Project IDCAP: Improve Digital Competence in Adult People

Project Number: 2018-1-PL01-KA204-051003

How to protect my personal data?

Competence area: Protecting personal data and privacy

Introduction

The module covers key topics in the area of personal data and privacy protection. The aims of the module are:

- to discuss security principles in a digital environment and inform about potential threats – information stealing, fake emails and other;
- to present basic security principles of technology use - what rules must be followed when using the Internet on publicly available Wi-Fi networks, what is secure connection and what are unsecure email attachments?
- to explain use of safe passwords - what are the principles you should follow when creating passwords? How to safely use passwords in everyday life?

1. Introduction to security in a digital environment

1.1. Computer security

Computer security means that our computer is protected against unauthorized access, use, disclosure, interference, alteration or destruction. It is both possible and necessary to take care of your own information and computer security. Information stored on a computer and published on the Internet can affect personal well-being, health and even life. There are many threats - privacy threats, password cracking or hacking, disclosure of personal information, viruses, uploading, downloading and sending of malicious files, and malicious people who want harm.

On the Internet, we have access to social networks, online chats, forums, special chat programs (like Skype), games, and more. If the necessary security standards are not met, people with bad intentions may not only find out about your private data, but also use your identity (impersonate you).

Computer viruses have become a "classic value". Different methods are used, for example, the user receives an email with a link to a popular website such as Youtube or Facebook with an enticing movie or image. Trying to watch it infects a user's defenseless computer with just one mouse click.

E-mail attachments are particularly dangerous because they may contain viruses and other malicious software. Opening an attachment in an e-mail can automatically install malware on your computer and you won't even notice it. Such malware can affect computer files, steal passwords, or spy on you, so you should be extra careful when receiving messages with attachments from unknown recipients.

Advises for dealing with unwanted email attachments:

Advice	Explanation
Never open suspicious email attachments	Even if you receive an email from someone you know, there is no guarantee that the person actually sent it. Malware can automatically send you messages that contain viruses. When receiving an email with an attachment, it is best to ask the sender himself to make sure he has sent an email.
Update the antivirus program	If the antivirus program is not updated, it cannot protect your computer from viruses.
Leave the *firewall* on your computer turned on	A computer firewall helps prevent people or malware from accessing your computer through the Internet.
If possible, before downloading email attachments, check for viruses	Many online email providers automatically check attachments before downloading them. If your computer prompts you to check for viruses by downloading attachments, do this by yourself.

1.2. Data security – phishing

Phishing is a type of cybercrime that combines a set of social engineering and technical tools to steal sensitive, personal, and financial information from a victim.

An attacker tries to pretend to be a real organization, a trusted authority, or a known person.

Most victims of phishing are encouraged to click on emails with the following topics:

- ✓ Formal notice of data leakage
- ✓ UPS Delivery Notice 1ZBE312TYI00015011B23
- ✓ IT Reminder: Your password will expire in less than 24 hours
- ✓ You need to change your password immediately
- ✓ Please read the important notice from your administrator

How to recognize phishing:

Too good to be true. These are messages, letters, calls that tell you that you have won the lottery or that you have been randomly selected to receive a prize or service.

Quick offer. Phrases: "last chance", "only 1 hour", "today only" and so on indicates a case of phishing. Fraudsters use manipulation that creates a sense of urgency. When receiving this type of message, it is advisable to check the truthfulness of the information directly with the company or service provider.

Hidden links with other keywords. Many fraudsters use simple keywords, phrases that will take you to a fraudulent site. These links often hide a completely different site from what you think. A very good way to make sure what you are opening is to click the *RIGHT* mouse button and select the *Inspect* option. See what link is associated with that link or keyword. What is it hiding? Be careful because spelling inaccuracies often hide fake links.

Strange attachments. If you are not expecting any specific information, you should not look at email attachments. One of the methods of cybercrime is to attach a file that may contain malware to an innocent message. It is advisable to

check the sender, the purpose of the message before opening it. The only secure format that can be opened by a .txt file.

How to avoid phishing:

Advice	Explanation
Be alert	Always carefully read emails from friends and strangers
Be careful of the various communication channels	Pay attention to different types of communication - emails, ads, phone calls, and other types of communication that ask for any financial information.
Click carefully	Avoid clicking on "enable content", which allows you to enable additional linking between different documents.
Don't click on suspicious links	Avoid clicking on links in emails, messaging applications, or ads. Explore links individually, using all the resources available.
Check the reliability of the sender	Be sure the e-mail is from a trusted source.

If you are a victim of phishing:

1) Change passwords for your applications and online accounts using another phone or computer.
2) Scan your computer for viruses and check for malicious software.
3) Report data theft to the police and keep a copy of the application.
4) Report to your organization / bank or the competent authority.

1.3. Computer User Safety - Information posted on social networks

There are two ways to look at the concept of computer user security. It is possible to talk about the potential of a computer to endanger the health of its user, such as the possibility of an electrical shock, even if slight. However, the most common risk to a person is the risk of self-published information.

Often there is a lack of awareness of how many varied threats are posed by social networks.

Social networks are an important part of today's everyday life - they are used to:

- Communicate;
- Get information;
- Post and share information, etc.

There are two types of threats to social networks: **technological** and **organizational threats**.

Technological threats are related to various technologies and their use in social networking. **Organizational threats** are related to the Internet user behavior, actions and activities of the user himself / herself. An organizational threat attack is usually caused by someone else on the social network.

The most common threats on social networks are:

- ✓ various types of malware or viruses;
- ✓ phishing attacks - phishing messages or emails containing links to websites that are infected with malware;
- ✓ sending spam;
- ✓ hidden clicks that cause the user to click on something other than the user originally intended;

- ✓ various types of forged profiles - some of which are semi-automated or fully automated and some are man-made;
- ✓ inference attacks are data and information mining techniques that analyze available data to obtain additional information about the victim. In social networks, they are used to refer to and identify users' personal and sensitive information that the user has not opted to share, such as religious beliefs and sexual orientation. The attack on the social network is based on information available on the victim's and his friends' profiles.
- ✓ cybermobing - emotional humiliation using modern technology. Foreclosure, humiliation, sexting, harassment, sending nasty pictures, mocking, lying about identity to get personal information, accessing other people's information, tracking, etc.

To avoid threats, different solutions offered by social networks can be used:

- authentication mechanisms,
- blocking users,
- personal settings of users,
- "report user" option.

The solutions listed can be used successfully to protect the user from fake profiles, emotional abuse, naive and risk behaviors.

Various security solution companies - AVG, Avira, Kaspersky, Panda, McAfee, Symantec - offer Internet security solutions to social network users. Their software usually includes an anti-virus program and firewall, sometimes offering anti-spam and anti-phishing protection for Internet users. Such software helps social network users protect their personal computers from threats such as malware, hidden clicks, and phishing.

Advices for safe social networking

Type	Example
Posting	Think carefully before posting information. Everything you post is likely to become public at some point and can negatively impact your reputation and future. Be careful - others can also post about you. You may even need to ask someone to delete the information they have posted about you.
Privacy	Practically all social networks have additional privacy options - set them up whenever possible. For example, does the website really need to know your location? Check privacy options regularly and make sure they work the way you think.
Passwords	Protect your social network accounts with a long enough and unique password or passphrase. A password phrase is a password that consists of several words, making it easy to remember and write down, but much harder to guess for cyber criminals.
Fraud	Like emails, social network notifications can be used for various fraud attempts. For example, a malicious person might try to sneak in your password or credit card information. Be cautious of the links you receive.
Contacts	Do not contact strangers and suspicious persons. Creating fake profiles is very simple, and many people use it to lie about their identity. The purpose of these profiles is to deceive, gain your trust and use it against you.
Terms of use	Familiarize yourself with the social networking terms - anything you post can become a social networking property.
Job	If you want to post something about your work, first find out if it is acceptable to your management.

Personalized fraud

The new form of cybercrime - personalized fraud - is becoming increasingly popular. Cyber criminals gather or buy information about millions of people and then use that information to personalize attacks. The more you know about such attacks, the easier it will be to detect and stop them.

Email and phone scams are not new, cybercriminals have been trying to fool people for years. Examples include 'You have won the lottery' or the famous fraud of the Prince of Nigeria. But in these traditional attacks, cybercriminals do not know what they will be dealing with. They simply make a general email and send it to millions of people. Because these scams are so generic and uniform, they are usually easy to recognize. Personalized fraud is different, the cybercrime is first investigated, and an email suitable to each victim is prepared. They do this by collecting information or buying a database of people's names, passwords, phone numbers and other information. Such information is easily accessible thanks to many hacked websites. It is also often freely available on social networking sites and publicly available resources of public authorities.

The attack works like this: they find or purchase information about people's usernames and passwords obtained from hacked websites, then find your email address and information related to you in such a database and send it to you (as well as to everyone else in this database) - an email with information about you, including the password you used on the hacked website. Cyber criminals give you this password as "proof" that your computer or device has been hacked, which is obviously wrong. Cybercriminals also claim that you have been sneaking into pornographic material on the Internet after hacking. The email threatens that if you don't pay the ransom, evidence of your shameful online activities will be sent to your family and friends.

The key is, in this and almost all such cases, cybercriminals have not hacked your device. They don't even know who you are or what websites you visit. Fraudsters are simply trying to use some of the things they know about you to intimidate you and make you believe they have hacked your machine and make

you pay them. Remember, the bad ones can use the same techniques for fraudulent phone calls.

What to do? Recognize such emails and phone calls as fraudulent. It's natural to feel afraid when someone has your personal information. But remember, the sender is lying! An attack is part of an automated massive campaign, not an attempt to attack you. Nowadays, it is becoming increasingly easy for criminals to find or buy personal information, so get ready for more personalized attacks in the future.

Signs to recognize an attack:

- Always be suspicious when you receive a very urgent email, message, or phone call. When someone uses emotions such as fear or urgency, they try to make you hurry.
- Anyone requesting payment in *BitCoin* cryptocurrency, gift cards or other non-trackable payment instruments.
- If you receive a suspicious email, do a Google search to see if anyone has reported a similar attack.

Always try to use long, unique passwords for each of your online accounts. Can't remember all the passwords? Use the password manager. In addition, use 2-step authentication whenever possible.

1.4. Digital footprints

The digital footprint is information that we consciously or unknowingly leave in the virtual environment - visual, audio and written information. There is also some information that is not self-generated, but created by parents, friends, work, etc. Not having a digital footprint today can be impossible l but being too active in social networks can also have negative consequences.

The digital footprint is based on your activity on the Internet: shopping habits, media, device usage, platforms you choose.

2. Basic principles of safe technology use

2.1. Internet connection

To prevent other people from using someone else's authentication data, such as username and password, **you need to make sure you are browsing securely!**

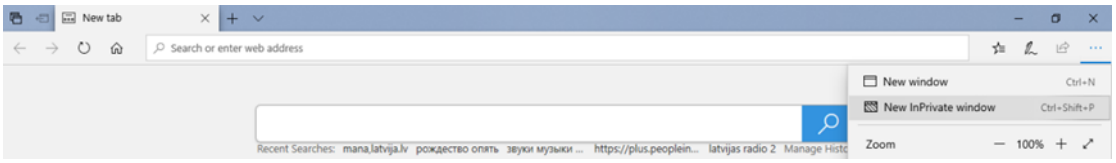
While browsing, the web browser stores information about the web pages you visit on the user's hard drive, which can be divided into three types:

a) A list of the pages you visit or the History of the pages you visit.
b) Information contained in web pages, which is usually stored in a so-called *Cachememory*. This is usually a folder called *Temporary Internet Files*.
c) Cookies - small text files. These files record, passwords, a list of pages visited, and the dates they were viewed. Browsers transfer this information back to the Internet servers. Usually, when you open a website in your browser, you are given the option to accept / refuse the use of cookies. It is recommended that you accept the use of cookies on websites that you plan to return to again.

When using a public computer, be aware that other people will be able to view the browser history of the sites the customer has visited, as well as the downloaded files. It is recommended that you clear your browser's history **Ctrl + H** and cookies to avoid any unpleasant situations. In many browsers, you can do this by pressing **Ctrl + Shift + Delete** on your keyboard.

If you don't want your browser to record your activity history and usernames and passwords, we recommend using private browsing. Private browsing may have a different name in each browser, but its essence is the same in all browsers. The images below show some examples of how to open a private browsing window.

Microsoft Edge



Google Chrome

Remember to protect your identity, passwords and security codes. This data can be used by unauthorized persons.

The following basic guidelines are recommended when using the Internet:

- Do not give your identity card, PIN codes and other access data to other persons;
- Do not post on the Internet and send copies of documents (passport, identity card, driver's license) via e-mail, communication applications or social networks;
- Do not forward passwords and other private information in e-mails or messages from communications apps (WhatsApp, Viber, Messenger, etc.) and social networks (Facebook, Twitter, etc.);
- Do not open attachments when receiving suspicious emails;
- Do not tell others too much about your life on the Internet and social networks, especially your financial situation, new things, leaving home, etc.;
- Think carefully about what photos to post on the Internet and how their publication might one day affect a person's life, such as relationships with friends, relatives, colleagues, current or future employers;
- When receiving an e-mail from a public authority or bank asking you to send your personal data to the authority, you should never do so, as the authority will never ask for the data in the form of an e-mail;

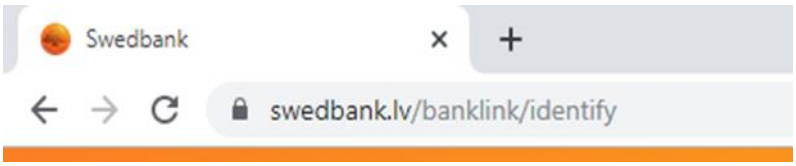
- When connecting to e-services, make sure that other people cannot see the access data you entered, and the information obtained as a result of the e-service;
- Make sure you have an antivirus program installed on your computer connected to the Internet;
- Turn off the computer overnight to not only save electricity, but also to reduce the risk of the computer being hacked and used illegally.

2.2. Secure connection - webpages with security certificates

Security means the protection of data stored on computer networks and computer systems against damage, loss or unauthorized access. Nowadays, the rapid availability of computer networks, and especially the Internet, is calling for this issue to be increasingly addressed. The main security problem in computer networks is their protection against unauthorized use, for example when making electronic payments, there is a possibility that data will be stolen and misused.

Encryption is used to secure data or message content against unauthorized use. Encryption is the process of processing data and messages by the originator or the sender of the message. In order to use such data or message content, it must be decrypted. The encryption key is used to encrypt and decrypt the data.

Websites that exchange encrypted messages are called **secure websites**.



A secure connection is usually represented by an icon 

Risks associated with online activities:

- unintentional disclosure of personal information. In order to use the services offered on websites, you often need to sign up with your personal information, such as name, date of birth, address. Before providing this information, make sure that the site is reliable and secure;
- harassment or intimidation by spreading malicious rumors or by sending threat messages;
- potential violence. By using social networks such as Facebook.com and making new contacts, you can meet a potential abuser, bully, etc. It is therefore necessary to think about what information to provide about yourself, and to critically evaluate the offers made.

In cases of fraud, harassment and emotional humiliation, inform law enforcement agencies, such as the police.

Child safety on the Internet

The following measures are recommended to protect children from negative effects when using the Internet:

- Place the computer in a room where the child's activities on the web can be monitored;
- Create child user accounts with limited computer user rights;
- Restrict browsing by turning on filters that prohibit access to websites containing child-bearing content (drugs, pornography, hate speech, weapons, etc.);
- Restrict the use of harmful games by prohibiting games on certain topics;
- Limit computer usage by setting a schedule for using your computer;
- For example: **User Accounts and Family Safety**.

2.3. Wi-fi

If your computer, tablet, or smartphone supports WiFi (wireless Internet), you can use the Internet without having to connect an additional cable to your device.

WiFi can be used both at home and outside it. If you want to use WiFi outside your home, you can often see different WiFi networks on your devices, but not all will have access because the network may be password protected.

In many places, for example, café, shops, parks you have the option of using free public WiFi. The best way to securely use public WiFi connections at public location is to find out the password and use a free connection via encrypted access. Publicly available WiFi is still one of the most commonly used ways to illegally connect to your mobile device and access your personal data.

2.4. E-mail attachments, included links and Spam messages

Spam or junk mail is called spam and junk. Spammers can easily and inexpensively send email to thousands of people at the same time. Such letters are anonymous.

How to fight against spam:

a) **Use a spam blocker.** Spam blocker can significantly reduce incoming spam. Most email providers like Google Gmail have an automatic spam blocker. If necessary, additional programs that block spam can also be used. However, in this case too, there is a likelihood of receiving them.

b) **Do not respond to spam.** If you receive an interesting spam message, you may be tempted to reply to it or click on the link to opt out of receiving further emails. By replying to the spam or by clicking on a link, you are unknowingly stating that this email address is working, and that new spam will be sent to this address in the future.

c) **Deactivate images.** The email may contain images that the spammer can track. When you open spam and allow images to be downloaded to it, you indicate that you are ready to receive new spam.

d) **Deactivate the message display pane**. When you click on a letter, it is automatically displayed in the presentation pane. Viewing spam may cause you to receive further spam.

e) **Check the spam folder regularly**. Sometimes spam blockers block not only spam, but also legitimate e-mails. Therefore, you should check your spam folder as often as possible to avoid missing an important message. Check your e-mail client's settings for which e-mails will be allowed and which will be blocked.

☑	Create multiple e-mail addresses to use them for different purposes.
☑	Do not reveal your private e-mail address on public networks.
☑	Do not create short e-mail addresses. Many spammers send e-mails to random e-mails. The shorter the address, the easier it is to discover.
☑	If you want to place an ad on the Internet, create a new e-mail address for this purpose.
☑	If you need to disclose your e-mail address, do so in a less comprehensible form, such as firstname.lastname@mail.com writing as firstname-lastname-et-mail-dot-com.
☑	Do not use your private e-mail address when signing up for public networks.
☑	Don't risk using option “unsubscribe”, as this will often only encourage to send you more spam.
☑	Change your private e-mail address if it was discovered and has a lot of spam.

2.5. Secure passwords

The passwords you choose are the most important and primary shield for protecting your accounts. Use a simple but secure way to create and store all your passwords.

Steps to simplify passwords:

1. *Password phrases*

The most important feature of passwords is that they must be long enough, the more characters there are in the password, the better. These are called password phrases, a type of secure password that uses short sentences or casual words:

- *Time for strong black coffee!*
- *missing-snail-crawl-beach*

Both passwords are secure, with over 20 characters, and both passwords are easy to remember, simple to write, but hard to crack. You will encounter web sites or situations that require the use of symbols, numbers or capital letters for the password. But remember, the key to the password is length!

2. *Password managers*

You need a unique password for each of your accounts. If you use the same password for multiple accounts, you put yourself at great risk. All a cyber-attacker needs are to hack the website you are using, steal all passwords, including yours, and then use your password to sign in to all your other accounts. It happens more often than you might imagine. It is possible to check www.haveibeenpwned.com how many websites you use have been hacked and your passwords may have been compromised. In such cases, one solution is to use a password manager. **Password Manager is a special computer program that stores all your passwords in a secure, encrypted way.** You only need to remember one password – for your password manager.

Password Manager then automatically retrieves your passwords to the appropriate sites when you need them and authenticates you. They also have other features, such as the ability to save your answers to security questions, alert you if you re-use your password, a password generator feature that will allow you to create and use secure passwords, and many more. Most password

managers also securely synchronize across a variety of devices, so you have easy and secure access to your passwords, no matter what system you use.

Write down your password manager password on paper and keep it in a safe place at home. Some password managers even allow you to print a password manager recovery tool. That way, if you forget your password manager password, you have a backup plan. Also, in an emergency, when needed, your trusted people will be able to obtain information on your behalf.

3. *Two-factor authentication*

Two-step verification (often called two-factor authentication or multi-factor authentication) provides an extra layer of security. It requires two things when you sign into your accounts, your password and a numeric code that would be generated on your smart device or sent to your phone. This process ensures that even if cyber-attackers have obtained your passwords, they cannot access your accounts. Two-factor authentication is easy to set up and you usually only need to use it once when you authorize from a new device. If you use a password manager, it is recommended to protect it with both a secure password phrase and two-factor authentication.

Simplified **2-step authentication** means that, in addition to entering something you know (a password), you also confirm it with something you have (for example, a code from a mobile phone). There is also a three-step authorization where you need to confirm access with something that is right for you - such as a fingerprint. The benefit of 2-Step Authentication is that the hacker also needs access to your mobile device to hack into your account.

3. Using passwords

3.1. Passwords: The first step in security

There are two types of passwords: secure and insecure. Most people use insecure passwords - passwords that are short, easy to remember, contain

personal information (such as name, surname, year of birth, important date, pet names, family names) or even the same password is used for multiple accounts.

Hackers often use password discovery software which checks many passwords until they find the right one. Insecure passwords can be discovered very quickly. Creating secure passwords reduces the likelihood that criminals will reveal your password and steal personal and financial information.

In order to protect your data, there are basic security principles that must be followed when using a password:

- When entering your password, be careful not to allow other people to see your fingers move on the keyboard or screen of your smartphone;
- Change your password every 3 months;
- Be careful not to save automatic account access. Always use the Exit, Logout, or End job buttons;
- Avoid using passwords on free-access Internet sites.

3.2. Principles of creating a secure password

When creating a user account on social networks, using an Internet bank or any other self-service portal, you must register with your username, password and other details.

Statement	**Explanation**
Never use personal information	Don't use names, birthdays, or family names as passwords. Personal information is often publicly available, so you can guess the password very quickly.
Use longer passwords	The password must be at least six characters long. To make your password more secure, you can use 12 or more characters to enter your password.

Statement	Explanation
Avoid writing down passwords on your notepad or phone	If you still want to write down your password, keep it in a safe place and do not show it to anyone. It is recommended that you encrypt your passwords and not write down the password itself.
Use randomly selected passwords	Random passwords are the most secure. Instead of thinking of your own passwords, you can use password generators. Random passwords are harder to remember because they are created by devices.
Don't use the same passwords for multiple accounts	If someone reveals the password for one account, the passwords for the other accounts will also be vulnerable.
Do not use words that can be found in the environment	For example, password *teacher1* will be an insecure password.
Include numbers, symbols, and lowercase letters in passwords	To create a secure password, you can replace letters with different symbols, for example, based on the word *Monday* and replacing the letters “o” and “a”, you can create the following secure password *M0nd@y!*

3.3. Case study and practical exercise

Mr. Berzins, a man in his best years, has finally decided to start using electronic services and is ready to sign up for the Road Traffic Safety Directorate (CSDD) website so he can find out about himself and his car remotely in the future.

In order to create or activate your CSDD account, the first time you log in to the website you must register with your e-mail, create your own password and enter it. After the account has been created for the first time, access to your CSDD account will continue with both the established access and your Internet Banking access.

The task of the situation is for the Mr. Berzins to come up with a password for the newly created CSDD account in his living room at his computer, so that no one can guess it.

The common scene – Mr. Berzins is sitting in living room of his country house behind an opened laptop. In the background is a sofa, on which a lazy Persian cat named Rudis is sleeping. Mrs. Berzins is sitting on the other end of the sofa and knitting a hat. Mr. Berzins has a black dog named Poga lying at his feet. Somewhere in the background a fireplace is crackling warmly over where the Berzins hunting trophy, an elk head with horns, is hanging. One wall of the living room is occupied by a bookshelf, where you can see recognizable works by different writers. On the covers of some books you can see their portraits, for example, Shakespeare, Dostoevsky, Chekhov, etc. On the other wall there is a photo of the Berzins family, where you can see their adult children and grandchildren. There's even a summer photo of Mr. Berzins and his wife posing at Niagara Falls. A little further is an ivy hanging from a shelf and a cactus grows on the windowsill.

1) Each of the significant key objects (elements) of the Berzins family house might be viewed a possible bad or **good** version of the password:

- Cat Rudis: *Rudis* / **RuD! $**
- Wife's Hobby: Knitting /**Kn*tt*ng**
- Indoor plant Cactus: Cactus / **sutcac**
- Hunting Trophy: Trophy / **Tr0fhy**
- Dog Poga: Poga / **50g** @

- Grandson12: Grandson12 / **Gr@nds0n**
- Wife Rosalie: Rosalie / **R0s@lie**
- Chekhov: Chekhov / **Ch3kh0v**
- Dostoevsky: Dostoevsky / **D0$t0j3v$ky**

Summary

This module contained three important topics related to personal data and privacy protection. Such as the basics for the security of your computer and the basic principles of data protection. To avoid phishing, learners were introduced to the ways how cybercriminals act to steal information. Considering that one of the most important problems of personal data protection nowadays is the posting and sharing of too personal information on various social networks, this module also provided safety guidelines of this topic.

In order to safely use digital devices outside the home, this module covered the topics of Internet connections and basic principles of safe Wi-Fi use. There were also explained the signs of insecure email and spam and provided tips on how to use passwords correctly and securely.

The concluding section of the module looks at examples of password creation and describes the situation - how passwords are created, what kind of passwords should be considered, and which should be avoided?

Bibliography

- *Drošība internetā.* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/drosiba/
- *E-rīki jeb ceļvedis e-pakalpojumu lietošanā*. (n.d.). Mana.latvija.lv. https://mana.latvija.lv/e-riki/
- *Esiet sveicināti Mācību e-vidē!* (n.d.). [e-learning environment]. Macibas.mana.latvija.lv. https://macibas.mana.latvija.lv/
- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- SEB. (n.d.). *SEB privātpersonām*. Seb.lv. https://www.seb.lv/private
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Valsts reģionālās attīstības aģentūra. (n.d.). *Valsts pārvaldes pakalpojumu portāls.* Latvija.lv. https://www.latvija.lv/
- *Mana Latvija.lv. Dari digitāli!* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Latvijas Drošāka interneta centrs. (n.d.). Drossinternets.lv. www.Drossinternets.lv
- Draudzīgs internets. (n.d.). *Interneta Drosības ABC*. Draudzigsinternets.lv. www.draudzigsinternets.lv