DSSI Training Course

MODULE 3 – SAFETY ONLINE

E-BOOK

DIGITAL SERVICES & SENIOR'S INCLUSION

Funded by the European Union

1. PROJECT INTRODUCTION

The DSSI consortium acknowledges the importance of facilitating access to the digital service environment and enhancing the inclusion of older people. Nowadays, a high percentage of older people have problems understanding new technologies and making use of them in their daily lives. In addition, this collective lacks the necessary tools and support to upgrade their digital skills and knowledge, which unfortunately further increases the exclusion of older people.

Therefore, DSSI was created with the main goal of defending the rights of older people (low-skilled, living in remote areas, with mobility difficulties, immigrants, etc.) so that they can access information and enjoy their right to participate in everyday society as independent citizens, through digitally active aging.

This will be facilitated by using library networks, as their role is starting to evolve into a hub for digital information and services, due to the accelerated digital transformation of the post-COVID era. In fact, the project is using the wide network of libraries as a digital information hub where senior citizens can acquire basic digital skills and apply their knowledge by searching and accessing the fantastic range of libraries' digital services on health and wellbeing, lifelong learning, cultural and social connectivity and finally e-commerce and e-governance.

Through the training Modules that are created in the DSSI Training Course, older people will be enabled to make full use of the wide range of library services available online and enjoy the benefits of inclusiveness. In addition, through this project, older learners will gain confidence to independently use a range of public and commercial digital services.

Funded by
the European Union

2. Obsah

Funded by the European Union

3. MODULE SUMMARY & LEARNING OUTCOMES

Module 3	Safety online
No. of Units	6
Topics/Units	• Basic terminology in Cyber security for not being lost • Where and why can we encounter attacks? • We look at phishing emails • We dive into phishing websites • How to create a safe password • Other online and offline threats
EQF-Level / Education Level	4
Duration	90 min
Learning objectives	• Theory and praxis with all relevant topics. • Encountering and learning from many specific examples. • Learning what to share and how to interact online. • Learning how to safely do commercial transactions. • Discussing experiences and possible problems.
Knowledge	• They understand basic terminology concerning the topics. • They gain basic online safety knowledge and apply it in daily life • They understand, gain basic knowledge on safety. principles and practices and can evaluate threats and apply measures.
Skills	• Participants will be able to recognize the threats of cyber attacks, analyze the situation and solve the problem. • They will be able to accurately determine what is a phishing email / site. • They will be able to create safe passwords and learn how to store them. • They will be able to able to apply safe commercial transactions. • They will be able to apply the knowledge on safety online in solving certain problems with cyber attacks, phishing emails, websites, etc.
Competence	• Participants will be able to combine the knowledge of online safety with the skills of safe behavior using online space and transfer it into the competence (specific situations like strange emails, websites or calls, phishing, passwords, commercial transactions, etc.)
Further Information/Sources	• Online course from Comenius University • What is malware, 2023. In: Cisko [online]. United States, California: Cisco Systems, Inc. [cit. 2023-03-27]. Dostupné z: https://www.cisco.com/site/us/en/products/security/what-ismalware.html • https://skillmea.sk/online-kurzy/uvod-do-it-bezpecnosti

Funded by the European Union

4. INTRODUCTION

The internet has become indispensable in our daily lives, impacting people of all ages, including seniors. Many essential activities now rely on internet access, highlighting its significance. Imagine going a week without it—no connecting with relatives, watching TV, reading news, playing games, or even browsing for dinner recipes. While the internet is a powerful tool, it also poses risks, with hackers exploiting vulnerabilities.

Despite common misconceptions, individuals are not immune to cyber threats. Many believe cybersecurity is solely the concern of large institutions, leaving seniors particularly vulnerable. Even with advanced security software, users often inadvertently disclose sensitive information like login credentials or credit card details.

Why would hackers target us? We might not consider ourselves important or wealthy, so why the interest? There are several reasons. The internet space has no borders, making us susceptible to attacks from anywhere in the world. Firstly, if we use computers, tablets, or smartphones connected to the internet, we are a potential target. These devices have processing power and store personal information, making them appealing to hackers. They may exploit our device for wicked purposes or simply harvest personal data, passwords, and credit card numbers to sell or misuse.

Imagine you have purchased a security door, and the company has installed it correctly, explained its use, and handed you the keys. If you start using the door by just opening and closing it, without locking the door, it becomes just a decoration. You as the final user are responsible for locking the door, so it can function properly.

Similarly, in the digital world, cyber-attacks are increasing in frequency and sophistication, requiring us to respond proactively and effectively to minimize potential risks. Our most valuable assets lie in our health, family, and finances, yet it is our financial resources that attract hackers' attention. Their primary aim is to gain access to our funds, as evidenced by instances where individuals, particularly seniors, have fallen victim to scams and unknowingly sent money to strangers. This course aims to equip you with the knowledge and skills necessary to make informed decisions and safeguard against such threats. Through comprehensive instruction, you will learn to identify and avoid cyber risks, ultimately empowering you to protect yourself and your assets. In essence, it is about using digital security measures as effectively as locking a security door.

Funded by
the European Union

5. GENERAL OVERVIEW & OBJECTIVES OF THE MODULE

The course comprises six topics, each covering theoretical information along with numerous practical examples.

- Theory and practice covering all relevant topics.
- Engaging with and learning from numerous specific examples.
- Learning about appropriate online interactions and information sharing.
- Acquiring skills to conduct commercial transactions securely.
- Discussing experiences and potential problems.

6. TOPICS

- Basic terminology in Cyber security.
- Where and why can we encounter attacks?
- We look at phishing emails
- We dive into phishing websites
- How to create a safe password
- Other online and offline threats

7. DESCRIPTION OF THE LEARNING OUTCOMES

- Learners understand basic terminology concerning the topics.
- Learners understand and gain basic knowledge relevant to safety online and can apply it into their everyday life.
- Learners understand and gain basic knowledge on safety principles and practices and are able to evaluate threats and apply measures.
- Learners will be able to recognize the threats of cyber-attacks, analyze the situation and solve problems.
- Learners will be able to accurately determine what is a phishing email or a phishing site.
- Learners will be able to create safe passwords and learn how to store them.
- Learners will be able to apply safe commercial transactions.
- Learners will be able to apply the knowledge on safety online in solving problems with cyber-attacks, phishing emails, websites, etc.
- Learners will develop skills to be cautious not only within the online space.
- Learners will be able to combine the knowledge of online safety with the skills of safe behavior in online spaces and transfer it into competence. This can ensure their cyber security in specific situations, so they know how best to approach strange emails, bogus websites and calls, phishing, passwords, commercial transactions, etc.).

8. CHAPTER 1: ESSENTIAL TERMINOLOGY IN CYBERSECURITY TO KEEP YOU ON TRACK.

This chapter covers internet safety basics, explaining important terms and concepts. It is essential to become familiar with these terms in order to stay safe online and protect yourself from cyber dangers.

1. **“MALWARE”** refers to malicious software designed to harm your computer, network, or server. Attackers can gain various benefits from malware, such as stealing information, using your computer for illegal activities, or coercing you into financial transactions or decisions. Within the category of malware, there are subgroups worth knowing about.
   a) **"VIRUSES"** were once common but are now less prevalent.
   b) **"KEYLOGGERS"** records your keystrokes as you type, either through physical devices or software.

2. **"TROJAN HORSES"** are another significant group, which is less common now. The include types like "ADWARE," "SPYWARE," "EXPLOIT," and "RANSOMWARE." This type of malware, downloads onto a computer disguised as a legitimate program.
   a) **"ADWARE"** spreads advertisements or monitors user behavior to tailor ads.
   b) **"SPYWARE"** infiltrates computers to gather sensitive information discreetly.
   c) **"RANSOMWARE"** locks computers and demands payment for access restoration.

3. **"SPAM"** and **"JUNK"** mail might seem similar in this context. However, they refer to unsolicited emails, often aimed at selling products. While some people view Spam and Junk mail as unethical, many businesses still use spam. However, spam email can also be a malicious attempt to gain access to your computer.

4. **"SCAMS"** involve deceitful attempts to obtain money, often with promises of large sums or romantic interests.

5. **"PHISHING"** involves fraudulent emails or websites posing as legitimate institutions to trick users into revealing personal information.

6. **"VISHING"** is similar but occurs over phone calls. This is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.

7. **"HOAXES"** are false, inflammatory information meant to provoke strong emotional reactions.

Understanding the fundamental terms and concepts of internet security is crucial for safeguarding ourselves in the digital age. By familiarizing ourselves with these terms, we empower ourselves to recognize and avoid potential threats online. Having appropriate knowledge, we can navigate the online world with confidence, protecting ourselves, and our personal information from cyber threats.

9. CHAPTER 2: WHERE AND WHY CAN WE ENCOUNTER ATTACKS?

In the online world, attacks often occur through automated software called **"MALWARE"**, which spreads in various ways to target internet users.

One common method is **"SOCIAL ENGINEERING"** where attackers exploit human behavior rather than technological vulnerabilities. They manipulate users by appealing to their emotions, leading them to trust and act upon deceptive information received via email, text, or phone calls. Victims may only realize they have been scammed when their computer is compromised, or their bank account is drained later on.

Other methods of spreading malware include so called **"INSTANT MESSAGING"** through social media or communication apps or text messages, vulnerabilities in **"outdated APPLICATIONS**", malicious **"ADVERTISEMENT BANNERS"** on websites, and **"infected DEVICES"** like USB drives. Additionally, illegally downloaded software or games, known as **"CRACK SOFTWARE"** can contain hidden malware, especially on shared home devices.

Lastly, **"E-MAIL"** remains the most common pathway for malware, accounting for 60% of all attacks. Users may receive emails containing links or, in the past, attachments, though email filters often catch the latter.

Recognizing and responding appropriately to these threats falls on the end user's shoulders. It is inevitable for individuals to stay alert and informed about various tactics used by cyber criminals to spread malware. Regularly updating software and applications, being cautious when clicking on links or downloading files, and implementing robust security measures are essential steps in minimizing risks of malware infections. Additionally, educating oneself and others about the importance of cybersecurity and practicing safe online habits can significantly contribute to overall digital safety.

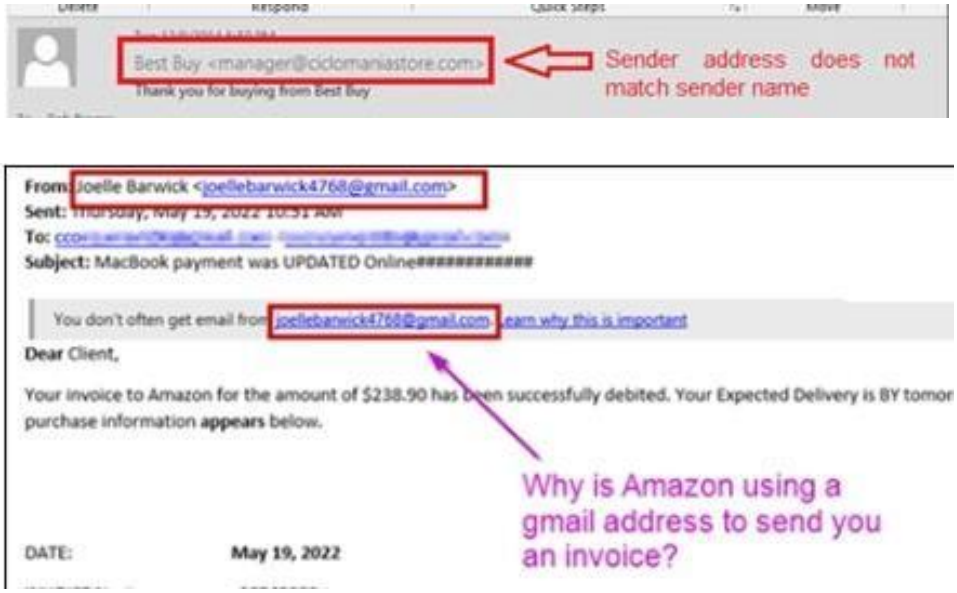
10. CHAPTER 3: WE LOOK AT PHISHING EMAILS.

In this section, we will discuss phishing. The term **"PHISHING"** sounds like "fishing," which involves catching something, but not fish. Instead, it is a method of tricking people into giving away their personal information. Attackers use bait, and if we are not careful, they will obtain our login details and other data we unintentionally provide.

Phishing can occur in various places, but the most common is through email. You might receive a seemingly legitimate request from someone, making it difficult to distinguish between what's genuine and what's not. When you receive an email, even if it appears to be from a trusted source like your bank, there are key things to pay attention to.

1. **Check the SENDER**

For instance, if you receive an email supposedly from your bank, it is essential to verify its authenticity, especially if you have an account with that bank. Before clicking any links, check the email address it was sent from. For example, if the email claims to be from your bank but the sender's address is something like "**test@castellodirivara.it**," which seems unrelated to your bank's official email domain, it is a red flag. In such cases, it is crucial not to click on any provided links and to remain cautious. The next step is deleting the e-mail or reporting the attack.



2. SPELLING and GRAMMAR:

check for correct spelling and grammar. Wrong spelling and grammar are frequent characteristics of phishing attacks. Phishing e-mails are usually translated into different languages by automated software, which makes certain frequent mistakes. However, as translation software keeps improving, spelling and grammar in phishing e-mails has improved, and the common spelling and grammar mistakes are disappearing. It is hard to distinguish from the original.

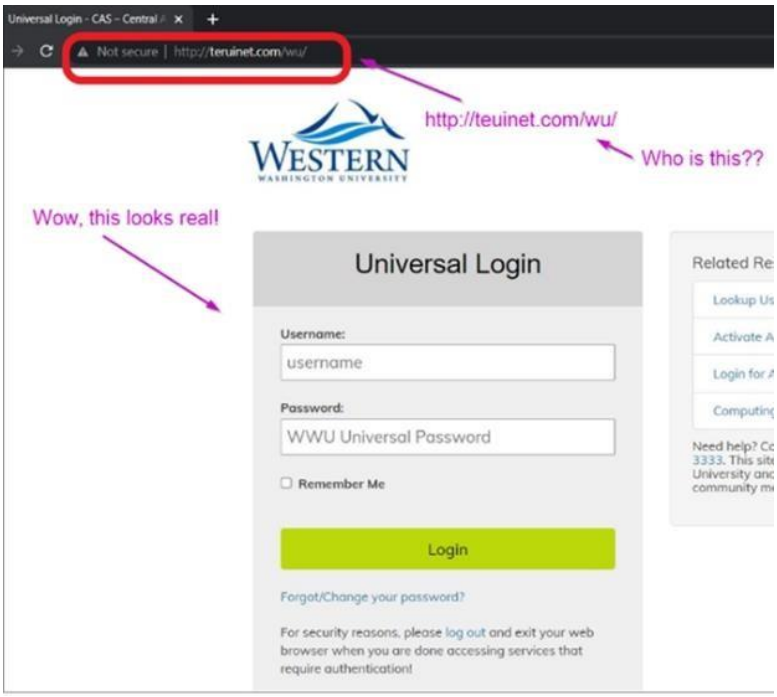
3. SUSPICIOUS LINKS.

Phishing e-mails often contain hypertext links. A hypertext link is a clickable text or picture that directs you to a different website when clicked. Usually, you can click on the link directly from the e-mail. However, it is important to be cautious before clicking on any link, even if it is tempting. To verify the link's destination, hover your mouse over the link. This action will display the URL to which the link leads, allowing you to confirm its legitimacy before proceeding. If it looks suspicious, do not click on the link, instead, delete the e-mail and or report it.

4. **THREAT** or **PRESSURE**

These are further characteristics of phishing e-mails. The attackers are trying to influence our emotions, by threatening or scaring us. They want us to act under pressure and click on a link or fill in a form with your login details. The most often pressuring factor used by attackers is **TIME**. For example: "if you do not do this now, you will lose access to all the systems you use." Or: "your account will expire within 24 hours."

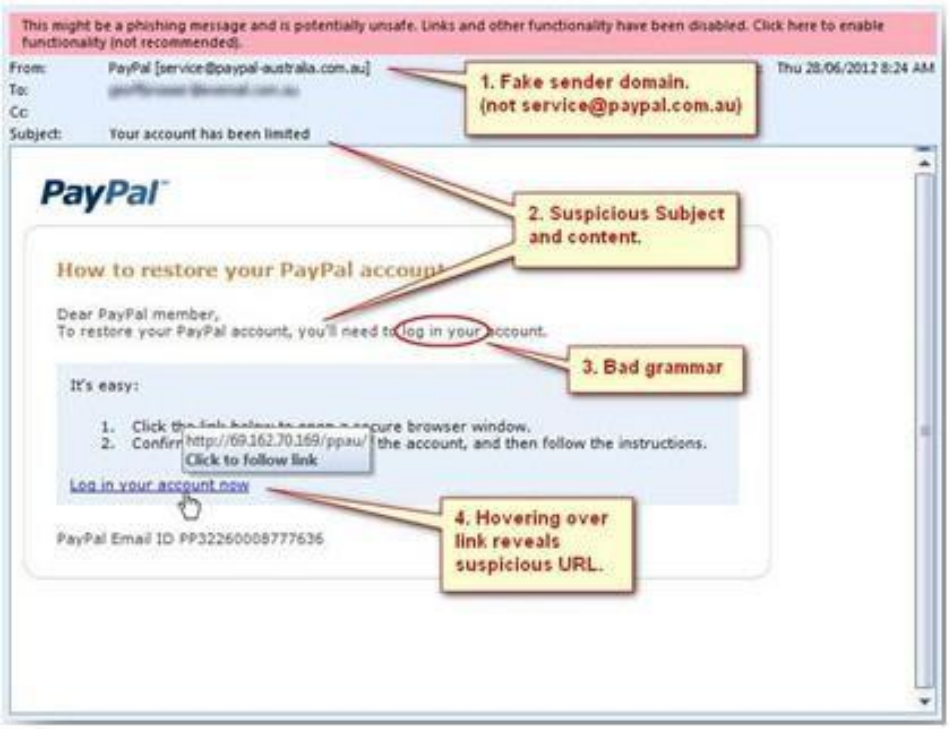
Sometimes phishing e-mails try to deceive us by making the e-mail we receive visually very similar to an official e-mail from any institution (Like police department or some serious institutions), but instead of a signature it only contains a screenshot, so it is not possible to copy an address or a phone number.



Some phishing attacks are incredibly sophisticated, making it challenging to distinguish them from genuine communications. Even experienced users can be deceived. Attackers often manipulate domain names subtly, changing just one letter, which may go unnoticed, leading us to trust the sender and click on malicious links. It is important to remember that reputable institutions will never ask for your login credentials via email.

Attackers may employ advanced techniques, such as using different character sets in web addresses. For example, they might replace a letter like "a" in "bank.com" with a similar-looking character from a different character set, like a Cyrillic "A". Although these characters appear identical in the browser's address bar, they lead to entirely different websites. This makes it challenging to recognize phishing emails or fraudulent websites.

Always remember: legitimate organizations will never request your login or credit card details via email. Stay vigilant and never provide sensitive information in response to unsolicited emails.



11. CHAPTER 4: WE DIVE INTO PHISHING WEBSITES.

In the previous topic we used the term **"phishing e-mail"** for an e-mail that has the goal to get to a website where we would fill in sensitive data. Now, we will look deeper into a phishing website.

At first glance the website looks the same as the one we regularly use, such as an online shop website, or website of our bank. It may look trustworthy, as it contains the logo, and nothing suggests it is not real.

Consequently, we trustingly log in and, by doing that, we provide the attacker with our login details, which enable them to access all systems with the log in information. The attacker will then be able to send out e-mails in our name. Not just advertisements, but even, let's say, porn.

1. **“ADDRESS BAR**” - when visiting a website, which asks us to fill in our login details, it is important to check the address bar. Is this the address that I am familiar with? Is there anything in the address that seems out of place or different? Are there symbols that should not be there?

2. “**TYPOSQUATTING”** is a common practice for attackers to replace symbols or characters with similar looking ones. For example, "m" can be replaced by "n", a small "i" with capital "I" and so on. This method is called typosquatting.

3. **“LOCK ICON”** and **“HTTPS”** are further issues we need to pay attention to.

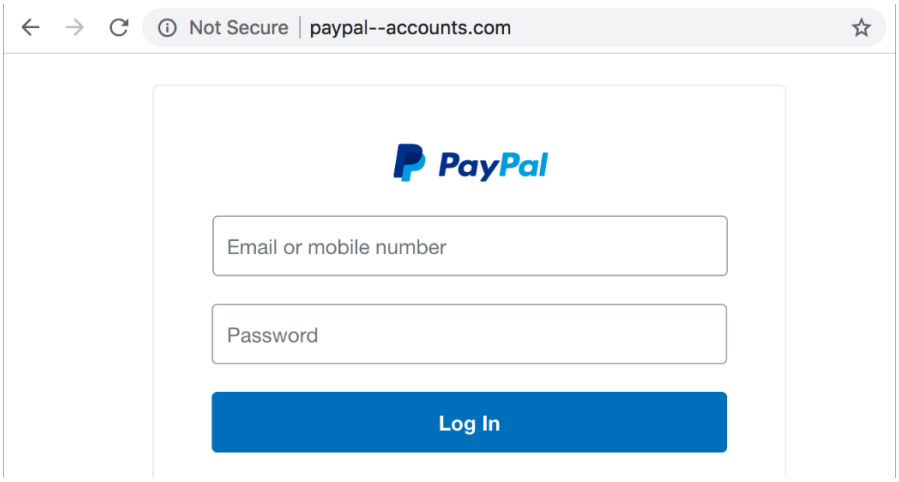
   A certified and secure site should show a lock icon at the beginning of the address row and the address should start with "https", where the "s" signals the site is secured and all data provided is coded using encryption for secure communication over a computer network.

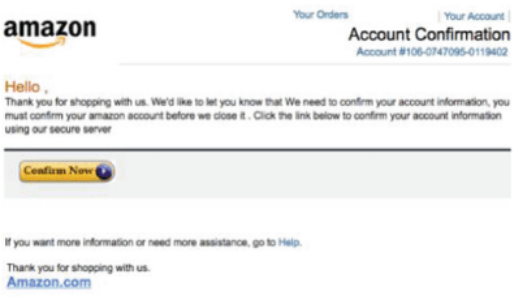
However, this does not always mean the site is safe. It is not that complicated to receive a secure certificate. Another issue to pay attention to is whether it is possible to highlight a text at places where it should work, for instance contact information. This could be, for example, contact information such as an address or a phone number.

It is easy for attackers to obtain a company logo and to make a print screen of the real website. In a few clicks, the phishing site is born. However, they don't want to invest enough time to re-type or copy the text, so text parts of sites are often replaced by pictures.

4. **"FAKE INTERNET SITES"** – how do we recognize a fake e-shop?

The content might appear visually similar or identical to the legitimate website, offering products at **suspiciously low prices.** There might be indicators of a large sale, and crucial information such as the seller's details, business name, or address may be missing. Additionally, the website might be missing general terms of use and conditions, provide only an anonymous contact form, and enable payment solely through bank transfer. Here are some examples of fake websites. Would you notice any of this?





12. CHAPTER 5: HOW TO CREATE A SAFE PASSWORD.

The topic of **PASSWORDS** is very important, as handing over our password is very much like handing over keys to our house. How can attackers obtain our passwords?

Most often, they acquire them from purchased or stolen password databases. They may also guess our password by studying our behavior on social media. What we publish and share might indicate our way of thinking and what passwords we might use. For instance, if we frequently share content related to a particular celebrity, our password might be connected to that person.

Celebrity names were the most common passwords in the past years. Hundreds of thousands of credentials included passwords connected to celebrities Taylor Swift, Bad Bunny, Jennifer Lopez, Ben Afleck, and Elton Musk. Swift's 10th album "Midnights" resulted in passwords such as taylor, taylor swift, swiftie, and midnights being used 186,000 times.

There is special software available to hackers for guessing a password. This picture below shows how long it takes for software to guess a password depending on the length and symbols used. (https://stlcom.com/blog/2021/07/how-long-would-it-take-someone-to-crack-your-password/)

NUMBER OF CHARACTERS	NUMBERS ONLY	UPPER OR LOWERCASE LETTERS	UPPER OR LOWERCASE LETTERS MIXED	NUMBERS, UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS, SYMBOLS
3	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
4	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
5	INSTANTLY	INSTANTLY	INSTANTLY	3 SECS	10 SECS
6	INSTANTLY	INSTANTLY	8 SECS	3 MINS	13 MINS
7	INSTANTLY	INSTANDLY	5 MINS	3 HOURS	17 HOURS
8	INSTANTLY	13 MINS	3 HOURS	10 DAYS	57 DAYS
9	4 SECS	6 HOURS	4 DAYS	1 YEAR	12 YEARS
10	40 SECS	6 DAYS	169 DAYS	106 YEARS	928 YEARS
11	6 MINS	169 DAYS	16 YEARS	6K YEARS	71K YEARS
12	1 HOUR	12 YEARS	600 YEARS	108K YEARS	5M YEARS
13	11 HOURS	314 YEARS	21K YEARS	25M YEARS	423M YEARS
14	4 DAYS	8K YEARS	778K YEARS	1BN YEARS	5BN YEARS
15	46 DAYS	212K YEARS	28M YEARS	97BN YEARS	2TN YEARS
16	1 YEAR	512M YEARS	1BN YEARS	6TN YEARS	193TN YEARS
17	12 YEARS	143M YEARS	36BN YEARS	374TN YEARS	14QD YEARS
18	126 YEARS	3BN YEARS	1TN YEARS	23QD YEARS	1QT YEARS

Figure 1 Source: https://stlcom.com/blog/2021/07/how-long-would-it-take-someone-to-crack-your-password/

"Keylogger" is another method attackers use to obtain our passwords. This involves software that records everything typed on a keyboard. While physical keyloggers are more common in companies, keylogger software can infiltrate various devices, often through spyware.

Just out of curiosity: it is not uncommon for someone to record another person typing their password, even using a drone circling the building. From our experience, it is also not unusual for people to share their passwords over the phone or at home. Sometimes, we might even see passwords written on papers or post-it notes stuck to walls, monitors, or directly on keyboards.

There are strong passwords and what we call "bad passwords". Simple passwords fall into this category. It is hard to believe that the number sequence "123456" has been the most used password on the Internet for the past 3 years! It is crucial to handle our passwords with care. We should not share them with anyone, whether it is by email or over the phone. One of the basic rules about passwords is to avoid using the same one for different systems. For instance, it is not wise to use the same password for social networks as you do for your bank or email account.

Why? Because if someone gets hold of one of our passwords, they may try to use it across various systems (not necessarily a person, but automated software). And what could happen? Once we suspect that our

password has been compromised, it is crucial to change it immediately. We must remember that no legitimate entity will ever ask us to provide our password via email or phone – whether it is our bank, phone service provider, or internet provider. **If someone asks you to verify your password, you should know it's a scam!**

A helpful tool for remembering passwords is to use "**password manager**" software, which securely stores all your passwords for you. This is safer than writing them down. Additionally, implementing **Multifactor Authentication** (MA) adds an extra layer of security. When logging in, the server requests a secondary form of authentication, such as a text message on your phone, on-screen numbers, a phone call, or an email to another address.

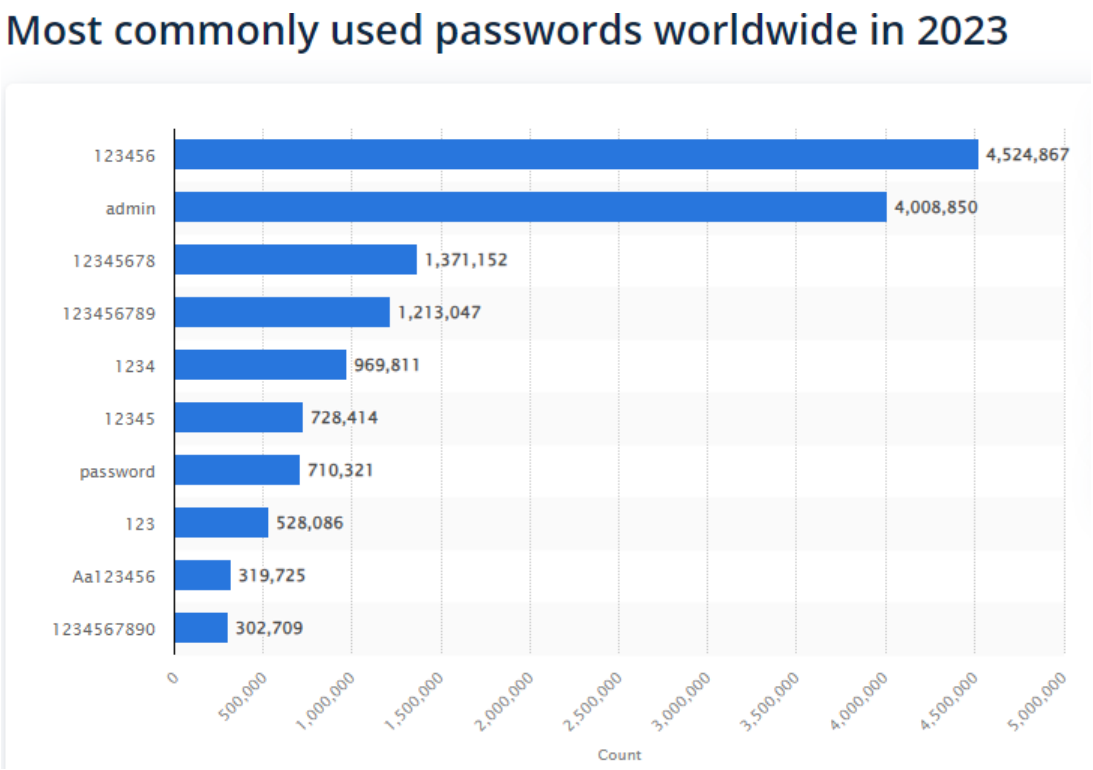


Figure 2 Source: https://www.statista.com/statistics/1454162/most-used-passwords-worldwide/

12.1. How can I create a strong password?

There are some general rules:

- a password should contain small letters, capital letters, numbers, and special characters,
- a password should be connected to you only in a way that is not easy to guess,
- a password should not contain: your name or a name of your loved one (in any form),
- a password should not contain your birth date or a birth date of your loved one (in any form),
- a password should not contain your login to the service or a part of it,
- a password should not contain your phone number or a part of it,
- a password should not contain your address, or any other personal information even backwards or forward,
- a password should not contain names of celebrities, name of movie heroes, favorite characters from games or shows, or names of your pets, any easily remembered words, even if you think nobody could guess those,
- do not write down your password on a paper or into a not protected document in computer.

The simplest way to create a strong password is by using a sentence. This can be a verse from your favorite song, a passage from a book, a quote, or a poem. Choose a sentence that you can easily recall.

For example, let's take the sentence: "**I come from Banska Stiavnica and I like to visit the Old castle**." Now, take the first letters of each word, respecting capitalization, to form a base password: "**IcfBSaIltvtOc**."

To enhance security, you can mix lowercase and uppercase letters, or replace some letters with similar-looking symbols. For instance, replacing "a" with "@" and "O" with "0" gives us: "**Icf8S@Iltvt0c**." This password provides sufficient security.

However, it is important to use different passwords for different accounts. You can modify the base password for other accounts by adding more letters and symbols. For example, for frequently used services like Facebook, Instagram, or Twitter, you could create modifications like these:

- for Facebook - "Icf8S@Iltvt0c:wWw.F8.com",
- for Instagram - "Icf8S@Iltvt0c:1nst@gr@M",
- for Twitter - "Icf8S@Iltvt0c=TwEEt").

If you find it challenging to create your own passwords, you can use a random password generator. However, it's important to note that generated passwords may be difficult to remember. In such cases, consider using a password manager for added convenience and security.

13. CHAPTER 6: OTHER ONLINE AND OFFLINE THREATS

- To share or not to share?
- What to share on social media
- How to set profiles on social media
- Who can ask me for my login and password?
- Who can ask me for my bankcard details?
- USB Keys, Tablets, Notebook
- Smartphone and contactless payment
- Practical usage of security settings

Sometimes, we accidentally expose our personal information through printed documents, which we may transfer between different places. Attackers often exploit this vulnerability by gaining access to sensitive information from printed documents. It is common for people to leave documents unattended in offices, or forget them in cafes, or public transportation, unaware of the risks associated with this practice. Regardless of how secure our digital networks might be, carrying sensitive information in paper form poses a significant security threat. Therefore, it is essential to exercise caution and minimize the use of printed documents whenever possible.

13.1. Portable hardware (USB keys, harrdisk)

USB keys are also susceptible to exploitation by attackers. For instance, attackers may strategically place "lost" USB keys in public areas, tempting unsuspecting individuals to plug them into their computers. Once connected, these USB keys can introduce malware or other security risks, compromising the security of the user's system.

Example: (*https://www.zdnet.com/article/criminals-push-malware-by-losing-usb-sticks-in-parking-lots/*)

Criminals push malware by 'losing' USB sticks in parking lots

Treat USB keys as potential threats. It is very important to avoid using USB keys whose origin is unknown. USB keys found or donated without proper knowledge of their source could pose significant risk.

13.2. Laptops, smartphones

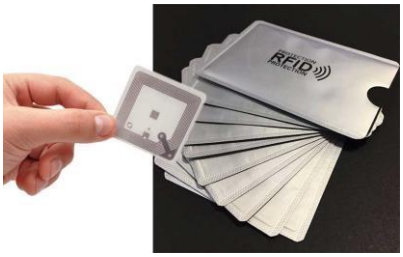
We need to be careful when carrying our devices. If our laptops are not password- protected and they are stolen or left behind in public places like trams, buses, or restaurants, this could lead to significant problems. Additionally, mobile devices such as smartphones and tablets are commonly targeted. Many people do not use passwords for their personal devices. Mobile device theft is frequent, with the motive often being not just the device value, but also the sensitive information stored on it.

13.3. Printed documents

Another concern arises with the disposal of printed and scanned documents. Do we crumple up drafts or documents with errors and simply throw them away? We need to be more mindful of how we handle documents. It is recommended to shred all documents we wish discard for added security.

13.4. Internet banking, payment cards and ATMs, payments via cellphone

- How can attackers obtain our payment card details?
- phishing → attackers trick users into providing their card details by filling out forms on dishonest websites.
- vishing → attackers deceive individuals over the phone into revealing their card information.
- How can attackers misuse my payment card?
- Portable terminal interception: attackers can intercept card details using portable terminals, sometimes concealed with packaging or entire wallets equipped with RFID protection.



- ATM skimming: be attentive at ATMs, checking for any irregularities such as additional attachments, adhesive, or raised keypads, which may indicate the presence of skimming devices https://www.mojevideo.sk/video/279ee/falosna_citacka_kariet_na_bankomate_%28vieden%29
- Surveillance: watch out for hidden cameras near ATMs or payment terminals that could capture your card's PIN or other sensitive information
- Contactless payment risks: Be cautious when making payments via cellphone or contactless methods, as attackers may exploit vulnerabilities in NFC technology

- NFC service management: Turn off NFC (Near Field Communication) services when not in use to prevent unauthorized access or data interception.

14. CONCLUSION / SUMMARY

Let's summarize the essential security protocols we need to follow for our protection.

Firstly, let's identify the situations that require our attention. In the case of an e-mail, we need to be suspicious if:

- an e-mail came from an unknown address,
- we do not know the sender,
- we are asked to provide login information,
- there is a threat that our account will be deleted if we do not log in,
- there is a strange link in the e-mail
- spelling or grammar in the e-mail might be incorrect,
- the e-mail is in English (in Slovak context)
- somebody offers to share a large amount of money,
- somebody wants us to pay for something we have not ordered; or the post office asks for money this way,
- somebody requests our credit card information, including the balance on our account as "a proof" we own the card.

If any of the above-mentioned signs appear in an e-mail, it is necessary to delete the e-mail immediately and report it. This can be done by contacting relevant entities such as your bank, post office, internet provider, original e-shop.

When viewing a website, you need to be suspicious if:

- the site you are supposed to log into doesn't have the lock icon in its address line,
- after clicking on a link, the address line starts with "http" instead of "https",
- the site and its address do not look familiar or just strange,
- there are no contacts on the site,
- the text is not clickable, or if the website is just a picture,

- unrealistically low prices.

If you encounter any of the above-mentioned situations on a website, close your browser and report the site.

Finally, the golden safety rules in the cyber space:

- update your system and applications regularly,
- use strong passwords,
- use different passwords for different services (one password for email, another one for social media, etc.),
- change your password regularly,
- report fake e-mails and websites,
- log out from your systems if you use public computers,
- pay attention to links in e-mails and do not just click on everything,
- always check the address line on websites,
- do not install unverified add-ons and extensions on your browser,
- avoid using unknown USB keys,
- use the Multifactorial authentication,

Do not send your password over e-mail, and do not share it over the phone.

15. TEACHING GUIDELINES – TRAINER'S GUIDE

Materials Needed:

- Slides for presentation
- Video projector and computer
- Computers with Internet access for activities

Recommended Time	Learning Activities/Advice for Trainer	Materials	Resource
10 min.	1. Welcome learners and introduce yourself. 2. Short activity to get to know participants Ask for an safety online experiences 3. Present the learning objectives and competencies	**Video-projector**: To display slides	Introduction – Learning Objectives
10 min.	**Introduction of the content** 1. Why is it so important 2. Theoretical background	**Video-projector**: To display slides	Introduction
15 min.	**Essential terminology in Cybersecurity to keep you on track.** 1. Explain: Malware generally 2. Explain Spam, Scam, Phishing, Vhishing 3. Explain Hoax	**Video-projector**: To display slides	Chapter 1
15 min.	**Where and why can we encounter attacks?** 1. Explain Social engineering 2. Explain other ways how to "meet" attacks 3. Explain about Emails – tell about examples	**Video-projector**: To display slides	Chapter 2
15 min	**We look at phishing emails** 1. Explain again term Phishing 2. Explain email address name @ domain extension 3. Key things to pay attention: a. Sender b. Spelling and grammar c. Suspicious links d. Threat and pressure 4. Repeat: legitimate organization will never ask for your username, password, credist card detail, personal information	**Video-projector**: To display relevant slides and multimedia content.	Chapter 3
15 min.	**We dive into phishing websites** 1. Explain interent address domain and extension	**Video-projector**: To display relevant	Chapter 4

	2. Key things to pay attention: a. Address bar b. Lock icon and https c. Typosquatting 3. Explain signs about fake eshops a. Low prices b. No contact information c. No policy	slides and examples.	
15 min	**How to create a safe password** 1. Explain the need of strong password 2. Show example how long does it take to "guess" the password 3. List the ways how attackers can "guess" your password a. Kelyoggers b. Stolen databases c. Camera/paper note 4. Give instructions how to create and remember strong password	**Video-projector**: To display relevant slides and examples.	Chapter 5
15 min	**Other online and offline threats** 1. Explain the need to be safe also a. By using USB b. By using smartphone c. By paying by card d. By paing by phone/watches/ring e. By using bankmachine 2. Inform about personal information throwed to bin	**Video-projector**: To display relevant slides and examples.	Chapter6
10 min	**Conclusion / Summary** 1. summarize the essential security protocols we need to follow for our protection. 2. Summarize golden safety rules in cyber space. 3. Open the floor for questions and answers. 4. Collect feedback from participants on the session. 5. Thank participants for their time and participation	**Video-projector**: To display relevant slides and examples.	**Conclusion/Summary**

16. SELF ASSESSMENT TOOL

MODULE NUMBER TO WHICH QUESTION REFERS	LEARNING OUTCOME (LO) TO WHICH QUESTION REFERS	QUESTION	POSSIBLE ANSWERS/ Multiple Choice
3	**Chapter 1**	What does the term "phishing" refer to in cybersecurity?	a) Scanning for viruses b) Sending fraudulent emails to obtain sensitive information c) Encrypting data to protect it d) Creating strong passwords
3	**Chapter 5**	Which of the following is considered a strong password?	a) Password123 b) 12345678 c) qwertyuiop d) 3D!hR9$@qL
3	**Chapter 1**	What is malware?	a) A type of software used for managing network traffic b) A malicious software designed to harm or exploit any programmable device c) A secure method of data encryption d) A network monitoring tool
3	**Chapter 3**	What is the best way to respond to a suspicious email?	a) Click on any links or attachments included b) Delete email (and or report it) c) Reply to the sender and ask them to verify the email d) Open the email on a public computer
3	**Chapter 2**	Which of the following is a common practice	a) Downloading software from unknown sources b) Clicking on pop-up ads c) Opening email attachments from unknown senders d) Keeping your operating system and software up to date

		to avoid malware infections?	
3	**Chapter 2**	Which of the following is a best practice for maintaining cybersecurity?	a) Using the same password for multiple accounts b) Clicking on links from unknown sources c) Regularly updating software and systems d) Disabling antivirus software
3	**Chapter 2**	What is social engineering in the context of cybersecurity?	a) Building social media profiles b) Manipulating people into divulging confidential information c) Engineering software to block social media d) Developing networks for social interaction
3	**Chapter 4**	What is a common sign that a website may be insecure?	a) The website uses HTTPS in the URL b) The website asks for multiple forms of identification c) The website URL starts with HTTP instead of HTTPS d) The website loads quickly and efficiently
3	**Chapter 5**	What is the purpose of multi-factor authentication (MFA)?	a) To allow users to bypass security measures b) To provide an additional layer of security beyond just passwords c) To store passwords securely d) To encrypt data during transmission
3	**Chapter 1**	What is ransomware?	a) A type of software used to protect data from theft b) A cyber attack where the attacker demands payment to restore access to the victim's data c) A secure method of data encryption

			d) A tool for monitoring network traffic