MIG-DHL

Migrants Digital Health Literacy

Handbook

Module 6

Being Active in the Digital Health Environment

Authors:

Josemar Alejandro Jimenez, Oxfam; Jenny Wielga, IAT

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. Project number: 2020-1-DE02-KA204-007679.

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

MIG-DHL Migrants Digital Health Literacy

This handbook is a part of the MIG-DHL Programm containing 6 learning modules in total, which has been developed within the Erasmus+ Strategic Partnership **MIG-DHL- Migrants Digital Health Literacy.**

The training contents at a glance:

MIG-DHL Programm

- Module 1: What is Digital Health Literacy and its relevance
- Module 2: Main health issues when landing in a new country
- Module 3: Healthcare Services
- Module 4: Turning Digitally Literate
- Module 5: Exploring Digital Health Tools
- **Module 6: Being Active in the Digital Health Environment**

You can find more information at the homepage: https://mig-dhl.eu/

Contract No. 2020-1-DE02-KA204-007679

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

MIG-DHL Migrants Digital Health Literacy

Declaration on Copyright:

Content

6. Being Active in the Digital Environment

For being active in the digital environment, it is very important to know how to protect privacy for improving the protection of personal data in the digital environment and also for protecting the physical and psychological health.

Therefore, this module focused on protecting privacy. The information in this module is a follow-up to the topics already addressed in Module 4. Especially related to the development of competencies in relation to security and privacy. These competencies refer to the ability to protect devices, content, personal data, and privacy in the digital environment. The implication of this action also allows the protection of physical and mental health, well-being and social inclusion. This part is related to the competence area 4 “Saftey” of DigiComp, which is already introduced in module 4.

6.1 Protecting privacy and personal data in the digital environment

For privacy and personal data do exist a lot of different risk factors in the digital environment. Some of the main risk factors, which are also pointed out in the training materials, are described in the following part more detailed.

6.1.1 Hacking

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. And while hacking might not always be for malicious purposes, nowadays most references to hacking, and hackers, characterize it/them as unlawful activity by cybercriminals—motivated by financial gain, protest, information gathering (spying), and even just for the “fun” of the challenge.

Hacking is typically technical in nature. But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data.

In fact, it's accurate to characterize hacking as an over-arching umbrella term for activity behind most if not all of the malware and malicious cyberattacks on the computing public, businesses, and governments. Common hacking techniques include:

- Botnets
- Browser hijacks
- Denial of service (DDoS) attacks
- Ransomware
- Rootkits
- Trojans
- Viruses
- Worms

Types of hacking/hackers

Broadly speaking, you can say that hackers attempt to break into computers and networks for any of four reasons:

- There's criminal financial gain, meaning the theft of credit card numbers or defrauding banking systems.
- Next, gaining street cred and burnishing one's reputation within hacker subculture motivates some hackers as they leave their mark on websites they vandalize as proof that they pulled off the hack.
- Then there's corporate espionage, when one company's hackers seek to steal information on a competitor's products and services to gain a marketplace advantage.

Hacking prevention

- Anti-malware protection: First and foremost, download a reliable anti-malware product (or app for the phone), which can both detect and neutralize malware and block connections to malicious phishing websites.
- Be careful with apps: Second, only download phone apps from the legitimate marketplaces that police themselves for malware-carrying apps, such as Google Play and Amazon Appstore. (Note that Apple policy restricts iPhone users to download only from the App Store.) Even so, every time you download an app, check the ratings and

reviews first. If it has a low rating and a low number of downloads, it is best to avoid that app.

- Protect your info: Know that no bank or online payment system will ever ask you for your login credentials, social security number, or credit card numbers by means of email.
- Update your software: Whether you're on your phone or a computer, make sure your operating system remains updated.
- Browse carefully: Avoid visiting unsafe websites, and never download unverified attachments or click on links in unfamiliar emails.
- Password safety: All the above is basic hygiene, and always a good idea. But the bad guys are forever looking for a new way into your system. If a hacker discovers one of your passwords that you use for multiple services, they have apps that can breach your other accounts. So make your passwords long and complicated, avoid using the same one for different accounts, and instead use a password manager. Because the value of even a single hacked email account can rain disaster down on you (Malwarebytes, 2020).

6.1.2 Computer viruses

A computer virus is one of the most common forms of hacking. Similar to a flu virus, it is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

How does a computer virus attack? Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to

execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed. This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do. While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.

How do computer viruses spread? In a constantly connected world, you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files. To avoid contact with a virus, it's important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

What are the signs of a computer virus? A computer virus attack can produce a variety of symptoms. Here are some of them:

- Frequent pop-up windows. Pop-ups might encourage you to visit unusual sites. Or they might prod you to download antivirus or other software programs.
- Changes to your homepage. Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.
- Mass emails being sent from your email account. A criminal may take control of your account or send emails in your name from another infected computer.
- Frequent crashes. A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on.

- Unusually slow computer performance. A sudden change of processing speed could signal that your computer has a virus.
- Unknown programs that start up when you turn on your computer. You may become aware of the unfamiliar program when you start your computer. Or you might notice it by checking your computer's list of active applications.
- Unusual activities like password changes. This could prevent you from logging into your computer.

How to help protect against computer viruses? How can you help protect your devices against computer viruses? Here are some of the things you can do to help keep your computer safe.

- Use a trusted antivirus product, and keep it updated with the latest virus definitions.
- Avoid clicking on any pop-up advertisements.
- Always scan your email attachments before opening them.
- Always scan the files that you download using file sharing programs (Norton, 2020).

6.1.3 Data theft

(includes: Associated identity theft, Credit card account information, Customer credentials)

Data theft is the act of stealing digital information stored on computers, servers, or electronic devices of an unknown victim with the intent to compromise privacy or obtain confidential information. Information can include anything from financial information, like credit card numbers or bank accounts, to personal information, like social security numbers, drivers license numbers, and health records.

How Does Data Theft Happen? Data theft occurs through a variety of means. Most often, it happens because someone hacked into a computer system to steal sensitive information, such as your credit card or personal information, or an employee at a company mishandled the information. With an increasingly digital world, hundreds of different businesses and organizations hold your personal information, such as your social security number, mailing address, birthdate, and bank account information.

How to Protect Yourself? Data theft is a real problem and it can happen to anybody. While there is no way to completely prevent data theft from happening, there are multiple steps you can take today to limit your risk.

- Pay using cash instead of credit or debit cards.
- Use a credit or debit card with pin-and-chip technology.
- Protect your computer from viruses and malware by installing, using, and updating antivirus and anti-spyware software on all your computers and electronic devices.
- Keep all operating systems and software programs up to date by regularly installing updates to security, web browsers, operating systems, and software programs as soon as they become available.
- Don't open questionable emails or email attachments as they could be phishing emails.
- Regularly check your credit card statements and credit report for unauthorized charges and new credit lines.
- Use a strong, unique password for all websites that require logins. Regularly change these, especially if an account password has been compromised in a data breach.
- Use only secure Wi-Fi connections.
- Properly dispose of documents containing sensitive information through shredding paper and removing all data from electronic devices (Michaud, 2021).

6.1.4 Spam-mails

Sometimes you receive unwanted e-mails - on the one hand, this is time-consuming because you have to sort through the unwanted e-mails, but on the other hand, so-called spam e-mails can also contain dangers such as viruses or harmful programmes that install themselves on your computer when you open the e-mail and can e.g. spy out your access data. Phishing is also a common type of online scam where criminals send official-looking emails in an attempt the user to reveal details that may be used for identity theft.

- Therefore:

- Avoid opening attachments unless they have been through an anti-virus program,
- remember to log off, especially when using a shared public computer,
- delete all emails from unknown persons,
- never reply to spam.

- How to identify spam mails?
  - Grammar and spelling mistakes
  - Mails in a foreign language
  - Missing name
  - Urgent need for action - especially in combination with a threat
  - Request to enter personal data (e.g. PIN or TAN)
  - Request to open a file
  - Never received any e-mails from the bank or not a customer so far (Verbraucherzentrale, 2021).

References

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. doi:10.2760/38842

Michaud, Katelyn. (2021). *What is Data Theft?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Google Search Operators.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Essential Skills for Consumer Health in a Networked World. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *What is a computer virus?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Hacking definition: What is hacking?* https://www.malwarebytes.com/hacker

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet*. https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

World Health Organization [WHO]. 2017. *Digital Health Literacy*. https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf