5. Internet – Addressing the challenge

> “To deny people their human rights is to challenge their very humanity.”
>
> *Nelson Mandela, Nobel Peace Prize laureate of 1993, anti-apartheid activist, President of South Africa 1994-1999*

> “The rights of every man are diminished when the rights of one man are threatened.”
>
> *John F. Kennedy, President of the USA 1961-1963*

CHECKLIST FACT SHEET 19 – CYBERCRIME: SPAM, MALWARE, FRAUD AND SECURITY

Have you set up strong different passwords for your accounts and configured two-factor security?

Have you explored security settings for your devices/accounts?

Are your operating system and your applications up to date?

Have you made a backup of your most important data?

CHECKLIST FACT SHEET 20 – LABELLING AND FILTERING

Have you thought about the cultural and moral implications of filtering?

Do you know the difference between a “black list” and a “white list”?

Are you familiar with the most commonly used labelling systems for children’s content, and what they signify?

CHECKLIST FACT SHEET 21 – ONLINE HARASSMENT: BULLYING, STALKING AND TROLLING

Do you have a clear family or school policy in place so that children understand the repercussions when they are involved in online harassment?

Do you protect your personal details sufficiently? Many online problems are caused through ill-advised sharing of photos and information.

Have you investigated how to build better social and emotional skills (otherwise known as social literacy) to overcome the anonymity and “facelessness” of online communication that facilitate bullying, trolling and harassment in general?

CHECKLIST FACT SHEET 22 – GETTING ASSISTANCE

Do you and your children/pupils know where to report illegal content?

Do you ever check statistics reported by helplines to understand emerging trends and risks?

What are the top five digital skills that will best protect you online?

Do you understand geolocation and Bluetooth sufficiently to use your mobile devices comfortably and safely?

M-learning and mobile wallets are areas in which the use of mobile devices is changing the way we learn, work and shop. What do you know about these recent evolutions?

Fact sheet 19

Cybercrime: spam, malware, fraud, security

While the Internet is a great way to access quality content and services, it can also serve the purpose of ill-intentioned people by disseminating spam, viruses, malware and scams.

- **Cybercrime** comprises offences against computers and data, for example illegal access to a computer (also called hacking), interception of a communication, preventing a computer from functioning or damaging or deleting data, but also offences committed by means of computers, such as fraud or sexual violence against children. Malware, spam and phishing and other forms of identity theft are some of the tools used by cybercriminals.
- **Malware**[1] is an umbrella term used to refer to a variety of forms of hostile or intrusive software, which includes viruses, trojan horses and others. The objectives of malware are very diverse. They can aim simply to disrupt the functioning of your computer by damaging the software or corrupting the hardware, or they may steal information and data which can be monetised in some way or

[1] https://en.wikipedia.org/wiki/Malware

another. Your infected computer may also become a "bot" that is controlled by criminals without your knowledge; it may then be used together with millions of other infected computers as part of a "botnet" to spread spam, commit fraud, or carry out attacks against hospitals, airports or banks.

- **Spam**[2] refers to the mass mailing of unsolicited messages to multiple recipients. It is most commonly associated with e-mail, but also applies to social networking, instant messaging, mobile phones and so forth. Fortunately, most e-mail services have efficient spam filters. Spam may also serve as a vector to spread different types of malware, for example when a recipient opens an attachment or a link indicated in the spam mail.
- **Phishing**[3] derives from "fishing for passwords" and is one form of identity theft. For example, recipients receive spam, which is disguised as legitimate mail from a known institution such as a bank or a social network. These mails often contain links to false websites, which are used to gather sensitive user information such as credit card numbers or passwords. The stolen identity information is then often used to commit fraud.
- **Internet fraud**[4] has greatly developed over the last few years as the possibilities for e-commerce and making payments online have multiplied. Internet fraud encompasses different types of fraud such as counterfeits, real estate fraud, premium service SMS ring tones, money transfer fraud and so forth.

SO HOW CAN YOU STAY SAFE?

Your online security can be compared to security at home. You protect the contents by keeping the windows closed and the door locked. A healthy degree of scepticism, critical thinking and ICT skills will also help in preventing you from falling for fraud, phishing, malware or scams online.

Many of the issues relevant for security are also relevant for privacy (see Fact sheet 9).

PERSONAL DEVELOPMENT AND EDUCATIONAL VALUE

Security is as important for your sake as for the sake of all Internet users. Malware, viruses and spam spread mostly through users themselves! If your computer or device is not safe, all your friends and contacts might be exposed to security risks as well!

Knowledge about Internet security and safety is very valuable for the further development of digital literacy skills, as it pushes users to dig deeper into the parameters and settings of their devices and the online services they use, and to gain better technical knowledge about how their devices, their operating systems and the Internet works.

POTENTIAL RISKS

Spam

- Spam is usually benign and the consequences are mostly a great loss of time by having to sort through it, or time wasted clicking on links.
- Spam often includes false or fraudulent information. Because the sender remains anonymous, it is usually not possible to prosecute for false claims.
- Spammers often prey on the goodwill of recipients in order to gather mail addresses for their databases. For example, mails may be sent requesting recipients to add their personal information to a list in order to support a petition or cause. Often citing a cause such as a sick child requiring surgery, it falsely claims that a company or organisation has promised that money will be paid each time it is forwarded.

[2] https://en.wikipedia.org/wiki/Spamming
[3] https://en.wikipedia.org/wiki/Phishing
[4] https://en.wikipedia.org/wiki/internet_fraud

- New techniques of spam appear every day. For instance, on social networks, spam can take the form of "click jacking"[5], with posts shared by friends that include catchy titles such as "the top 10 ways to lose weight" or "you won't believe what this girl does in front of her webcam". The consequences can be that you visit a website that exposes you to a ton of advertising to generate revenue, or forces you to like a page that will spam you with many more posts.
- There are many types of online fraud and new ones appear every day as technology evolves. A common fraud is called "419", named after a Nigerian law prohibiting this type of victimisation. This typically involves promises of a share of a large sum of money in return for help with bank transfers. Another fraud consists in asking the victim to send money as a rental deposit guarantee via Western Union before visiting an apartment for rent.

Phishing and identity theft

- The risks of falling prey to phishing and identity theft are much more serious. Depending on what information you have provided through the phishing attempt, the detriment can be anything from losing control of a relatively unimportant online account such as an online forum to losing control of extremely important accounts such as your main e-mail address which can then lead to all of your online accounts being compromised!
- Once your accounts have been compromised, your data can be at risk. The contents of all your e-mails can be downloaded for instance. This data can prove to be very valuable, either for extorting money from you or your contacts, using your accounts online to order items, using your credit card, impersonating you online, etc.

Malware

- The risks of installing malware are akin to phishing and even spam or worse. Malware can be used for phishing purposes to steal information about your accounts (using a key logger[6] for instance), for spamming purposes to bombard you with pop-ups, notifications or default home screens inside your browsers, and also for other purposes, such as stealing information and data directly from your computer or disrupting the functioning of your computer, taking control of your computer to commit crimes, activating microphones or cameras of your devices to spy on you, and potentially destroying the content altogether.
- Techniques aimed at fooling the user into installing malware are developing rapidly as well. An example is a fake pop-up window which realistically emulates an antivirus scan of your computer. At the end of the fake scan, dangerous viruses are supposedly identified on your computer, and to get rid of them you must install a software – which is actually a Malware or virus!

IDEAS FOR CLASSROOM WORK

- Ask the children and young people to work in groups of three or four and propose a strong password for a fake online account. Make it clear that they should come up with a new password and not an existing password that they already use! Have the different teams present their password and ask the rest of the group to identify the features of a strong password by looking at the proposals.
- A strong password:
  - ▶ is at least eight characters long;
  - ▶ does not contain a word found in a dictionary, does not contain a reference to your personal life or your user name, real name or company name;
  - ▶ contains characters from each of the following categories: uppercase letters, lowercase letters, numbers and symbols.

[5] https://en.wikipedia.org/wiki/Clickjacking
[6] https://en.wikipedia.org/wiki/Keystroke_logging

- A CERT (computer emergency response team), also known as CSIRT (computer security incident response team) is an expert group that handles computer security incidents. Have your students find your national CERT/CSIRT and find out more about the role and functioning of these teams.
- Victims of cybercrime often do not report the crime to the police, and so offenders continue with their business and find new victims.

► Ask your students to find out about how to report a crime to the police or other public authorities, including through hotlines.

► Ask your students to find out what constitutes cybercrime under the laws of their country.

GOOD PRACTICE

- One of the consequences of Internet users expecting to get everything online for "free" has been the continuous development of malware or spam attached to "free" software or services that are used online. The online environment is a shared responsibility and is the result of users' individual online behaviours and choices. By financially supporting quality services/content/software (via donations for open source endeavours or purchasing licences or subscriptions to commercial organisations) you contribute to making the online environment safer.
- User friendliness can be the enemy of security. For instance, you can configure your operating system to ask for an administrator password whenever an important action is performed (for example installation of new software). It can be extremely frustrating and tedious, but that is the price to pay for more security! Keep that in mind when setting up your operating system's security settings.
- If you are managing more than one user of a computer or network, make sure each user has appropriate rights. Restricting unnecessary user rights can help avoid accidental or deliberate security problems.
- Make sure you trust the source before downloading anything to your computer. Be particularly aware of peer-to-peer software[7], which is notorious for aiding the distribution of malware (see Fact sheet 14 on music and images). Whenever you install software, make sure you read all the steps before clicking on the "next" button. Pay specific attention to pre-ticked boxes which may install malware to your computer!
- Install anti-virus software[8] and keep it updated.
- Install security patches or operating system updates as soon as they become available. You can set some operating systems and programs to update automatically or inform you as soon as a patch is available for download.
- Install a firewall[9] to control traffic to and from your computer.
- Use different e-mail accounts for different purposes to avoid giving out your "personal" e-mail address all the time (for example registering on forums, filling out forms, etc.) and avoid distributing your e-mail address on a large scale. Bear in mind that if you include your e-mail address on a website, web crawlers can pick it up and add it to distribution lists for spam. Also, do not respond to spam. This will confirm your e-mail address to the spammer. Be aware that links promising to remove you from their mailing list may not be genuine.
- If you do need to post your e-mail address, you can disguise it by adding characters such as Tom(dot)Smith(at)gmail(dot)com, or posting it as a picture so that it cannot be automatically copied.
- Maintain a healthy scepticism about e-mails you receive. Do not open e-mails if you do not

[7] https://en.wikipedia.org/wiki/Peer-to-peer
[8] https://en.wikipedia.org/wiki/Antivirus_software
[9] https://en.wikipedia.org/wiki/Firewall_(computing)

trust the source. Always check the e-mail address of any notification you receive to check whether it is genuine.

- Be especially wary of attachments. If you receive something that looks suspicious, or that you have not requested, delete it immediately without opening it.
- Never click on links from recipients you do not trust, and more especially on links that use shortened URLs where it is impossible to see the "original" URL address. Remember that even recipients that you trust can send you infected messages if their account or device has been compromised.
- Never send or post private information such as a username and password or a credit card number by e-mail. No online service will ever ask you to submit your username and password via e-mail and you will only be asked to share details such as your credit card number on very rare occasions (for example, when reserving a hotel room you may need to send this information to the official reservation e-mail address of the hotel).
- Use different passwords for your most important accounts and be sure to set up two-factor security measures whenever possible (adding your mobile phone number or an extra security phrase/question). Make sure that your passwords have no obvious connection to you, are at least eight characters long and use a combination of letters (lower case and upper case), numbers and symbols.
- Make regular backups of all your data on an external hard drive. Many backup software programs exist and automatically and regularly backup your data. Some of these are even included inside your operating system (Windows, MacOS, Linux, etc.). Be sure to stay informed[10].

FURTHER INFORMATION

- Truth or Fiction is a website for Internet users to check up on claims made by commonly forwarded e-mails: *<http://www.truthorfiction.com/>*.
- Find out more about combating spam: *<http://spam.abuse.net>* and *<http://www.spamhelp.org/>*.
- For information about Microsoft security, see: *<http://www.microsoft.com/security/>*.
- For information on Apple security, see: *<http://www.apple.com/support/security/>*.
- ENISA, the European Union Agency for Network and Information Security gives regular updates on digital security issues: *<http://enisa.europa.eu>*.
- The Council of Europe has a web page entitled "Action against cybercrime": *<www.coe.int/cybercrime>*.
- TechTarget is an information security magazine: *<http://informationsecurity.techtarget.com/>*.
- Helpful information and user tests on topics from cookies to IP addresses to browser checks can be found at: *<http://www.2privacy.com/>*.
- Online security advice from the government of the UK can be found at *<https://www.getsafeonline.org>* and for the United States at *<http://www.us-cert.gov/>*.
- Find your national computer emergency response team through a web search using CERT and your country name.
- Although the information security guidelines offered by the Direct Marketing Association *<http://www.the-dma.org/guidelines/informationsecurity.shtml>* are intended for direct marketers, they also provide useful tips for anyone concerned about online security.

[10] https://en.wikipedia.org/wiki/List_of_backup_software

- Relevant UN Convention on the Rights of the Child articles:

Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Article 17 – Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand, and should not promote materials that could harm children.

Article 34 – The government should protect children from sexual abuse.

Article 36 – Children should be protected from any activities that could harm their development.