description, title, or URL seems in any way "off" to him/her, he/she may find another site that is more reputable, especially when using that site in a research capacity.

2.2.1.2 Introduction to malware – How to avoid

Risk number 9 in the introduction talks about malware. Malware is a term that is used for malicious software that is designed to do damage or unwanted actions to a computer system. Examples of malware include the following: Viruses, worms, trojan horses, spyware and rogue security software.

Here is a brief description of each of these types of malicious software so that the teacher is familiar with the terminology and especially with the way each of these software works.

- **Computer viruses**
  A computer virus is a small software program that spreads from one computer to another and interferes with computer operation. A computer virus might corrupt or

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

delete data on a computer, use an email program to spread the virus to other computers, or even delete everything on the hard disk. Computer viruses are frequently spread by attachments in email messages or by instant messaging messages. Therefore, the user must never open an email attachment unless he/she knows who sent the message. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Computer viruses also spread through download on the Internet. They can be hidden in pirated software or in other files or programs that someone might download.

- **Computer worms**
  A worm is computer code that spreads without user interaction. Most worms begin as email attachments that infect a computer when they're opened. The worm scans the infected computer for files, such as address books or temporary webpages, that contain email addresses. The worm uses the addresses to send infected email messages, and frequently mimics (or spoofs) the "From" addresses in later email messages so that those infected messages seem to be from someone you know. Worms then spread automatically through email messages, networks, or operating system vulnerabilities, frequently overwhelming those systems before the cause is known. Worms aren't always destructive to computers, but they usually cause computer and network performance and stability problems.

- **Trojan horses**
  A trojan horse is a malicious software program that hides inside other programs. It enters a computer hidden inside a legitimate program, such as a screen saver. Then it puts code into the operating system that enables a hacker to access the infected computer. Trojan horses do not usually spread by themselves. They are spread by viruses, worms, or downloaded software.

- **Spyware**
  Spyware can install on a computer without the users' knowledge. These programs can change the computer's configuration or collect advertising data and personal information. Spyware can track Internet search habits and can also redirect the web browser to a different website than the one the user intends to go to.

- **Rogue security software**
  A rogue security software program tries to make the user think that his/her computer is infected by a virus and usually prompts hime/her to download or buy a product that removes the virus. The names of these products frequently contain words like Antivirus, Shield, Security, Protection, or Fixer. This makes them sound

Erasmus+

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

(including the X in the corner). Close the window via Windows Task Manager (press Ctrl-Alt-Delete).

- **From another piece of software:** Some programs attempt to install malware as a part of their own installation process. When installing software, pay close attention to the message boxes before clicking Next, OK, or I Agree. Scan the user agreement for anything that suggests malware may be a part of the installation. If you are unsure, cancel the installation, check up on the program, and run the installation again if you determine it is safe.

- **From illegal file-sharing services:** You're on your own if you enter this realm. There is little quality control in the world of illegal software, and it is easy for an attacker to name a piece of malware after a popular movie, album, or program to tempt you into downloading it.

2.2.1.3. How to remove malware

If someone suspects malware—or he/she just wants to be careful— there are a few steps he/she should take.

a) **Back up all files and other data**
Files and data are critical. Therefore the moment someone realizes his/her computer is malware-infected, he/she must back up all the files and other data, before the malware gets to those files and other data and corrupts them. Moreover, such backing up will help get back on track quickly.

b) **Disconnect from the Internet**
Next best thing is to disconnect the PC from the internet to prevent further damage, since the internet is the breeding place for malware. And every moment the user

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

stays connected with it, especially after a malware infection, is going to worsen his/her situation.

c) **Scan computer in safe mode**
Switch to safe mode and scan the computer. Without getting too technical, safe mode is a restricted mode which allows only healthy applications to run thereby reducing the risk of malware spreading to other parts of the PC. At best, such a cleanup can improve the PC performance. Another simple but effective measure would be to clean up the temporary and download files.

d) **Use malware removal tool**
If there isn ’t already one, download a legitimate anti-malware program. Next, install and run it. Programs like these are designed to search out and eliminate any malware on a device.

Once the device is clean, it’s a good idea to change the passwords, not only for the PC or mobile device, but also for email, for social media accounts, for favorite shopping sites, and for online banking and billing centers.

Removing malware is neither an easy task nor an attractive one. Therefore it's best to let experts handle the situation if someone thinks he/she cannot solve the problem by himself/herself.

2.2.1.4 Securing Internet accounts

Passwords are like keys to our personal home online. We should do everything we can prevent people from gaining access to our password. We can further secure our accounts by using additional authentication methods. Some main tips are:

- Close the accounts that you are not using for a long time
- Create a strong password (i.e. make your password a sentence)
- Unique account – unique password
- Write it down and keep it safe
- Change your passwords regularly
- Lock down login (strong authentication)
- Check your account activity
- Keep your software updated
- Specify your trusted contacts

More ideas about Internet safety can be found in the additional literature proposed.

Erasmus+

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543

2.2.1.5 GDPR

Another important issue teachers should be aware of is the GDPR. The General Data Protection Regulation ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA, and applies to an enterprise established in the EEA or—regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.

Controllers of personal data must put in place appropriate technical and organisational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject. The data subject has the right to revoke this consent at any time. (from Wikipedia, the free encyclopedia)

Erasmus+

This project has been funded with support from the European Commission. This 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.
Submission Number: 2017-1-PL01-KA201-038543