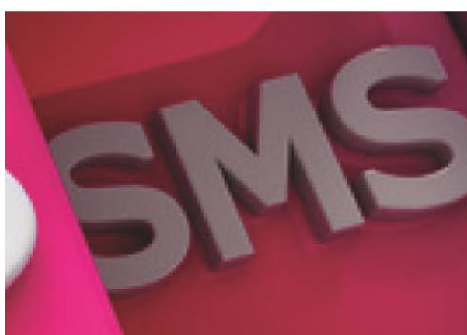




Module 4

ICT AND ONLINE SECURITY

8 classroom hours and 6 hours e-learning



Project website: www.smartwomenproject.eu

Strategic Partnerships for Vocational Education and Training

Smart Women

Project ID: 2016-1-MT01-KA202-015202

In the framework of the Smart Women project, seven partners from European countries have created an innovative European Training Model, focused on women, aiming for **encouraging entrepreneurship** and putting business ideas into practice.

The Smart Women Model combines online learning using online learning platforms and face to face training based on project collaboration, peer-learning, guidance, coaching and counselling.

Project Partners: MCA (Malta), LIKTA (Latvia), Dedalo Fundacion (Spain), EOS (Romania), Cyprus Computer Society (Cyprus) and ALL DIGITAL (Belgium).

DISCLAIMER

The European Commission support for the production of this handbook 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.

ICT AND ONLINE SECURITY

With the development of information technology, data security issues become increasingly important in digital security policy. The security issue is topical for every IT user individually, as well as for businesses, institutions and organizations.

Information security is related to computer security. Information protection can be achieved by realizing protection against computer viruses and hackers, computer damage, by granting passwords and restricting access rights, and regular duplication of important data. During the course you will acquire knowledge and skills on these issues, as well as knowledge of online safety aspects and EU regulations related to the protection of personal data.



LEARNING OBJECTIVES






Having completed this module, you will be able to:

- Understand the key concepts relating to the importance of secure information and data, physical security, privacy and data protection;
- Protect and securely dispose devices;
- Understand the principles of backing up and restoring data appropriately and safely;
- Protect a computer, device, or network from malware and unauthorised access;
- Browse the World Wide Web and communicate on the Internet securely;
- Understand security issues related to communications, including e-mail and instant messaging;
- Understand the principles and risks of cloud security;
- Understand the principles and risks of mobile security.



ANNOTATIONS

The following icons are used in the text with the meaning indicated.

Icon	Used as
	Concepts & Theory
 Resources & Links	Resources & links the student can use for further reading
	Review Exercise
	Tasks to be performed by student individually
	Tasks to be performed by students in groups

MODULE OUTLINE

The course is implemented using a blended-learning approach and includes 8 hours of classroom and 6 hours of e-learning

- **ICT and online security and safety concepts**
 - Data threats:
 - (Malicious, accidental threats to data from individuals, service providers, external organisations.
 - Threats to data from extraordinary circumstances like: fire, floods, war, earthquake.
 - Threats to data from using cloud computing like: data control, potential loss of privacy.
 - Value of information:
 - Basic characteristics of information security like: confidentiality, integrity, availability.
 - The reasons for protecting personal information like: avoiding identity theft, fraud, maintaining privacy.
 - Understand the reasons for protecting workplace information on computers and devices like: preventing theft, fraudulent use, accidental data loss, sabotage.
 - Personal Security:
 - Social engineering and its implications: unauthorised computer and device access, unauthorised information gathering, fraud.
 - The term identity theft and its implications: personal, financial, business, legal.
- **Managing digital identity**
 - Measures for preventing unauthorised access to data like: user name, password, PIN, encryption, multi-factor authentication.
 - Good password policies: adequate password length, adequate letter, number and special characters' mix, not sharing passwords, changing them regularly, different passwords for different services.
 - Common biometric security techniques used in access control like: fingerprint, eye scanning, face recognition, hand geometry.
- **Managing and protecting data and devices**
 - Principles to Secure and Back up Data:
 - Ways of ensuring physical security of computers and devices like: do not leave unattended, log equipment location and details, use cable locks, access control.
 - The importance of having a backup procedure in case of loss of data from computers and devices. The features of a backup procedure like: regularity/frequency, schedule, storage location, data compression.
 - Back up data to a location like: local drive, external drive/media, cloud service.
 - Secure Deletion and Destruction of data.
 - Secure use of cloud services:
 - Selecting the cloud service and provider.
 - Securing your data by appropriate sharing policies and authentication.

- Choosing the right settings of cloud services.
- Secure local networks and wireless networks:
 - Protection from malware.
 - Different ways that malware can be concealed on computers and devices like: Trojans, rootkits, backdoors.
 - Types of infectious malware and the way how they work like: viruses, worms.
- Anti-virus software and its limitations:
 - The importance of regularly updating software like: anti-virus, web browser, plug-in, application, operating system.
 - Principles of Quarantine and deletion of infected/suspicious files.

➤ **Secure online communications**

- Establishing secure Browser Settings and secure browsing:
 - Select appropriate settings for enabling, disabling autocomplete, auto save when completing a form.
 - Delete private data from a browser like: browsing history, download history, cached Internet files, passwords, cookies, autocomplete data.
 - Learn that certain online activity (purchasing, banking) should only be undertaken on secure web pages using a secure network connection.
 - Identify ways to confirm the authenticity of a website like: content quality, currency, valid URL, company or owner information, contact information, security certificate, validating domain owner.
- Secure e-mailing:
 - Introduction to term digital signature, purpose of encrypting, decrypting an e-mail.
 - Common characteristics of phishing like: using names of legitimate organisations, people, false web links, logos and branding, encouraging disclosure of personal information.
 - Danger of infecting a computer or device with malware by opening an e-mail attachment that contains a macro or an executable file.
- Secure social networking:
 - The importance of not disclosing confidential or personal identifiable information on social networking sites.
 - How to apply and regularly review appropriate social networking account settings like: account privacy, location.
 - Potential dangers when using social networking sites like: cyber bullying, grooming, malicious disclosure of personal content, false identities, fraudulent or malicious links, content, messages.

➤ **Secure mobile communications**

- Learn how mobile applications can extract private information from the mobile device like: contact details, location history, images.
- The possible implications of using applications from unofficial application stores like: mobile malware, unnecessary resource utilisation, access to personal data, poor quality, hidden costs.
- Learn how to set safely the application permissions.

- Emergency and precautionary measures if a device is lost like: remote disable, remote wipe, locate device.

- **Data Privacy and Protection**

- The background and principles of data protection.
- Legal acts regulating personal data collection and protection in EU.
- Best practice principles of persons' data collection:
 - Legal agreement with physical person or legislation requirements to collect data.
 - Accuracy, transparency and minimization of data.
- Entrepreneurs responsibility to store and protect data.

ICT and Online security

ICT and online security	iii
Learning Objectives	iv
Annotations	v
RESOURCES & LINKS THE STUDENT CAN USE FOR FURTHER READING.....	V
REVIEW EXERCISE	V
Module Outline.....	vi
LESSON 1 - ICT AND ONLINE SECURITY AND SAFETY CONCEPTS	10
1.1 Data threat	11
1.2 Steps to take for data protection	12
1.3 Information security	13
1.4 Data protection policy in the company	14
1.5 Characteristics of Information Security	16
1.7 Additional Resources	20
1.8 Review Exercise	21
1.9 Tasks	22
LESSON 2 - MANAGING DIGITAL IDENTITY.....	23
2.1 Measures for preventing unauthorized access to data	24
2.2 Good password policies.....	26
2.3 Multi-factor authentication and biometric security techniques	27
2.4 Additional Resources	28
2.5 Review Exercise	29
2.6 Tasks	30
LESSON 3 - MANAGING AND PROTECTING DATA AND DEVICES.....	31
3.1 Principles to Secure and Back up Data	32
3.2 Secure use of cloud services.....	34
3.3 Secure local networks and wireless networks	36
3.4 Protection from malware.....	37
LESSON 4 - SECURE ONLINE COMMUNICATIONS	40
4.1 Secure browsing	41
4.2 Secure e-mailing	44
4.3 Secure social networking.....	46
4.4 Potential dangers using social networking.....	47
LESSON 5 - SECURE MOBILE COMMUNICATIONS.....	49

5.1 mobile communications	50
5.2 Delete data from a device that you no longer use	51
5.3 How to protect oneself?	52
5.4 Mobile security applications	55
5.5 Additional Resources	58
5.6 Review Exercise	59
5.7 Tasks	60
LESSON 6 - DATA PRIVACY AND PROTECTION	61
6.1 Data Privacy and Protection	62
6.2 Principles of Good Practice in Personal Data Processing	63
6.3 Additional Resources	64
6.4 Review Exercise	65
6.5 Tasks	66
Module Completion	67

LESSON 1 - ICT AND ONLINE SECURITY AND SAFETY CONCEPTS

After completing this lesson, you should be able to:

- Understand the importance of protecting devices, information and personal data
- Understand the main security and safety risks and protection measures

1.2 STEPS TO TAKE FOR DATA PROTECTION

Concepts

When it comes to computer security, you have to look after many aspects such as risk analysis, kinds of threats, security policy, and then come protection techniques. Viruses, keylogging, worms and phishing attacks are all around your system to damage it, but there are ways through which you can assure the security of your system. The main ways of computer security include:

- **Antivirus programs**, which can scan and keeps you alert about viruses.
- **Firewall** of your system, which can be configured for enabling you to transfer selected information between your system and internet.
- **Backup** is another way of protecting your important files and documents, as this helps to restore lost files because of virus attack.

When it comes to data threats, you should be aware that data can be attacked not only by hackers, but also by extraordinary situations like fire, flood, war, earthquake, and using cloud computing.

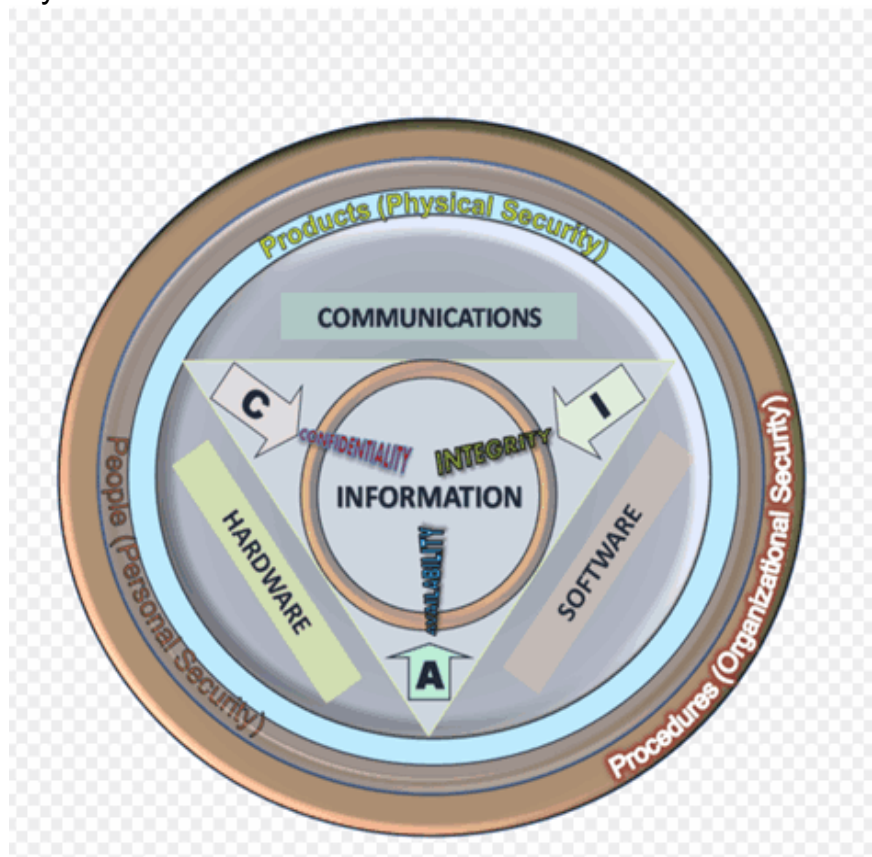
1.3 INFORMATION SECURITY

Concepts

Speaking about Safety issues related to the use of technology often the concept of Information Security is mentioned.

What is meant by that?

In the field of information technology, many technologies are used for the benefit of the people of the present era. Where there are many advantages of the information technology some disadvantages are also present that really throw a bad light on the technological devices and processes. However, the major advantage of the information technology is providing the information security to the data that is used in the transmission of the data or producing the new technical products. It is defined as the technology designed to protect the information from the different types of hackers and the from identity theft and protect your information from unauthorized use is called as **information** security. Basically, this technology used in the field of computer networking due to its importance in maintaining the security of the information that needs security and confidentiality.



1.4 DATA PROTECTION POLICY IN THE COMPANY



Concepts

In the context of security, it is definitely necessary to talk not only about private individuals' data but also about the data from institutions and companies. In order to ensure complex access to equipment and data protection, it is unlikely that separate operations will be sufficient, but a complex approach, which includes strategies, goals, division of functions and implementation of various solutions will be necessary.



Should organisations adopt data protection policies and what are the benefits these policies provide?

What do we understand with data protection policy?

Policies can take many different forms. They may be public facing statements of a company's commitment and approach to the collection and use of customer personal data or an internal policy directed at telling employees how personal data collected about them will be

handled.

Policies are also used to foster certain behaviours, limit negative actions or drive forward particular good practices so that employees, for example, can do their jobs with knowledge and confidence. A policy can therefore, be a guide to action with detailed information on the steps to achieve the objective of the policy being delivered by separate procedures.

Considering the law there are a number of reasons why we need data protection policies, with legal requirements being foremost. Data protection laws in the EU place legal responsibility upon the shoulders of the data controller who determines how and why personal data of individuals is processed. Central to these obligations are eight data protection principles, comprising enforceable standards over the way personal data is collected, managed and used.

The principles do not, however, provide a template for compliance. They typically use non-specific terms to describe processing such as "adequate", "relevant" "fair" and "appropriate" and for this reason, compliance by the controller is down to interpretation - applying the principles to specific circumstances. Although there is no explicit statement in the law that policies must be used, there is an implicit presumption that policies are needed to deliver compliance by helping an organisation and its employees to understand the nuances, consider the data and apply the law appropriately.

Avoiding bad publicity

Legal reasons for using policies are clearly very important but equally important are the practical and commercial risks of not having policies. In reality damage to brand and reputation can be more dangerous for an organisation than any risk of action or a fine.

Improving business processes

That said, it is not just about the law or avoiding bad press. There are also positive and practical commercial benefits from using data protection policies. These include enabling uniformity and consistency in decision-making, helping to build a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through greater transparency, instilling trust and confidence in individuals when they are deciding whether to share their data.

Things Business Owners Can Do To Secure Their Sites

- **Upgrade Site to HTTPS**

The first thing business owners should do is update their site. Business owners need to have their retail site switched to an HTTPS server. Besides being a better way to secure a site, people are beginning to look for HTTPS servers before they start shopping. Google intends to give an SEO boost to sites that have HTTPS and there is even a suggestion that regular sites be marked as less than secure in search results. Having an HTTPS server can make consumers feel more at ease about shopping on a site.

- **Keep Employees Informed on Proper Security Protocols for Site**

To make sure employees are not the weak link in the security chain, business owners need to have rules in place to ensure a site, and the personal data within, stays secure. In a recent report noting the after effects of the recent Sony breach, Forrester Research noted that 46 percent of security breaches of retail companies are caused by internal incidents, while 33 percent come from external attacks. The company should have rules about which employees have access to personal data from customers and there should be rules about creating proper passwords for login systems. This is more important than you realize.

- **Have a Policy in Place For Breaches**

The sad truth of the matter is that business owners need to prepare for the worst when it comes to security. According to estimates from Forrester Research, three out of five (60 percent) US companies will discover a breach of sensitive data in 2015. Some of these will be big breaches, but a lot of them will be smaller ones. Handling these smaller incidents correctly can limit the fallout from a breach. Being able to quickly correct the problem, notify customers and offer assistance when possible will help a brand mitigate any damage to a brand caused by security breaches.

1.5 CHARACTERISTICS OF INFORMATION SECURITY

Concepts

Due to the importance of information security, it has many important features that are really helpful for the protection of confidential data from leaking and also help to protect from hacking. Some important characteristics of information security are as follows:

- Integrity;
- Confidentiality;
- Authentication;
- Management of Risk.

Integrity:

Information security plays a very important role in maintaining the security in different types of drastic conditions such as the errors of integrity. As we know that information security is used to provide protection to the documentation or different types of information present on the network or in the system. So there are many viruses that can infect the computer, slow down the working and also break the integrity of the system. Therefore, information security provides valuable and easy steps to prevent the different types of errors created due to integrity.

Authentication:

Another important characteristic of information security technology is that it can provide the authentication method to protect documents or files from different types of hackers and also protect them from infection of different viruses. In the authentication method, information security provides the opportunity to the user that he or she can assign different types of special or secret words that are called as passwords to the required information that has to be protected.

Confidentiality:

Confidentiality is the process that is used to protect information on the network by avoiding unauthorized persons from seeing your information on networking technology such as internet technology. For example, different types of thieves use different methods to steal confidential information on the internet without the knowledge of the person, such as credit card numbers and steal all the money. However, information security plays a vital role in preventing information from disclosure and unauthenticated use. In addition, your data remain safe from different types of identity theft technologies used by thieves.

Management of Risk:

Information security also takes part in managing different types of risk that are harmful for information and can disclose private or important information easily. The characteristic feature of information security is that it is very helpful in removing different types of threats and increases the reliability of information present on the network, but stopping different spam to infect information.

Benefits of Information Security

As we know that information security plays a very important role in defending information from different types of disclosure. Therefore, it has several benefits that really encourage us to use information security technology. One

Although banking websites are encrypted, you should still practice privacy protection by changing your passwords frequently and by never logging in unless you are on your protected network at home.

Avoid posting vacation details

You may not be the only one excited that you are posting a status update about your upcoming trip. Unless your Facebook status updates are completely protected, you may literally be leaving your front door open to break-ins and home robberies. Never share your vacation plans on social networking websites.

Protect your employment record

Status updates are not just for talking to your friends and followers; they can also give a future employer a quick gauge as to what type of employee you might be like. Sharing personal information such as your likes and dislikes about politics, religion or your current job can shut the door on future job opportunities. Be aware of what you are posting on Facebook and Twitter, and ensure a spotless record before you get the job.

Manage your business online reputation

If you run a business online, you know that practicing business reputation management is something you must do on a daily basis. Failure to protect your company's electronic privacy can destroy your online reputation. Criminals can take your business information, create false email accounts and fake employee names, and even hack into your corporate computer system. Protect your company's digital privacy by running your intranet on a secure server.

Secure your credit card information

Credit card scams are on the rise. Although improvements to SSL technology have allowed you to feel more secure using your cards online, it is still a good idea to safeguard your credit card number and security PIN. In addition, you can protect yourself by asking the credit card company to add extra security questions to your account and alerts to your credit bureaus.

Gain admission to the school of your choice

In much the same way that your social network status updates and tweets can prevent you from gaining a new job, they can also damage any chances you or your loved ones have of gaining admission to college. Recruiters and admissions clerks search for applicants online, often judging them solely on their Facebook profile. Check out this article about how Facebook has become the judge and jury of your online reputation. Keep your personal information private.

Protect your insurance

Having proper home insurance is often a necessity for obtaining a mortgage. Like home insurance, life insurance gives you peace of mind that your family will be protected. If you post personal information on the World Wide Web about risky behaviours involving you or your home, you could be denied your insurance plan. Always protect your privacy by avoiding status updates detailing behaviours that your insurance company might deem perilous.

Defend yourself in legal proceedings

Being involved in a lawsuit is stressful, but if you are leaking personal data on the Web you could damage your ability to win your case. Never share any type of legal information or post specific details about any type of legal dealings. You may be underestimating those who search for you online.

Guard your medical information

Posting your personal information on the Web can prevent you from receiving adequate medical care. Criminals troll websites specifically looking for detailed

medical information. When they have obtained your personal data, they will use it to gain personal medical attention for themselves or to sell to others. You could possibly be denied medical attention due to unpaid debt. Always protect your electronic privacy by not posting any medical-related data, including information about specific medical conditions.

1.7 ADDITIONAL RESOURCES

You may explore the following learning resources to enrich and upgrade your knowledge and skills.



- Read: Cybersecurity; <http://ec.europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity.en.pdf>
- Read: Data protection. Better rules for small business; http://ec.europa.eu/justice/smedataprotect/index_en.htm
- Read: Company data protection policy; <https://resources.workable.com/data-protection-company-policy>
- Read: Cyber Crime VS Cyber Security: What will you choose?; <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose>
- Read: Safer Internet day; <https://www.europol.europa.eu/newsroom/news/safer-internet-day>
- Watch: Cyber Security – Top 10 Threats; <https://www.youtube.com/watch?v=dVW1FNWSaTg>

1.8 REVIEW EXERCISE



To ensure that you have mastered the concepts presented in this lesson, you may attempt the following review exercise. Read the instructions carefully before you answer.

Questions may vary in type and can include: multiple choice with three or more options, listing responses or filling blanks of one or more words or completing sentences or any other innovative question you may come up with.

1. Malware software are the following except:
 - a. Archivers;
 - b. Viruses;
 - c. Trojans;
 - d. Computer worm.

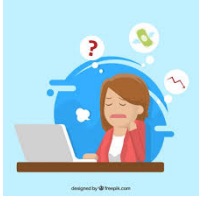
2. Cyber-attacks are the following except:
 - a. Attacks to computer systems;
 - b. Attacks to authentication;
 - c. Attacks to applications;
 - d. Attacks to water pipe systems.

3. Antivirus programmes:
 - a. Meant for creating safe passwords;
 - b. Meant for scanning computer and keeping you alert about viruses;
 - c. Meant for creating data copy;
 - d. Not meant for any previously mentioned functions.

4. The confirmation of the user in the network is:
 - a. Authentication;
 - b. Audit;
 - c. Authorization;
 - d. Confidentiality.

5. Data protection policy in the company is the following except:
 - a. Avoiding bad publicity;
 - b. Sending e-mail to all customers without their agreement;
 - c. Improving business processes;
 - d. Considering the law.

1.9 TASKS



Now is time to do some practical work and apply the knowledge you gained during the lesson. Read the instructions carefully before you attempt the tasks.

Task 1.

Imagine that you must create a new policy of data protection in your company. Please describe the three most important actions to begin with.

Discuss your plan with a group member.

LESSON 2 - MANAGING DIGITAL IDENTITY

After completing this lesson, you should be able to:

- Understand the term digital identity
- Know measures to protect your digital identity
- Understand authentication means in the computer systems
- Make and use strong passwords

2.1 MEASURES FOR PREVENTING UNAUTHORIZED ACCESS TO DATA



Concepts

- *Data* means numbers and facts.
- *Information*: data structured, summarized or in other ways processed in a certain context, which have a clear meaning.
- *Digital identity* means information which represents and identifies certain person in the computer systems.
- *Username*: an unique combination of symbols, which identifies user in particular computer resource.

Personal data online

The digital identity can be intentionally created or unintentionally left information on some entity, not necessarily correct. Using digital identities users can join computer resources, participate in the computer network and communicate with other digital identities.

The digital identity² may consist of user ID (alias, username, login name, nickname etc) and some personal data such as person's name, image, address, phone, occupation, family status, height, weight and other attributes from real life. In addition, digital entity can have properties which have particular meaning only in the digital world (such as email addresses, access rights to various digital resources, online profiles, avatars or even browsing traces).

The digital identity as well as personal data in the real world can be used for malicious intent: by using it the criminals can pretend being you, defraud sensitive information from you and your relatives, purchase goods or services on your behalf. This is the reason why this data has financial value and can be bought and sold. The theft of personal data is usually called identity theft.

In computer systems, each user is unique and can have its own unique access rights to various resources and use own settings or environment. On example, Facebook user can access and modify own content and profile but has very limited access rights on others' pages.

On the internet it's necessary to separate your personal identity from the business identity. The business identity aims to be a public one, but personal private. So you should not mix them, e .g. should use different users, profiles and contacts online.

In the personal life:

- The most important rule using the internet is not to disclose your identity: name, surname, address, e-mail address, and other individual data. Indeed, we do not disclose them to the first person met in real life.
- Do not use your real name on the internet – create a nickname.
- Be careful when communicating with other people on the internet, who ask for personal data.
- Information about work, relatives, personal website address, as well are private data, should not been disclosed to anyone.
- Do not enter your real data on every website, requiring registration. If the registration is necessary to download a document or other file from the website

² https://en.wikipedia.org/wiki/Digital_identity

only once, use a temporary e-mail address (search web for “temporary mailbox” or “trash mailbox” service).

In the business:

- Any information must be posted responsibly, on trusted and respected sites.
- Avoid anonymous participation and expressing personal moods online, use your business identity and contacts.

2.2 GOOD PASSWORD POLICIES



Concepts

Every computer or network resource user is recognised under its login name and password. This data shall be kept as a secret and shall not be disclosed to colleagues and even relatives.

Make passwords, which are difficult to guess and store them securely!

- Do not disclose your password to anybody.
- Choose a difficult password, containing small and capital letters, numbers and signs. The longer the password is, the harder it is to guess it. For example, the password P@5Sw0rd is more difficult to guess than one with ABC letters.
- Do not use passwords, created from personal names, addresses, telephone numbers and other words, that can easily be guessed.
- Remember the passwords; do not write them down on paper.
- Use different passwords on different Internet websites, because if you enter your usual password on an insecure website, it can be known to malicious people.
- Periodically change the passwords for a better safety. It is recommended to change workplace PC password every 30-40 days.

You can make strong passwords and check their strength using online tools such as <https://passwordsgenerator.net/> or <https://howsecureismypassword.net/>

Often several people share the same computer or other digital device. Even at home every desktop or notebook user shall have his individual login name and password. Then every user's environment, settings, document storage places will be separated and will be some protected from other computer users.

On shared computers it is sufficient to create different users which can have their individual desktop, document folders, software and settings. One user could be an Administrator, who has all rights and can adjust all setting of the computer, rest users can have either full either limited rights to computer resources. The less the user's rights, the less damage can be done by its software.

Be aware of the fact, that Microsoft Windows users' passwords protect personal files only from other Windows users. Using certain software, it is possible to disclose and change Windows users' passwords.

The least secure method is entering passwords using a keyboard: spyware in that computer can register and transfer all symbols entered. More secure way is to enter the passwords using password keeping software, which automatically enters them, or screen keyboard (virtual keyboard). Some of such software can store data on cloud storage and grants access for passwords from many digital devices.

2.3 MULTI-FACTOR AUTHENTICATION AND BIOMETRIC SECURITY TECHNIQUES



Concepts

The “classic” way to recognise the user is by its login and password. This unique pair usually has too many combinations to guess it by humans. But when computers being more and more fast, they often successfully guess passwords getting them from dictionaries or trying different permutations of symbols. The passwords can be relatively easily stolen or disclosed too. So usage of only passwords is becoming less reliable today.

The better solution is multi-factor authentication (MFA)³. It is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). The best security can be granted by using biometry – verifying user’s biological properties such as fingertips, face and hand geometry or retinal pattern. It is not even necessary to have sophisticated equipment to measure them, - often the smartphone camera can be enough. Most modern business notebooks have embedded fingertips readers too.

³ https://en.wikipedia.org/wiki/Multi-factor_authentication

2.4 ADDITIONAL RESOURCES

You may explore the following learning resources to enrich and upgrade your knowledge and skills.



- How to make strong passwords
Resources & Links
<https://securingtomorrow.mcafee.com/consumer/family-safety/15-tips-to-better-password-security/>

2.5 REVIEW EXERCISE

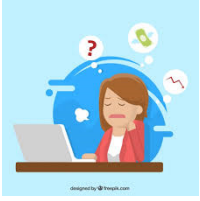


To ensure that you have mastered the concepts presented in this lesson, you may attempt the following review exercise. Read the instructions carefully before you answer.

Questions may vary in type and can include: multiple choice with three or more options, listing responses or filling blanks of one or more words or completing sentences or any other innovative question you may come up with.

1. Mark the best password:
 - a. Passw0rd
 - b. 78#\$\$%LDFww
 - c. Me1980Hero

2.6 TASKS



Now is time to do some practical work and apply the knowledge you gained during the lesson. Read the instructions carefully before you attempt the tasks.

Task 1.

Make three examples of strong passwords. Evaluate them online. Discuss results in the forum.

LESSON 3 - MANAGING AND PROTECTING DATA AND DEVICES

After completing this lesson, you should be able to:

- Understand data and devices protecting;
- Know data backup importance and implementation;
- Understand the advantages of cloud services;
- Understand network securing means;
- Know malware types and how to protect against it.

3.1 PRINCIPLES TO SECURE AND BACK UP DATA



Concepts

Ways of ensuring physical security of computers and devices

Workplace computer security starts with appropriate staff habits. In all cases, it is recommended to⁴:

- Do not leave the computer (desktop, notebook, smartphone) unlocked even for few minutes. The not authorised persons may get in, discover data or damage it. Most business operational systems can be locked in few seconds, by pressing Ctrl + Alt + Del and choosing command Lock. Locked computer continues to work but can be unlocked only by the same user or computer administrator.
- Lock the office door when you are away.
- Log off before leaving for hour(s). Shut down when leaving for long time. After logging off the most of cached in memory as well as temporary data is cleared. When system is shut down, it is impossible for hackers to get in from the network.
- Don't leave personal portable devices (notebooks, notepads, smartphones, etc.) out. They also have to be protected by strong passwords (or PINs) and no sensitive data stored inside.
- In open workspaces portable devices must be physically secured with e.g. cable lock and checked daily.

The importance of a backup

Data usually has much higher value, than the computer itself. Thus it is necessary to focus on the data safety. Data can be lost in case of malware breaches, damage of storage devices, and loss of removable media or whole notebook theft. It is recommended to regularly make backup copies of important data, existing on the computer. Especially it is recommended to perform backups before travelling, because many computers being lost during it (for example, at the airports together with baggage).

Backup copies must surely be done on other media such as on another computer storage, USB flash memory, DVD or cloud storage. If you lose a computer or if the computer's drive gets out of order, a backup copy remains in the place. If your laptop or removable media contain confidential information, then you should take care of additional safety. It is best to encrypt the information using reliable tools.

Back up data to a location

The simplest way to make backups is to start any file manager and copy necessary files to selected storage (such as network drive, USB flash memory and DVD or cloud storage).

Better is to set operational system to make backups automatically and regularly, as described on <https://support.microsoft.com/en-us/help/17143/windows-10-back-up-your-files>.

But possibly the best way is to store your important documents on cloud storage (the service of hosting files on internet servers). Here⁵ you can find extent list of such service providers and look for free online storage compatible with your device operational system. Also you can search online for Top 10 most popular cloud storage service providers.

⁴ Michael P. Small, Ralph C. Burgess. Computer Security in the Workplace – A Quick and Simple Guide

⁵ https://en.wikipedia.org/wiki/Comparison_of_online_backup_services

Most of modern cloud storage services offer special software to be installed on your device and which will synchronise any changes within particular folders with corresponding folders on cloud. Thus the documents on all your devices (computers, notebooks, tablets and smartphones) could be synchronised by your cloud storage that means newest versions of documents will replace older ones. In case you lose any device or accidentally delete a document, you can restore former content from the cloud.

Secure Deletion and Destruction of data

Recovering deleted data from the most kinds of computer storage (such as a hard drive, flash drive, memory card etc.) usually is possible because the actual data is not deleted, and only information about the data location is removed instead. By using any of dozens of available online recovery software, it is possible to find and restore most of deleted files, including ones with personal and sensitive information.

The only way to permanently erase data in the storage is to destroy it by overwriting it with random data several times using special software⁶. Even in that case exist technologies to recover data, but usually recovering costs are greater than ordinary data value.

⁶ <https://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/>

3.2 SECURE USE OF CLOUD SERVICES



Concepts

Selecting the cloud service and provider

The key considerations selecting cloud service must be security and reliability. Documents stored on the cloud should be encrypted and can't be accessed publicly (except intentional public sharing). Among the most favourite are cloud storages such as:

- Dropbox, which offers 2 GB free storage initially, but it can be increased later as bonus for promotion this service. Dropbox has file sharing, recovery and versioning features as well as simple online editing tools.
- Google Drive offers 15 GB free storage, which is already integrated for Android devices and Google online and offline services such as G Suite (previously Google documents suite). Users of other platforms can use this storage too by installing particular desktop application.
- Mega (mega.nz) provides as large as 50 GB free storage, a simple drag-and-drop interface, app for mobiles and files synchronization for desktop computers.
- OneDrive (formerly SkyDrive) is integrated into Windows 10's file explorer and no additional software is required in this case. Microsoft Photos and OneNote can also use OneDrive to sync pictures and notes across all your devices. For Android and iOS devices an app should be installed. 5 GB free storage is provided.
- For iPhone users iCloud storage is offered. Actually, free 5 GB space isn't enough to backup all files, but for most important ones.
- I Drive offers continuous syncing of your files, even those on network drives. The online interface supports sharing files by email, Facebook and Twitter. Files deleted from computer are not automatically deleted from the server. 5 GB for free.

Securing your data by appropriate sharing policies and authentication

- The first, as always using online services create your account choosing a unique, strong password. Test it using online strength evaluation tools. Enable two-step verification where applicable.
- Monitor activity on your account. In most cloud services you can track changes to files and folders, including edits, deletions, and joined users to shared resources. Usually you can turn on alarm by email when new connection from unknown machine appears.
- Do not store documents in shared folders, or select right people to share with. If the folder is shared, other users can review or even edit containing documents. Often particular folders on cloud storage are shared to all by default e.g. Public, Photos etc. Usually you can share (or then unshare) any folder with other users, invite them to join folders and email to them links to your documents. If cloud storage allows sending links for any people, check twice can't your files be seen without authorisation.

Choosing the right settings of cloud services

Here⁷ can be found short guide on managing sharing on your cloud storage account. The owner of files can limit access to shared files:

- By selecting right people,

⁷ <https://support.google.com/drive/answer/2494822>

- Choose if that people can view, comment, or edit document,
- Change sharing settings for already shared resources.

The user can transfer ownership of file to another user (and can't take it back then!).

3.3 SECURE LOCAL NETWORKS AND WIRELESS NETWORKS



Concepts

Local network can consist of any digital devices (such as PC, network printers, storage devices) connected by cables as well as by radio waves.

Home and small business networks usually are built by connecting every network device to router, which is connected to internet and switches network flow between all devices. The very important feature of routers is to maintain network security by protecting internal network from external (internet). Usually, default router settings are enough to avoid intrusions into local PCs, but you can ask specialists to turn on additional security options.

Wireless networking (Wi-Fi) could be used by hackers to get into your network even without entering your building. Although there are no absolutely secure wireless connection protection methods, it is worth to use particular measures and proper hardware settings to prevent intruders in high degree.

The simplest wireless network consists of a Wi-Fi router which is connected to internet by cable, has short antenna and can serve many wireless devices in some distance range (usually in approx. 10 meters' radius circle). The router can be maintained from any PC connected to it (USB cable connection preferable). Some advices on WiFi security you can find here⁸.

⁸ <https://heimdalsecurity.com/blog/home-wireless-network-security/>

3.4 PROTECTION FROM MALWARE



Concepts

When surfing on the internet, communicating by email or exchanging documents malicious software (or **malware**) can get into your computer. It usually follows the users' behaviour, transfers private information and sensitive data without their knowledge, and can make financial losses too.

In general, malware is any software that is developed for the purpose of doing harm to computers or via computers. Malware usually exploits security weaknesses and mistakes (so called bugs) in any applications, and exploits the willingness of a user, to take over computer protection and management.

The most common way to spread malware is email. A virus operating in the infected computer attaches its copy to the emails and sends them to all addressees from the address book. The attached file can pretend as an important document, invoice or even a picture. If the file is opened and run, the computer can be infected.

Using any removable media dramatically increases malware risks. On example, virus can spread when using a USB flash drive.

Malicious software usually operates unnoticed, but sometimes you can notice unusual operations of the computer, for example:

- The operation of programmes is slower and simple actions lasts longer than usually;
- Operating memory of the computer becomes insufficient for the programmes;
- Various ads are opened even out of the browser;
- The homepage of your browser is changed without your knowledge;
- Internet or *Windows* files browser shows a new toolbar, which is difficult to remove.

It is possible to protect yourself from risks occurring because of many internet and computer viruses, not only by using special software tools – internet firewalls, antivirus software, antispyware, email filters etc., but encouraging users to behave online safely and in smart way.

Types of infectious malware

Malicious software can be of several types.

Viruses

Computer viruses are small pieces of software and usually are able to spread to a large extent.

Computer viruses usually spread by email, other communication channels or are inside various software, and when it is started, viruses also start operating. However, it is also possible to get viruses by simply browsing the affected websites.

Viruses can destroy, corrupt, compromise data, send electronic mail, log and steal passwords entered by keyboard, format hard disks, disable particular operating system functionality. Some viruses try to turn off installed antivirus software.

Worms

Worms are programs spreading by electronic mail or communication channels. The worms copy themselves very quickly, and immediately occupy the computer working memory and spread through all over the computer network. Worms do not affect documents on the computer, but seriously disrupt the operation of a computer and networks. Worms are usually attached to emails and are run by opening the email attachments.

Trojans

This is a kind of malware hidden in other, some useful software. Trojans do not spread themselves, but they use the curiosity and trustfulness of internet users. When the useful programme is downloaded and run, the Trojan inside starts operating, which usually installs backdoor (makes the computer accessible to everyone or only to certain intruders of the internet). Then the intruders can break into the computer, collect stored data and even control the computer and use it to attack other computers. Trojans are commonly used to create **botnets**, a distributed networks of thousands of compromised computers (called zombies), which allow hackers to use anonymously the power of the many computers for distributed denial-of-service attacks and email spam.

Macro Viruses

These viruses infect documents, created by office software, for example, almost all Microsoft Office documents where the macro commands are intended for documents automation. In the current office software usually the macros are denied by default, but users can allow them to run.

Regarding the threat of macro viruses, the users must carefully open email attachments. The questionable email attachments should be never opened neither previewed in email software like as Microsoft Outlook, because any macros inside will be started in that way. Some suspicious macros can be recognised and blocked by email programs, but many not.

Malware online

Internet websites may contain malicious *Java*, *JavaScript* and *ActiveX* programs. It is sufficient to visit such infected website and the malicious software is downloaded to the computer and starts operating in it. Virus code can be hid even in pictures.

Hoaxes

False messages (hoaxes) are an attempt to trick people into believing something is real or true, and are also considered as certain viruses. The authors of which, for example send “successful” letters, inform about certain computer viruses, ask for support etc., and encourage sending such e-mails to all their friends. Such messages do not make harm to the computer, but unnecessary overload email delivery systems and may let fraudulently make profit from donations if asked. When you receive such emails, do not forward them and immediately delete them. If unclear, you can search online for subject of message.

The most famous types of hoaxes are known as the Nigerian email scams (see examples on <http://www.hoax-slayer.com/nigerian-scam-list.shtml>).

Scareware

Significant part of all malware is fake antiviruses and antispyware. User visiting compromised website gets fake alert on her/his PC/smartphone is infected. Next the user is offered to download given “antivirus software” which actually is set of malware. This social engineering trick is called **scareware**.

Recently, fake PC or smartphone acceleration and optimization programs are actively offered too.

Spyware

Various spyware (adware) programs are very similar to Trojans, which register the computer user’s activity and send these data via the internet without the user’s knowledge and agreement. The main purpose of spyware is to “customise” web search results and display specific advertisements based on customer online behaviour. Some spyware also sends spam messages to the user’s email contacts.

That spyware can even be added to a legal programme, sold under a licence. Such spyware probably occurs on your computer too – researches indicate that 4 of 5 computers contain some spyware.

Many antivirus programmes do not protect from all kinds of spyware. Special software removes spyware and adware more effectively.

Keyloggers

Keyloggers register user typing activity, record everything that user types: passwords, credit card numbers, logins, other sensitive information, and send back to the cyber criminals.

Anti-virus software and its limitations

Specific software equipment secures your computer from viruses. One kind of antivirus software (antivirus scanners) scans computer media and searches for contaminated data, and tries to remove them if detected. Other, resident antivirus applications operate during the whole usage of the computer and monitors the applications run, documents opened and saved.

It is necessary to use resident antivirus software and update it regularly, so it can recognise the latest viruses.

Although antivirus programs use some of the computer resources and sometimes respond incorrectly, they quite effectively protect against most malware. Therefore, it's not allowed to turn off antivirus protection and endanger both the computer and data as well as other users.

It remains possible that even a good antivirus application would let in new unknown viruses which could damage data stored on the computer. Therefore, it is necessary to regularly make backup copies of the most important data on other media, in order to recover the lost information later.

Once computer is compromised, it should be completely cleaned and fully restored from backups to trust it again. Often host systems are infected by complex set of malware. When only part of malware is removed, rest part activates and launches another malware version.

The importance of regularly updating software

Even the best software programme equipment contains some bugs and safety gaps. Software developers patch these gaps and propose either new and safer programme versions or only the patches for them, i.e. updates.

When the updated software occurs, it is recommended to immediately download and install it. If you do not do this, old and known safety gaps create serious risks to the safety of your computer and data.

One of the most potentially vulnerable programmes on your computer is the internet browser. Use only contemporary and safe browsers. Only a properly set modern browser will protect your computer from malicious Java, JavaScript and ActiveX programmes, occurring on the websites.

If you don't use some software for a long time, uninstall it. Any unnecessary software only increases the safety risks.

LESSON 4 - SECURE ONLINE COMMUNICATIONS

After completing this lesson, you should be able to:

- Recognise main online communication means
- Understand safe online communication principles
- Identify possible online threats
- Know privacy protection options in social media

4.1 SECURE BROWSING



Concepts

Not only benevolent people use the Internet. As in real life, there are malicious people, who illegally seek to gain profit, cheat, improperly use trust of people. Some people simply enjoy breaking into other people's computers, to do harm, spread viruses, steal, and damage data in various ways. So browsing the internet and enjoying its services we are facing lot of potential online dangers and should manage that risks properly.

Setup a browser

Every time using ITC the user must find a right balance between safety and convenience. Most current internet browsers offer lot of features making browsing online more user friendly such as remembering data entered, autofill forms and passwords, keeping browsing history, caching webpages, storing online bookmarks etc., that can reduce privacy and data security in large degree. All popular browsers have built-in security features, but failing to correctly set up your browser's security features can put you at a higher risk for malware infections and malicious attacks. While it is impossible to guarantee complete protection from cyber threats, proper settings will greatly increase the security of your web browser.

Browse the Web for your browser privacy and security guide, on example, you can find advise about key security settings on:

- [https://www.us-cert.gov/publications/securing-your-web-browser#Internet Explorer](https://www.us-cert.gov/publications/securing-your-web-browser#Internet_Explorer)
- <https://www.veracode.com/blog/2013/03/browser-security-settings-for-chrome-firefox-and-internet-explorer>
- <https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/#Browsersettings>

Delete private data

It is usual to empty your browser's cache of web pages and stored passwords as well as clear the browsing history or cookies, for example, if you use a web-based email service from a public computer. In one hand, you will free browser's storage and it will operate more effectively, and in other, you'll erase your browsing traces and leave no sensitive information. If you do not clear your private data, the next person using the same computer could get to your personal information. Most browsers have the command Clear History in their settings (search the Web for detailed instructions)

Secure network connection

Before giving any information to a website, you should make sure it is secure. Below are some quick tips that you can use to tell if a site is secure⁹.

- Look at the URL of the website. If it begins with "https" instead of "http" it means the site is secured using an SSL Certificate (the s stands for secure). SSL Certificates secure all of your data as it is passed from your browser to the website's server. To get an SSL Certificate, the company must go through a validation process. All browsers show a green address bar with a lock icon if valid SSL certificate persists.

⁹ <https://www.digicert.com/blog/buy-site-know-website-secure/>

- Look at the Domain. Cyber attackers will sometimes create websites that mimic existing websites and try to trick people into purchasing something on or logging into their phishing site. These sites often look exactly like the existing website, with addresses similar to real such as “amaz0n.com”, “amacon.com.xyz” etc.
- Look for signs that the company is real. If the company lists a physical address and phone number there is a higher chance that they are a real business. Reputable companies will list their information so you can contact them if there is a problem, their return policy as well as their shipping policy. If you can't find these policies on their site, you probably don't want to purchase from them. Reputable sites should tell you how they protect your information and whether they give your information to third parties. You should make sure a site has a privacy statement and read it before you make a purchase. Know these rules also when creating your own business website!

Safe use of services

There are several rules, how to safely use banking online. Most of these rules are suitable using any online services.

- Protect your passwords and other identification means. Remember – nobody and in no circumstances (even a bank) has a right to require you to provide these passwords on telephone, e-mail or other ways.
- Do not write your password anywhere down. Immediately change the password if you suspect that it can be disclosed.
- When you finish using the online service, logout and close the internet browser. This is necessary even when you leave the computer just for a moment. This way you will ensure that unauthorized people cannot log on to your account.
- When you connect to your banking online, always make sure, that you are on the exact webpage you want. Always enter the webpage address yourself, do not use references from your e-mail, otherwise you risk getting onto a false website.
- The internet connection should be encrypted: the website address should start by https://, and the symbol of a closed lock or a symbol of a key has to be indicated near browser address bar.
- When you connect to your banking online use only safe computers.
- In unexpected case – immediately inform your bank.

Before buying on any website, try to evaluate the authenticity of a website like: content quality, currency, valid URL, company or owner information, contact information, security certificate, validating domain owner.

When you purchase goods or services online, avoid direct entering the data of your payment card. It is recommended to use services of famous third parties. For example, *PayPal* safely transfers money in many countries.

Use separate credit cards for an account on the internet, and keep only such amounts you need only for the purchase object.

When you buy goods and services online, you have to know the following things as well:

- Before you purchase the goods you should inquire the conditions, under which the seller is obliged to accept or change inappropriate goods, or the laws of which country are applied;
- Pay attention to the fact, whether the seller declares the security of personal data transferred and whether it is obliged to comply with the requirements determined.

Every time you are asked to provide your personal data, consider if it is really necessary for purchasing goods and services. It is recommended to enter only required data and leave optional fields empty.

4.2 SECURE E-MAILING



Concepts

Email messages are easy to counterfeit and they can be taken over by unauthorized persons. Therefore, additional precautions should be taken in addition to the measures mentioned before.

Basic precaution measures

The most common way to spread malware is email. A virus operating in the infected computer attaches its copy to the emails and sends them to all addressees from the address book. The attached file can pretend as an important document, invoice or even a picture. If the file is opened and run, the computer can be infected.

When you receive a message with the attachments, evaluate whether it is worth the risk and view the attachment. Messages containing viruses have the following features:

- The subject or text of the message is not present or contains non-meaningful symbols instead;
- It is indicated about a win in the lottery, in which you did not take part, information, which you did not request, or references to activities you are not concerned;
- You are informed about problems with your bank account (think first, do you really have account in that bank?) or a failure to perform payment transfer;
- The sender of the message is not related to its content or a letter is written in a style or language, which you do not use to communicate (for example broken automatically translated text).

Even if you know the sender of the message, it absolutely does not mean, that the message is sent by sender and from her or his mail account. It is very easy to counterfeit the sender's address. If you decide to open the attachment, at first save it somewhere on your computer, and only then open it. In this case the antivirus software will do its work – it will check whether the added file is safe or not.

Never click on web links in the emails. Webpages can be infected, and weblinks in the documents can be counterfeited (e.g. under known links yourbank.net or google.com may be hidden links to malware sites). Never download software from unknown or untrusted sources. Anti-virus and anti-malware software should always be installed and constantly updated.

Recognize phishing

Phishing is a technique to gain data by insidiousness, when pretending being a different person, bank representative, etc.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.

Spam

It is impossible to completely avoid such messages; however, it is possible to decrease the flow of them, by following these simple rules:

- Use e-mail programmes with effective spam filters. Many reliable suppliers of e-mail services notify or remove spam as well, in order that you do not receive them;
- Do not publish your personal e-mail address on websites and discussion forums (and if you have to do this, try to write it in such a way, that it could not be noticed by spam robots, like “name at domain dot com”);
- Do not use unreliable suppliers of e-mail services: they can sell your e-mail addresses and other data;
- Do not provide your personal e-mail address on any unknown website, which requests you to register. You can enter temporary e-mail address instead;
- Do not reply on spam – some of them are send on the address guessed, and if you reply, you will only confirm, that spam has reached its goal;
- Do not click links in the message – if you show your attention, you will become a more important target; moreover, links can lead to infected websites or virus files.

In accordance with the European law, any advertising messages may only be sent with the consent of the recipient. When you are sending any bulk email messages, you should provide an option for receiver to opt-out from them.

4.3 SECURE SOCIAL NETWORKING



Concepts

Do not disclose confidential or personal identifiable information on social networking sites

Using social media conflicts with the important principle of using the Internet – protect your personal identity from identity theft. Users in the social networks leave a trail of personal information that can make stealing their identity a whole lot easier. Messages, photos, moods, places, friends, likes, interests and other information together with activity time left on a network give quite much data on users' personality, habits and living environment. Moreover, the participating in the social network itself encourages not to protect, but to display up more and more data to attract other users.

Here¹⁰ you can find some safe social networking rules:

- Never share your personal (social security) ID, your birth date, home address or home phone. Of course, you should protect all of your passwords, PIN numbers, bank account and credit card information.
- Don't provide personal details such as dates, places, peoples, photos what allow to identify you.
- Check out the settings, configuration and privacy sections of social network to limit visibility of the content you publish. E.g. on Facebook you can share every content to the particular friends only.
- Don't trust any user, examine its identity and behaviour before. Billions fake profiles exist on social networks.
- Check out your profile as others see it on social networking sites. Also search yourself on Google. Once published online, any information is almost impossible to remove, it is immediately duplicated by number of search and backup engines!

When using social networks for business, create and use a different profile than personal.

Appropriate social networking account settings

Social networks users tend to overshare personal life details in order to feel connected to friends, family, and co-workers. But these private details can be used maliciously by cyberthieves to access sensitive accounts, create fraudulent identities, and compromise careers. Here¹¹ you can find detailed advice how to manage privacy in most social networks.

¹⁰ <https://www.networkworld.com/article/2346606/microsoft-subnet/microsoft-subnet-12-tips-for-safe-social-networking.html>

¹¹ <https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings>

4.4 POTENTIAL DANGERS USING SOCIAL NETWORKING



Concepts

Social media present the medium for people communication as well as for spreading various internet threats. Some of them are¹²:

- **Privacy Threats.** Most of social media allow to provide any information for everyone to see by instant messaging, photos, sharing, etc. It can have privacy issues by placing too much of personal information which malicious people may take advantage of you. You should conform good practices on privacy protection to avoid them.
- **Malicious Content.** Attackers may make use social media to spread malicious content or code. Do not click on unsolicited links from stranger or sources you do not know. Nevertheless, even you are visiting pages of someone you know, always be cautious when clicking on links or photos, because links, images or other file formats may include malicious code. Do not accept to download and install applications or plugs-ins that you do not know well.
- **Social-Engineering Attacks.** Malicious people explore the trust relationships of a victim by scrutinizing the data of the victim unwittingly. They try to manipulate people, by making them perform various actions and they do not always understand that. For example, to tell about their password, to forward secret documents or simply to pay money. Just keep your personal network to people you really do know. There is no need to add as many friends as you can. Do not trust someone you have just met online any more than you would trust a stranger encountered on the street.
- **Identity Theft.** Social networking sites typically do not authenticate new members. The people you meet on a site may not be who they claim to be. Malicious people may impersonate celebrities, corporations, government officials, etc. to persuade users to visit these fake profile pages to their advantage. Check the authenticity of the account by all means to ensure you know who you are connecting with. Do not give out your personal information unless you know whom you contact is the genuine user.
- **Cyberbullying.** Cyber bullying is a situation when someone is repeatedly threatened, harassed, embarrassed or otherwise targeted by another person using messaging, email or any other type of digital technology. Block or ignore unwanted people that you do not trust. Post only information that you are comfortable with others seeing and knowing about you. Do not confront the stalker, this could only arouses more anger or emotional attacks. Do not response to cyber-bullies, as this may usually encourage more bullying messages being received.

Inappropriate information on the Internet

Whereas data on the Internet is public to all, you can often detect information, containing such content, which is limited or restricted by law.

Restricted information is information, that under the valid legislation is forbidden to be made public and (or) to be distributed (pornography, information, which contains mockery, humiliation, which promotes detestation or incites discrimination of a group of people, or a person belonging to it, because of their gender, sexual orientation, race, nationality, language, origin, social status, religion, beliefs or attitudes, etc.).

¹² <https://www.infosec.gov.hk/english/yourself/socnetwk.html>

Limited information is information, regulated to protect juveniles. This is information, which affects their physical, mental and moral development negatively (physical or psychological violence, simulation of criminal offenses, of erotic nature, which arouses fear or horror, encourages self-mutilation or suicide, etc.).

Where to apply?

It is necessary to apply on the security violations, illegal use of data, undesirable emails or harmful content of the internet to the national Computer Emergency Response Team (search Web for CERT in your country).

LESSON 5 - SECURE MOBILE COMMUNICATIONS

After completing this lesson, you should be able to:

- To protect mobile devices by simple means.
- To use the mobile applications in a safe way.
- To identify and avoid major risks related to use of mobile devices and mobile applications.

5.1 MOBILE COMMUNICATIONS



Concepts

Nowadays phones, tablets and other portable devices equipped with an Internet connection are considered to be mobile devices.



Considering what data mobile devices contain nowadays, they are comparable to personal computers. As a result, malicious people who were previously interested in accessing users' personal computers nowadays are also interested in accessing mobile devices.

What might potentially be of interest to potential villains on mobile devices? First of

all, they are a variety of sensitive data:

- Where you live, work and places you frequently visit;
- The contact details for everyone in your address book and applications, including family, friend;
- Call history, including inbound, outbound, and missed calls;
- SMS (texting), voice, and multimedia messages;
- Chat sessions within applications like secure chat, games, and social media;
- Location history based on GPS coordinates or cell tower history;
- Web browsing history, search history, cookies, and cached pages;
- Personal photos, videos, audio recordings, and emails;
- Stored passwords and access to personal accounts, such as your online bank or mail;
- Access to photos, files, or information stored in the Cloud;
- Any health-related information, including your age, heart rate, blood pressure, or diet.

5.2 DELETE DATA FROM A DEVICE THAT YOU NO LONGER USE



Concepts

As you can see, the mobile device contains a lot of information. We often forget about it when we change devices, buy new ones. The question arises what happens to the data.

It's likely that at least some of them will be needed on the new device as well, so we can use the backup feature with Samsung Cloud, Google Account synchronization, or other features.

Data from the old device **must be deleted!**



The easier way to securely wipe your device is use its “factory reset” function. This will return the device to the condition it was in when you first bought it. We can find that factory reset will provide the most secure and simplest method for removing data from your mobile device. The factory reset function varies among devices, listed below are the steps for the two most popular devices:

- **Apple iOS Devices:** Settings/General/Reset/Erase All Content and Settings;
- **Android devices:** Settings/Privacy/Factory Data Rest.

Considering a mobile device as your own personal computer, the device's protection methods should be similar to those that are used to protect your computer from attacks.

Research data suggests that the biggest threat to our mobile devices is:

- Malware;
- Phishing Attacks;
- Outdated operating systems;
- Untested Mobile Applications.

5.3 HOW TO PROTECT ONESELF?

Concepts

- **Require Strong Authentication, Use Password Controls**

Many modern mobile devices include local security options such as built-in biometrics - fingerprint scanners, facial recognition, voiceprint recognition and so forth - but even older devices will work with small, portable security tokens (or one-time passwords issued through a variety of means such as email and automated phone systems). Beyond a simple account and password, mobile devices should be used with multiple forms of authentication to make sure that possession of a mobile device doesn't automatically grant access to important information and systems.

Likewise, users should be instructed to enable and use passwords to access their mobile devices. Companies or organizations should consider whether the danger of loss and exposure means that some number of failed login attempts should cause the device to wipe its internal storage clean. (Most modern systems include an ability to remotely wipe a smartphone or tablet, but mobile device management systems can bring that capability to older devices as well.)

There are opportunities, but unfortunately mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms.

Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.

Two-factor authentication

Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped.

Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access.

- **What will help if a mobile device is stolen or lost**

Securing your smartphone against theft is not a minor issue. Regardless of this, if you accidentally leave it somewhere or it is stolen, the consequences can be very unpleasant in many respects.

It should be remembered that there are many good applications in the play store, and perhaps a couple of them are installed on your phone that can help in such cases.

Along with following [Google's security tips](#), you should look at one of the following services to make sure you can remotely lock, wipe, or seek out the location of your wayward phone. Install apps from trusted sources only

Google offers its own solution with [Android Device Manager](#), and like most of its services it works best if you stick close to Google's ecosystem. It can locate your phone on a map, make it ring, and lock it, or totally wipe it.

Google recently unveiled the ability to [type "find my phone" into Google search](#) in order to pull up a map of where your device is located.

- **Be careful with downloading the application**

Before downloading an app, research both the app and its publishers. Check other users' reviews and ratings if available.

- **Log out of sites after you have made a payment**

Never save usernames and passwords in your mobile browser or apps. Once the transaction is completed, log out of the site instead of just closing the browser.

Don't bank or shop online using public Wi-Fi connections.

- **Keep your operating system and apps updated**

Download software updates for your mobile device's operating system as soon as you are prompted.

- **Turn off Wi-Fi, location services and Bluetooth when not in use**

Cybercriminals can access your information if the connection is not secure.

Don't allow apps to use your location services unless they need to.

Ensure your Bluetooth is turned off completely and not just on invisible mode.

You should remember that transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted Wi-Fi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network, it uses communications ports to connect with other devices and the Internet. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.

The GAO report went on to state that connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information.⁹ Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

- **Avoid giving out personal information**

Never send your personal information in response to text messages or emails claiming to be from your bank or another legitimate business.

Regularly review your mobile statements to check for any suspicious charges.

- **Don't jailbreak your device**

Jailbreaking can significantly weaken its security, opening security holes that may not have been readily apparent.

Mobile devices may have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features (known as "jailbreaking" or "rooting") changes how security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.

- **Install a mobile security app**

If available, use a mobile security solution that detects and prevents malware, spyware and malicious apps, alongside other privacy and anti-theft features.

Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software.

5.4 MOBILE SECURITY APPLICATIONS



Concepts

Highlights of 360 Security - Free Antivirus, Booster, Space Cleaner



Scan installed apps, memory card content and new apps automatically. 360 Security's latest protection technologies against viruses, adware, malware, trojan etc.

Junk File Cleaner

Delete all types of junk files (system cache, image cache, video cache and advertisement cache) to free up the storage space.

Speed Booster

Boost speed to improve the performance and RAM of your phone, boost your games to make them run smoothly.

Multi-function lock screen

- Automatically check phone status when locked to provide optimization suggestions
- Handy tool can turn on the dial, camera, flashlight quickly and turn on or off WIFI, Bluetooth, etc.
- Provide high-quality wallpaper to make your lock screen more beautiful
- Manage notification to avoid missing any important info
- Support to operate music player on the lock screen
- Full charge notification alarm to avoid overcharging

CPU Cooler Master

Intelligently saves your device's power by knowing when to automatically trigger 360 Security's Battery Saver feature and make your phone stay with durable power and never overheated.

Anti-theft

An all-in-one anti-theft solution, should you lose your beloved phone. A suite of features: Erase, Locate, Alarm & Lock can assist you with retrieving the lost device and protecting personal data. You can trigger remote features via our web interface at <http://findphone.360safe.com>

Privacy

Privacy & App Lock – Prevent data on the device such as Facebook, Instagram, Whatsapp, Snapchat, photo albums and other important & private documents from falling into the wrong hands.

Intruder Selfie

Instantly snap a photo of anyone who breaking into your apps and record the date & time in App Lock for check.

Fingerprint Lock

Unlock screen quickly and easily with your fingerprint if your device has the fingerprint sensor, no fear of forgetting pattern or PIN code any more.

Real time protection

Scan installed apps & local APK files and also monitor each installation process, provide the best payment & shopping security.

Malware Scanner

With an independently proven 100% detection rate, Malware Scanner is always up to date with the latest Intel on viruses and automatically scans apps for malware as you install them. You can also scan for malware manually at any time.

Account Privacy

How safe is your email address? Now you can find out whether your account details have been leaked or not by simply validating your e-mail with Bitdefender Mobile Security. We will run a check for you and let you know if time has come to change your password.

Smart Unlock

Make your life less complicated. When you are using a trusted Wi-Fi network such as your home hub, Smart Unlock grants you direct access to your apps by disabling the PIN code.

Fingerprint Sensor Support

Unlock secured apps with the tip of your finger on devices with Fingerprint Sensor.

PIN Timeout

A someone else tries to gain access to your PIN protected apps. There will be a 30-second timeout after each five consecutive incorrect attempts.

Web Security

Whether you are using Android's default browser or Chrome, Web Security detects malicious content and keeps your browsing safe.

Snap Photo

Active defence against thieves and intruders: your phone will snap a mugshot of any person who tries to tamper with your phone in your absence.

Privacy Advisor

Find out if any of your apps peek into your private data and leak it online. Privacy Advisor also tells you when apps access the Internet without your knowledge and download unwanted data.

Wear ON - cybersecurity for smart watches

Bitdefender Mobile Security also protects any Android Wear devices connected to your smartphone (Android 4.3 and up required). With Phone Alert, your smart watch will vibrate when you step too far away from your main device. Use the Scream function to ping your phone, and it will scream for you even if you left it on silent.

5.5 ADDITIONAL RESOURCES

You may explore the following learning resources to enrich and upgrade your knowledge and skills.



- Read: Mobiles security; Resources & Links
https://en.wikipedia.org/wiki/Mobile_security Learning Resource 2
- Read: 5 elements covered by a comprehensive mobile security strategy;
<https://blogs.dxc.technology/2016/07/29/5-elements-covered-by-a-comprehensive-mobile-security-strategy/>
- Read: The 6 Best Security Apps for your Phone;
<https://www.safervpn.com/blog/best-mobile-security-apps/>
- Watch: Mobile Security & Antivirus for Android;
http://download.cnet.com/Mobile-Security-Antivirus/3000-20432_4-75332025.html

5.6 REVIEW EXERCISE



To ensure that you have mastered the concepts presented in this lesson, you may attempt the following review exercise. Read the instructions carefully before you answer.

Questions may vary in type and can include: multiple choice with three or more options, listing responses or filling blanks of one or more words or completing sentences or any other innovative question you may come up with.

1. The biggest threat to the mobile devices are:
 - a. Phishing Attacks;
 - b. Phone protection with 8 symbols long password;
 - c. Outdated operating systems;
 - d. Untested Mobile Applications.

2. The easier way to wipe your device securely, is:
 - a. Deleting every file separately;
 - b. Deleting the internet browsing history;
 - c. Switching of mobile data;
 - d. Using the function “factory reset”.

3. Which of the mentioned functions could be considered as the good practice examples for the safe use of mobile devices?
 - a. Being careful with downloading the applications;
 - b. Installing any interesting application available in the apps store;
 - c. Turning off Wi-Fi, location services and Bluetooth when not in use;
 - d. Keeping your operating system and apps updated

4. Mobile security applications are:
 - a. Google Chrome;
 - b. Web Security;
 - c. PIN Timeout;
 - d. Smart Unlock.

5.7 TASKS



Now is time to do some practical work and apply the knowledge you gained during the lesson. Read the instructions carefully before you attempt the tasks.

Task 1.

In the Internet find more information about at least 3 mentioned Mobile security applications including the customer comments. Discuss the obtained information with your group members.

LESSON 6 - DATA PRIVACY AND PROTECTION

After completing this lesson, you should be able to:

- Understand the EU regulation for personal data collection and protection;
- Understand the best practices and responsibility of entrepreneurs collecting, storing and using personal data.

6.1 DATA PRIVACY AND PROTECTION



Concepts

Reform of data protection rule in the EU

In January 2012, the European Commission proposed a comprehensive [reform of data protection rules in the EU](#).

On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the [Regulation](#) will enter into force on 24 May 2016, it shall apply from **25 May 2018**.

The [Directive](#) enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business.

The data protection reform is a key enabler of the Digital Single Market, which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Everyone has the right to the protection of personal data

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations, which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners, which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Therefore, common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU.

The EU's [Data Protection Directive](#) also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad.

6.2 PRINCIPLES OF GOOD PRACTICE IN PERSONAL DATA PROCESSING



Concepts

Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Physical persons should know that their personal data is collected, used, viewed or processed in some other way and the scope of data processing. At the basis of transparency principle is a demand that all information and communication regarding the personal data processing is easily accessible and easily understandable and clear and simple language should be used.

Personal data may be legally processed if:

- Data subject has given permission to process his data, or
- Data subject essential interests require his data processing, or
- The reason for processing is other people's legal interests, but only that far if they are not abolished with interests in the protection of the fundamental rights of the data subject.
- Legitimate processing of sensitive personal data is subject to special, strict regime.
- Honest processing means processing transparency, especially in respect to vis-à-vis data subjects.
- Personal data processing managers must inform data subjects before their data is being processed, at least about the aim of the processing and about the manager's identity and address.
- If it is not allowed to process personal data secretly and in a hidden way if it is not allowed by a concrete law.
- Data subject has the rights to have access to his data in any place where it is processed.

Processing personal data is legitimate only if it:

- is in accordance with the law; and
- tries to achieve a legitimate aim; and
- is necessary in democratic society to reach a legitimate aim.

You can find out more about the comprehensive reform of the data protection rule in the EU by watching the [video](#).

6.3 ADDITIONAL RESOURCES

You may explore the following learning resources to enrich and upgrade your knowledge and skills.



Resources & Links

- Read: Data protection; https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection_en
- Watch: General Data Protection Regulation (GDPR) requirements, deadlines and facts; <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>
- Learning Resource 2

6.4 REVIEW EXERCISE



To ensure that you have mastered the concepts presented in this lesson, you may attempt the following review exercise. Read the instructions carefully before you answer.

Questions may vary in type and can include: multiple choice with three or more options, listing responses or filling blanks of one or more words or completing sentences or any other innovative question you may come up with.

1. When did the European Commission propose a comprehensive reform of data protection rules in the EU?
 - a) 2018;
 - b) 2012;
 - c) 2000;
 - d) 2015.

2. When do EU Member States have to transpose The Directive into their national law?
 - a) by May 2018;
 - b) by May 2020;
 - c) by August 2018;
 - d) by December 2019.

3. The objective of the Data protection reform in the EU is:
 - a) to give back the control over their personal data to the citizens;
 - b) to simplify the regulatory environment for business;
 - c) to increase the availability of data to the interested parties;
 - d) to decrease the amount of available personal data.

4. Which are the principles of Good Practice in Personal Data Processing in relation to the data subject?
 - a) Lawfulness;
 - b) Fairness;
 - c) Transparency;
 - d) Publicity.

6.5 TASKS



Now is time to do some practical work and apply the knowledge you gained during the lesson. Read the instructions carefully before you attempt the tasks.

Task 1.

After looking through the study materials and watching the video about the data protection reform in the EU, describe at least 5 data protection actions which must be observed in every enterprise.

MODULE COMPLETION

Congratulations! You have reached the end of the ICT and Online Security book.

You have learned about the key skills relating to key ICT and online safety activities, including:

- Understanding the key concepts relating to the importance of secure information and data, physical security, privacy and data protection;
- Understanding the principles of protecting and securely disposing devices;
- Backing up and restoring data appropriately and safely;
- Protecting a computer, device, or network from malware and unauthorised access;
- Browsing the World Wide Web and communicate on the Internet securely;
- Understanding security issues related to communications, including e-mail and instant messaging;
- Understanding the principles and risks of cloud security;
- Understanding the principles and risks of mobile security.