Topic: Digital Security
Lesson 1: Computer Protection

Aim	Objectives
Master communication skills and competences in basic security measures, computer protection and maintenance	At the end of this lesson, students will be able to: • state the main digital threats related to password and hardware security • describe the main attributes of password security • analyse assaults related to hardware security • speak about hardware maintenance • discuss and present findings in pairs and small groups • write a summary/ based on different media

I. Lead-in

1. What should be taken into consideration while dealing with security in IT? Share your opinion with the group.

2. Work out the meaning of the words and phrases in the box. Then watch the video "Security Awareness: Passwords" [43] and discuss the questions.

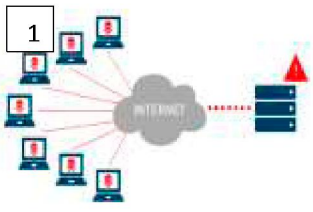
a) What is the video purpose?
b) What security assaults are illustrated in the video?
c) What password security guidelines are recommended?
d) How secure is your password? What can you do to make it stronger?

- ✓ new hires
- ✓ to sugarcoat sth
- ✓ to be up to code
- ✓ to be at liberty to discuss
- ✓ to compromise security
- ✓ dude
- ✓ to drag on
- ✓ to hide sth in plain sight
- ✓ better safe than sorry

II. Vocabulary Focus

1. Restore the correct order of the letters in the words and word combinations about security assault types. Capital letters go first. Then match the types with the pictures below.

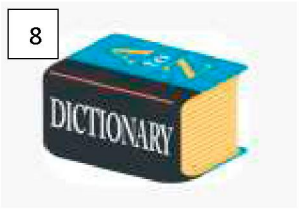
a) enalDi fo icervse _____
b) ssPwdaor hingack _____
c) tiyIndet eftht _____
d) ackBl eecrns of eadth _____
e) ctnaioryDi aacktt _____
f) eyKoerggl _____
g) mpCteour eftth _____
h) eowPr userg _____



5 

6 

7 

8 

2. Decide if the words below have a "protective" or "destructive" meaning in relation to security and distribute them between the two categories. Work with a groupmate.

Protective		Destructive
✓ Erase	✓ Password	✓ Malicious
✓ Copy	✓ Shield	✓ Theft
✓ Steal	✓ Censor	✓ Attack
✓ Pirated	✓ Defense	✓ Malware
✓ Infect	✓ Detect	✓ InfoSec
✓ Hacker	✓ Protect	✓ Countermeasures

3. Make a list of 10 key terms that are related to security. Use the word cloud on the right. Share your ideas with the group.

4. Read the abstract, name the methods hackers employ to steel passwords and underline the words and word combinations that give you a view on each method.

Password hacking is a big serious problem nowadays. When someone gains unauthorised access to your personal data and uses it illegally, it is called identity theft.

Password thieves can easily find your password if you write it down on a yellow sticky note hidden under your keyboard or in plain sight on top of your monitor. If a hacker doesn't have physical access to your work area, but your computer is connected to a network, your password can be discovered by hacker using a remote computer and software tools that systematically guess your password, intercept it, or trick you into revealing it.

The brute force attack uses password-cracking software but its range is much more extensive than the dictionary attack. Because it exhausts all possible combinations of letters to decrypt a password, a brute force attack can run for days to crack some passwords.

Sniffing is a process of monitoring and capturing all data packets passing through a given network. Sniffers are used by a network/system administrator to monitor and

troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as passwords, account information, etc.

A dictionary attack helps hackers guess your password by stepping through a dictionary containing thousands of the most commonly used passwords. Password dictionaries can be found on black hat sites and packaged with password-cracking software, such as John the Ripper. Unfortunately, dictionary attacks are often enough to break a password because many users choose passwords that are easy to remember and likely to be in the most commonly used list.

As users became better at identifying phishing messages, password thieves resorted to the use of key loggers. Short for keystroke logging, a keylogger is software that secretly records a user's keystrokes and sends the information to a hacker. A key logger is a form of malicious code called a Trojan horse, or Trojan.

Trojans are computer programs that seem to perform one function while actually doing something else. They can be embedded in email attachments, software downloads, and even files.

5. Read the passage about authentication below and answer the questions.

a) What is user authentication?
b) What are the pros of two-factor authentication?
c) How does it work?

In the context of digital security, user authentication is any technique used to verify or confirm a person's identity. Authentication techniques such as passwords, PINs, fingerprint scans, and facial recognition can prevent unauthorised access to the data on Web sites or stolen devices. Two-factor authentication increases security by verifying identity based on two components, such as a password and a verification code. It is most useful for verifying logins initiated from a device that was not used previously to log in. After a valid password is entered, a verification code is sent to a secondary device, such as a mobile phone, known to belong to the user. The verification code is then entered, in addition to the password, as the second authentication component.

6. Complete the sentences with the words and word combinations in the box.

authentication protocol; biometrics; identity theft; brute force attack; password; password manager

1. A(n)_____ is a method of breaking encryption code by trying all possible encryption keys.
2. A special set of symbols used to restrict access to a user's computer or network is referred to as _____.
3. A(n) _____ is software that keeps track of sites at which a user has registered and the password that corresponds to each site.

4. _____ is the use of physical attributes, such as a fingerprint or retinal scan, to verify a person's identity.
5. _____ is an illegal practice in which a criminal obtains enough information to masquerade as someone.
6. A(n) _____ is passwords, user IDs and biometric measures used to verify a person's identity.

7. Complete the passage with the target vocabulary of this section.

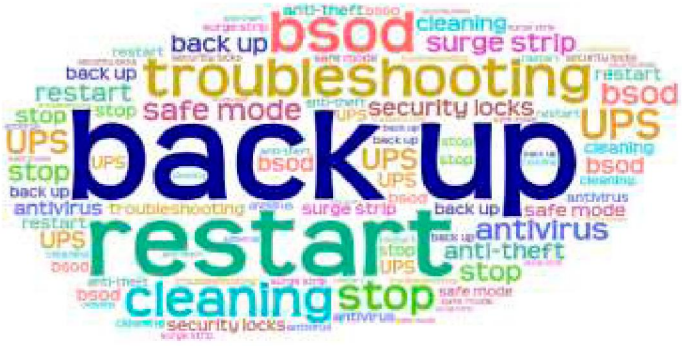
Passwords and user IDs are the most common authentication 1) _____. Password theft has become a serious security problem that has led to many cases of 2) _____ theft, when unauthorised individuals gain access to personal data. Hackers guess, discover and steal passwords using a variety of techniques. A(n) 3) _____ attack tries passwords from a list of commonly used ones. A(n) 4) _____ force attack tries every possible combination of letters and numbers. 5) _____ intercepts information sent out over computer networks. A(n) 6) _____ is software that secretly records a user's keystrokes and sends them to a hacker. To keep passwords safe, you should consider using tiered passwords or standalone password 7) _____ software that generates secure passwords and keeps track of which password corresponds to each site you access.

8. Choose one of the tasks and summarise information on it. Work in groups of three or four people. Report your ideas to the rest of the group.

1. Name and analyse the types of security assaults.
2. Describe how two-factor authentication works when you log in to a gmail account from a device you have never used before.
3. List the techniques hackers employ to get your password and explain how they work.

III. Language Box

1. What should be taken into consideration while dealing with computer protection and maintenance? Use the word cloud to get some ideas.



2. Read the abstract "Digital Security Basics" and consider the following key ideas. Work with a groupmate.

Security in IT	Physical security	Information security	Application security	Counter-measures

Digital Security Basics

Security in information technology (IT) is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organisations of all types and sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat.

Physical security is the protection of personal, hardware, software, networks and data from physical actions, intrusions, and other events that could damage an organisation. This includes natural disasters, fire, theft and terrorism, among others. Physical security for enterprises often includes employee access control to the office buildings as well as specific locations, such as data centres. An example of a common physical security threat is an attacker gaining entry to an organisation and using a USB storage device to either copy and remove sensitive data or physically deliver malware directly to systems. Threats to physical security may require less tech-savvy on the part of the attacker, but physical security is just as important as information security.

Information security, also known as infosec, encompasses a broad set of strategies for managing the process, tools and policies that aim to prevent, detect and respond to assaults to both digital and non-digital information assets. Infosec includes several specialised categories, including application security – the protection of applications from threats that seek to manipulate application and access, steal, modify or delete data. These protections use software, hardware policies and are referred to as countermeasures. Common countermeasures include application firewalls, encryption programs, patch management, and biometric authentication systems.

3. Work out the meaning of the words and phrases in the box. Then watch the video "Security Awareness: Computer Theft" [43] and discuss the questions.

a) What is the video purpose?
b) What security mistakes has David made?
c) What security tips from the list below are mentioned in the episode?

- ✓ to grab a churro
- ✓ a gal
- ✓ to wipe sth remotely
- ✓ to turn up
- ✓ to be kidding sb
- ✓ to order a tank top
- ✓ to shop frisky
- ✓ asap

- ✓ Never leave your portable computer unattended, especially when you at a coffee shop, the library or the airport.
- ✓ Use tracking and recovery software, such as CyberAngel and LoJach for Laptops which secretly sends a message as soon as a thief uses a stolen computer to log on to the Internet.
- ✓ If your computer got stolen, get IT department to wipe it remotely.
- ✓ If you have to leave your portable computer in your car, never leave it in plain view. Lock it up in the boot or cover it up.
- ✓ Use Apple's Find My iPhone system to track missing iPhones, iPods, and iPads.
- ✓ Record your portable computer's make, model, and serial number and store them away from the computer.
- ✓ If your computer got stolen, call IT to change your logins asap.
- ✓ Use STOP (Security Tracking of Office Property) plates which contain a unique ID number. Each plate ID number is registered in the international STOP database, thereby making it virtually impossible for a thief to resell a computer that has a STOP label.
- ✓ Secure your portable computers with anti-theft devices such as security locks

4. Study the guidelines about hardware protection below and share your opinion on the questions with a groupmate.

a) What is a power surge? What danger can it bring?
b) How can a computer be protected from power surges?
c) How does a surge strip work?
d) What is a UPS?

To ensure that your computer stays in good running condition, it is essential to protect it from power surges. A power surge is a sudden increase in electrical energy affecting the current that flows to electrical outlets. Power surges often occur before or after power failures.

Computer and peripheral devices require stable current and are particular sensitive to sudden bursts of electricity energy. Smaller surges can slowly damage your computer's circuit board and other electrical components.

You can protect your computer equipment from power surges by plugging it into a surge suppressor, instead of directly into a wall outlet. For added protection during thunderstorms, shut down your computer, turn off all your

A surge strip (also called a surge suppressor or surge protector) is a device that contains electrical outlets protected by circuitry that blocks surges. Some surge strips also have sockets for modem connections that prevent surges from travelling down telephone or cable lines and into your computer.

A UPS (uninterrupted power supply) is a device that not only provides surge protection, but also furnishes desktop computers and network devices with battery backup power during a power outage.

If your desktop computer is connected to a UPS when a power outage occurs, the battery backup allows you to save what you're doing and properly shut down your computer.

peripheral devices, and unplug the surge suppressor and all computer-related cables from wall outlets, including the cable for your modem	A UPS with high-performance battery might give you enough backup power to keep your computer running for several hours

5. Preventive hardware maintenance can save more than the cost of repairs. Look at the pictures and say what you should and should not do to prolong hardware lifespan.

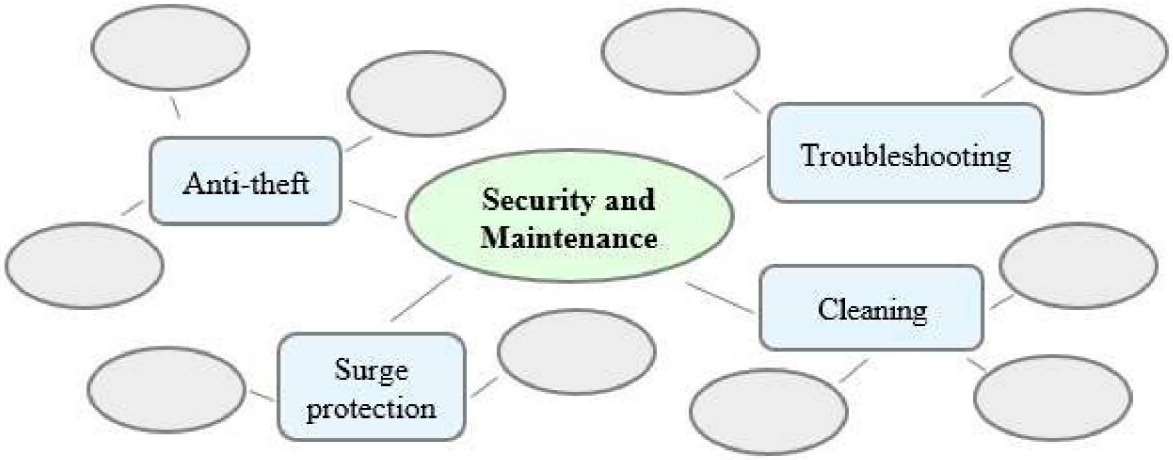
6. Say what you do with regard to a computer maintenance routine. Use the ideas in the box if necessary. Add any other recommendations to the list. Work with a groupmate.

- ✓ Back up your files regularly, particularly those that are most important to you. Test your back up procedures periodically.
- ✓ Run utilities that ensure peak performance for your hard disk drive.
- ✓ Delete your browser's history and cache files on a monthly basis in order to free up space for your temporary files. The free space results in faster downloads from the Internet.
- ✓ Apply the latest operating system, driver and security updates.
- ✓ Scan your computer for viruses and spyware once a week.
- ✓ Keep antivirus and spyware definitions updated

7. Study the steps for troubleshooting hardware problems and restore the best sequence of your actions. Work in groups of three or four people.

- ✓ Write down all error messages and any other information that goes with them.
- ✓ Make sure all components are plugged in and that there are no loose cables.
- ✓ Try to duplicate the problem by going through the same steps that led you to it.
- ✓ Look for troubleshooting tips in your user's manual, on your vendor's website.
- ✓ Run your antispyware and antivirus software.
- ✓ A simple reboot of your computer might clear up the problem.
- ✓ While in Safe Mode you can use the Control Panel's Add/Remove Programs to uninstall recently added programs or hardware that might be interfering with the operation of other components

8. Complete the concept map and get ready to speak about hardware security and maintenance. Work in groups of three of four people.



IV. Decision Bank

1. Do the quiz to find out whether you stay up to date with regard to password security.

1. Which of the following is the most commonly used (and therefore weakest) password?	a) 123456 c) Iloveyou b) Asdf d) Monkey
2. Ideally, what characters should you use in a password to make it strong?	a) letters and numbers b) mixed case (upper and lower) characters c) special symbols d) all of the above
3. How long should a strong password be?	a) 8 characters c) as long as possible b) 15 characters d) it does not matter
4. Strong passwords can be difficult to remember. What can you do to avoid forgetting them?	a) use mnemonics (acronyms or phrases that are easy for you to remember) b) develop a password strategy c) use password management software with encryption d) all of the above

2. Look at the tips below and distribute them between those that can compromise or enhance password security. Then watch the video "Tech Tips: How to Create a Strong Password" [47] to check how close your ideas were to the real ones.

Weak Password	Strong Password
✓ use eight or twelve characters	✓ indicate your phone number
✓ make common passwords	✓ change the formula/your passwords
✓ use upper and lowercase letters	✓ use your social security number
✓ include personal info	✓ provide your personal contact info
✓ use different passwords for every site	✓ do an overhaul

- ✓ provide kids' or pets' names
- ✓ mix all up
- ✓ employ a password manager app
- ✓ create a unique password formula
- ✓ use common words
- ✓ save passwords in web browsers
- ✓ combine numbers and symbols
- ✓ create something unique

3. Watch the video again and consider the key ideas. Work with a groupmate.

1. No password is a hundred percent secure.
2. The best passwords are hard to crack but easy to remember.
3. The way strong password should look like.
4. Hot tech tips that help create a strong password.

4. Using the summary of the guidelines below create a secure multi-task password. Compare it with a groupmate's one and explain what makes it unique, strong and easy to remember.

- ✓ Start with the first letters of a phrase that generates a password containing numbers and proper nouns.
- ✓ Aim for a length of 8 to 12 characters.
- ✓ Use uppercase letters somewhere other than at the beginning of the password.
- ✓ Add the site name to create a unique way to remember the site it is used for.
- ✓ Create a password using four or more words to achieve good entropy.

V. Conclusion Worksheet

Everyone who uses the Internet needs to know how to do it safely. Do an online research and gather information on the following aspects. Report your findings to the group. Work in groups of three or four people.

- ✓ The warning signs of a weak password.
- ✓ What you can do to protect yourself from such a danger.
- ✓ What you should do if you become a victim of identity theft.
- ✓ What Web site services exist to protect consumers from identity theft.

VI. Web Search

Explore the resources in the list to obtain additional information on computer protection and digital security basics. Report your findings to the group.

https://legaldictionary.net/identity-theft/

https://www.investopedia.com/best-password-managers-5080381

https://www.security.org/how-secure-is-my-password

VII. Revision Point

1. Read the abstract "How a Password Manager Works" and translate it into Belarusian or Russian. Use a dictionary if necessary.

How a Password Manager Works

The core function of a password manager (sometimes called a keychain) is to keep track of passwords so users don't have to memorise them. Some password managers also have the ability to fill in forms with stored address and credit card data. Password managers are available as operating system utilities, browser extensions, and standalone utilities. Most password managers can generate unique passwords composed of random letters, numbers, and symbols. These passwords have very good entropy and do not have to be memorised because they are stored and automatically retrieved by the password manager as needed. When you initially register for an account with a Web site or app, the password manager may display the user ID you typically use; usually it is your email address. You are then asked if you would like to enter a password or use an auto-generated password. Password managers may display a strength meter that indicates password security – a feature that is useful if you create a custom password rather than using one generated by the password manager.

2. Read the abstract related to the most common authentication protocols and complete the gaps with the words and word collocations in the box.

biometrics; ATMs; login; IDs; password; PINs; two-factor; authentication protocol; verifies; retinal pattern; legitimate

User 1) _____, passwords, and personal identification numbers 2) _____ are a fact of everyday life in the information age. They are required for activities such as using 3) _____ and debit cards, logging in to Windows, accessing wireless networks, making an iTunes purchase, instant messaging, and reading e-mail. Many Web sites encourage you to sign up for membership by choosing a user ID and 4) _____. Security experts use the term 5) _____ to refer to any method that confirms a person's identity using something the person knows, something the person possesses, or something the person is. For example, a person might know a password or PIN, possess an ATM card or a credit card. A person can also be identified by 6) _____, such as a fingerprint, facial features, or a(n) 7) _____.

Authentication protocols that use more than one means of identification are more secure than others. Computer-related security is primarily based on passwords associated with user IDs. The level of protection depends on good password selection and management on the part of users. A user ID is a series of characters – letters, numbers or special symbols – that becomes a person's unique identifier. It is also referred to as a user name, 8) _____, screen name, or online nickname. User IDs are public. Because they are not secret, they do not offer any level of security. The rules for creating a user ID are not consistent throughout all applications, so it is important to read instructions carefully before finalising your user ID.

A password is a series of characters that 9) _____ a user ID and guarantees that you are the person you claim to be. Login screens for many applications provide a "forgot my password" link. A personal question provides an alternative authentication protocol to ensure that you are not a hacker pretending to be a(n) 10) _____ user who has lost a password. Both passwords and PINs are classified as something-the-user-knows authentication methods.

In practice, PINs tend to be a short sequence of numbers that can be entered using a numeric keypad, whereas passwords tend to be longer sequences of letters, numbers and special characters that require a full qwerty keyboard for entry. PINs are commonly used with 11) _____ authentication protocols, whereas passwords are used in conjunction with single-factor authentication protocols.

3. Choose the options from the ones given in italics to make true sentences.

There are several *indistinct/clear* signs that your computer is in trouble. The most *obscure/obvious* sign is failure to power up. A loud beep at startup time can also *indicate/disguise* a problem. If your computer's screen remains blank or error messages *appear/disappear*, you might have a hardware problem. Hardware problems can also show up as unexpected restarts at *regular/random* intervals, or as a peripheral device that stops working. Windows users might *face/overlook* the blue screen of death (also called BSoD). The blue screen of death indicates that the operating system has *missed out/encountered* an error from which it cannot recover. And in this case the computer no longer *ignores/accepts* any commands.

4. Get ready to speak on the topics below and assess your performance according to the following scale.

Comprehensive	Rather confident	Limited

- Digital security basics.
- Computer protection and maintenance.
- Types of password assaults.
- Password security, authentication.

Lesson 2: Malicious Software

Aim	Objectives
Master communication skills and competences in malicious software, its types and ways to secure a computer	At the end of this lesson, students will be able to: • define malicious software and its types • explain different malware threats • state ways to protect your computer from viruses • list types of antivirus software • present and discuss findings in pairs and small groups • write a summary based on different media

I. Lead-in

1. Consider the definition of a biological virus. Does it resemble a computer virus? Give the definition of a computer virus.

Biological virus – a very small organism that infects living cells, known as the host by attaching itself to them and using them to reproduce itself; this often causes harm to the host cells

2. Work out the meaning of the words and phrases in the box. Then watch the video "Security Awareness: Removable Media" [43] and discuss the questions.

a) What is the video purpose?
b) What security assault is illustrated in the video?
c) What security guidelines can be recommended in this situation?

- ✓ a terabyte
- ✓ a little fella
- ✓ to take sb/sth over there

II. Vocabulary Focus

1. Consider the definition of "malicious" on the right and define what malicious software or malware is. Use the following collocations and phrases.

- ✓ a computer program
- ✓ enter surreptitiously
- ✓ cause disruption
- ✓ interfere unknowingly
- ✓ gain unauthorised access
- ✓ lead to private information leakage
- ✓ deprive user's access to

Malicious [məˈlɪʃ.əs] – intended to cause damage to a computer system, or to steal private information from a system

2. Match the types of malware on the left with the appropriate definitions.

1. Virus 2. Trojan horse 3. Worm 4. Bot 5. Spyware 6. Keylogger 7. Adware 8. Ransomware 9. Rootkit	a) is a type of malware that is disguised as a legitimate program; it seems to perform one action but actually does something else. b) is any software that installs itself on your computer and starts covertly monitoring your online behaviour without your knowledge or permission. It relays this data to other parties. c) is software that displays unwanted pop-up ads which can appear on your computer. d) is a program that, when executed, replicates itself by modifying other computer programs. e) is malware that prevents or limits users from accessing their system. f) is a program that masks its or other software existence. g) is a program that records every keystroke made by a computer user to gain fraudulent access to passwords. h) is a program that performs automated, repetitive, pre-defined tasks. i) can replicate itself without any human interaction, it can be transmitted via software vulnerabilities or could arrive as attachments in spam emails or instant messages

3. Read the statements about malware and replace the words in bold with the synonyms in the box. Make any changes if necessary.

payload; replicate; lurk; inadvertently; disrupt; unleash; devastating; contract; trigger

1. The worm's **haul** is a connection proxy that allows the attacker to initiate network connections through an infected computer.
2. Trolls **hide** on sites like Twitter, YouTube and Facebook.
3. I **accidentally** pressed the wrong button.
4. The hacker has **released** the virus he can't control.
5. The effect of this virus is **destructive**.
6. Because of malware, you might not even know that your computer has **agreed with** a virus.
7. These settings **copy** everyday activities but are scaled-down to be accessible to even the youngest visitors.
8. If it succeeds, the technology has the potential to **alter** seriously the current market of IoT devices.
9. It was not clear what malware **caused** such damage.

4. Read the abstract "What Is a Virus?" and choose the options from the ones given in italics to make true statements.

What Is a Virus?

A computer virus is a set of program instructions that *separates/attaches* itself to a file, reproduces itself, and *joins/spreads* to other files. A common misconception is that viruses spread themselves from one computer to another. They don't. Viruses can *replicate/originate* themselves only on the host computer.

A key characteristic of viruses is their ability to *emerge/lurk* in a computer for days or months, replicating themselves. While this replication takes place, you might not even know that your computer has *contracted/obtained* a virus; therefore, it's easy to *deliberately/inadvertently* spread infected files to other people's computer. A virus also *keeps/delivers* a payload, which can be as harmless as displaying a pesky message or as devastating as trashing the data on your computer's storage device. It can *corrupt/upgrade* files, destroy data, or otherwise *disrupt/arrange* computer operations. A trigger event, such as a specific date, can *hold/unleash* some viruses. Viruses that deliver their payloads on a specific date are sometimes referred to as *logic/time* bombs. Viruses that deliver their payloads in response to other system event are referred to as *time/logic* bombs.

5. Read the passage about a Trojan horse. Match the words in bold with the synonyms in the box.

ignorant; disguise; infamous; reproduce; harmful; propagate

It is not designed to **spread** itself to other computers and it doesn't **replicate** itself. Trojans are stand-alone programs that **masquerade** as useful utilities or applications, which victims download and install **unaware** of their **destructive** nature. They are **notorious** for stealing passwords using a keylogger that records your keystrokes as you log in to your computer and various online accounts.

6. Read the statements about different types of malware. Restore the correct order of the letters in the words in bold.

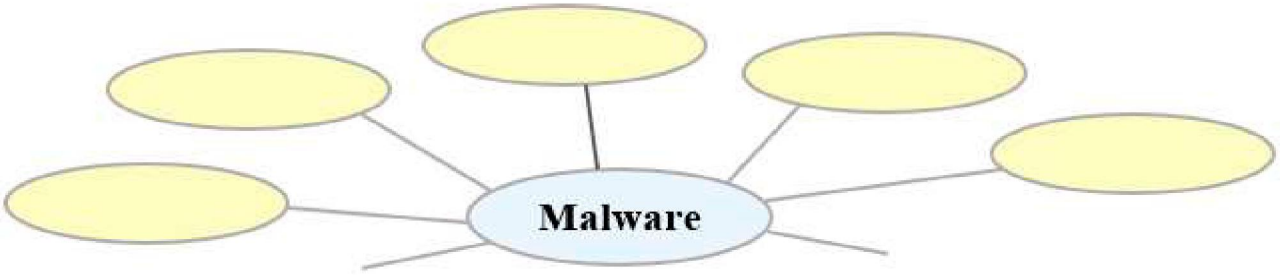
1. **arswepy** is a type of program that secretly gathers personal information without the victim's knowledge, usually for advertising and other commercial purposes.
2. Clicking the attachment activates the **owmr**.
3. Because an intelligent agent behaves somewhat like a **tboor**, it is often called a bot.
4. Just like **jtnaor**, spyware can monitor keystrokes and relay passwords and credit card information to cybercriminals.
5. **wareda** is sponsored by an advertiser and is used to make money.
6. Since this software has administrative access, it means **itkorot** can modify any software, including any that may be used to detect or circumvent it.

7. To get **erramnswao** on your computer or devices, **licybcerrmain** tricks you into downloading a program that looks legitimate.
8. To steal personally identifiable information cybercriminals use **ygregolek**.
9. This **svuri** is triggered when a program capable of executing a macro is run.

7. Choose the options from the ones given in italics to make true sentences.

1. *Trojan horse/Bot* is not designed to replicate itself.
2. *Worm/Spyware* secretly gathers personal information without the victim's knowledge, usually for advertising or other commercial purpose.
3. *Bot/Spyware* initiates communication with central server on the Internet to receive instructions.
4. *Worm/Spyware* monitors your web-surfing and purchasing behaviour and sends a summary to third parties.
5. *Spyware/worm* has the capability to travel without any help from a person.
6. *Trojan horse/Bot* can be used in groups of computers to be controlled by a third party for Distributed Denial-of-Service (DDoS) attacks.
7. *Spyware/Trojan horse* can give a malicious party remote access to an infected computer.
8. *Adware/Ransomware* displays pesky messages and pop-up ads.
9. *Spyware/Ransomware* encrypts your data and demands ransom for the encryption key.
10. *Keylogger/Spyware* gets every your keystrokes to steal your password or credit card number.
11. *Worm/Virus* causes network traffic jams.
12. *Virus/Bot* allows hackers to take control of your device and turn it into a zombie.
13. *Bot/Spyware* links your computer to others in a botnet that can send millions of spam emails.

8. The days when viruses were the greatest threat to computers are long gone. Today, there are lots of types of malware. Complete the concept map and summarise the facts about the types of malware. Report your ideas to the group.



III. Language Box

1. What are the signs to watch out if the device is infected? Use the prompts. Share your ideas with a groupmate.

- ✓ Irritating messages or sounds.
- ✓ Frequent pop-up ads, at times with some provocative content.
- ✓ The sudden appearance of a new Internet toolbar on your browser's home page.
- ✓ An addition to your Internet favourites list that you didn't put there.
- ✓ Prolonged system startup.
- ✓ Slower than usual response to mouse clicks and keyboard strokes.
- ✓ Browser or application crashes.
- ✓ Missing files.
- ✓ Your computer's security software becomes disabled and cannot be restarted.
- ✓ Periodic network activity when you are not actively browsing or sending emails.
- ✓ Your computer reboots itself frequently.

2. Work out the meaning of the words/phrases in the box. Then watch the video "Security Awareness: Internet Downloads" [43] and discuss the questions.

- ✓ to spruce up sth
- ✓ a pitch deck
- ✓ to figure sth out
- ✓ to look super sketchy

a) What infection method is shown?
b) How can you avoid computer infection?
c) Are there any other ways to avoid security threats? Use the ideas in the box below.

- ✓ Install and activate security software on any digital device that is at risk.
- ✓ Keep software patches and OS service packs up to date.
- ✓ Do not open suspicious e-mail attachments.
- ✓ Obtain software only from reliable sources; and before running it, use security software to scan for malware.
- ✓ Do not click pop-up ads – to make an ad go away, right-click the ad's taskbar button and select the Close option.
- ✓ Avoid unsavory Web sites.
- ✓ Disable the option *Hide extensions for known file types in Window* so you can avoid opening files with more than one extension, such as a file called *game.exe.zip*

3. Read the statements related to protection from malware and work out the meaning of the collocations in bold from the context.

1. Criminals use malware to steal personal information and **commit fraud**.
2. Hackers use malware to **hijack your computer** and use it to send spam.
3. Scammers send messages to **trick people into** buying worthless software.
4. Use a **pop-up blocker** and don't switch it off.
5. Don't **open attachments** in e-mails unless you know what they are.
6. Free stuff may **sound appealing** but free downloads can hide malware.

7. If you **take precautions**, malware can find its way onto your computer.
8. If you **suspect malware** on your computer, the first thing to do is to disconnect from the Internet.
9. Delete the files that a system scan **flags as malware**.

4. Watch the video "Protect Your Computer from Malware" [40] and put the ideas into the correct order.

1. Steps for initial computer protection.
2. Definition of malware.
3. Signs of computer infection.
4. Ways to deal with computer infection.
5. Purposes of using malware.

5. Watch the video again. Match the beginnings (1–7) of the statements with the appropriate endings (a–g).

1. Install security software from a reliable company and
2. If you're not sure how,
3. Use a pop-up blocker, and
4. Download software only from
5. If you suspect malware,
6. Update your security software and
7. The most important thing you can do

a) don't click on links and pop-ups.
b) websites you know and trust.
c) set it to update automatically.
d) stop doing things that require passwords or personal info, such as online shopping or banking.
e) use the Help function and search for automatic updates.
f) to prevent malware is to keep your computer software up-to-date.
g) run a system scan.

6. One of the ways to secure computers is installing and updating robust antivirus software. Read the abstract "Antivirus Software" and answer the questions.

1. What type of software is antivirus?
2. What devices does antivirus software run on?
3. How does it identify malware?
4. What is the process of searching for malware called?
5. What are the two techniques to look for a virus?
6. What is a virus signature?

Antivirus Software

The best defense against malware is antivirus software. It is a type of utility software that looks for and eliminates viruses, Trojans, worms, and other malware. It is available for all types of computers and data storage devices, including smartphones, tablets, personal computers, USB flash drives, servers, PCs, and Macs. Popular robust antivirus software includes Norton AntiVirus, Kaspersky Anti-Virus, F-Secure Anti-Virus, Windows Defender, and Avast.

Modern antivirus software runs as a background process and attempts to identify malware that exists on a device or is entering a device as a download, email message, attachment, or Web page. The process of searching for malware is sometimes referred to as scanning or performing a virus scan. To identify malware, antivirus software can look for a virus signature or perform heuristic analyses.

A virus signature is a section of program code that contains a unique series of instructions known to be part of a malware exploit. Although they are called virus signatures, the unique code may identify a virus, worm, Trojan, or other malware exploit.

Heuristic analyses – techniques that detect malware by analysing the characteristics and behaviour of suspicious files

Virus signatures are discovered by security experts who examine the bit sequences contained in malware program code. When discovered, virus signatures are added to a collection of virus definitions, which form a database that is used by antivirus software as it works to scan files that may harbour malware.

7. Mark the statements as true or false. Correct the false ones. Address Task 6 if necessary.

1. Antivirus software is a type of utility software that looks for and eliminates a virus.
2. Antivirus software is available only for personal computers but not for smartphones.
3. Modern antivirus software identifies malware that is entering a device as you download something.
4. The process of searching for malware is sometimes referred to as scanning.
5. To identify malware, antivirus software can examine the length of the program.
6. A virus signature is a section of program code with a common series of instructions.
7. Virus signatures are discovered by users who examine if the program is loading or not.
8. When virus signatures are discovered, they are deleted.

8. Consider the examples of computer disasters. Discuss how you could prevent them or limit their effects. Work in groups of three or four people. Then compare your ideas with the other groups.

1. You open an email attachment which contains a very destructive virus.
2. Someone guesses your password and copies your sensitive data.
3. Your hard disk crashes and much of your data is lost permanently.
4. Someone walks into your computer lab and steals the memory chips from your PC.
5. Your backup USB flash fails to restore properly.
6. A software bug erases necessary pictures, documents, and videos on your hard drive.

IV. Decision Bank

1. Look at the examples of cyberwarfare attacks. How do they affect the world? Have you ever encountered any of them? Do you know how to deal with them?

2. Read the two definitions of cyber weapons, consider which one is done by a security expert and which is done by a legal expert. List their similarities and differences.

A device or any set of computer instructions intended to unlawfully damage a system acting as a critical infrastructure, its information, the data or programs therein contained or thereto relevant, or even intended to facilitate the interruption, total or partial, or alteration of its operations.
Cyber weapon could be defined as a computer code that is used or designed to be used with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.

3. Read the abstract "Cyber Weapons – New Weapons of Mass Destruction" and discuss the questions.

1. What is cyberspace?
2. What illegal activities do people commit in cyberspace?
3. What parameters can cyber weapons be classified by?
4. What makes cyber weapons so attractive?
5. What economic spheres does cyber weapon strike most often?
6. What are the most dangerous effects of the use of cyber weapons?

Cyber Weapons – New Weapons of Mass Destruction

Information and Communication Technology has created a virtual world with no boundaries. This virtual world is called "cyberspace". Worldwide, people and, in some cases, the governments are engaged in the exploitation of the cyberspace for illegal activities like espionage, theft of technology, financial frauds and so on. They have, accordingly, developed means and methods to carry out such activities by way of viruses, rootkits, and malware. These are the initial steps in the evolution of cyber weapons which till date do not have a formal definition.

Cyber weapons may span, in theory, a wide range of possibilities: from Denial-of-Service attacks (which typically have a low level of penetration) to "tailored" malware like the Stuxnet characterised by high intrusiveness and a low rate of collateral damages.

Cyber weapons can be classified according to the following four parameters such as precision that is the capability to target only the specific objective and reduce

collateral damages; intrusion that is the level of penetration inside the target; visibility that is the capability to remain undetected; ease of implementation that is a measure of the resources needed to develop the specific cyber weapon.

The use of cyber weapons is complementary to conventional military strikes. It could be possible to support offensive operations by destroying enemy's defence/critical infrastructure. In this way, cyber weapons are more efficient and less expensive, and the attack is carried out at the speed of light. The preparation phase of this attack is easy to hide from prying eyes and the development of cyber weapon is hard to identify.

The above advantages make cyber weapons very attractive to those "small" states that despite having reduced funds for military expenses can compete with the most powerful countries in the new domain. At present, nearly 140 countries in the world are engaged in the development of an offensive cyber warfare capability.

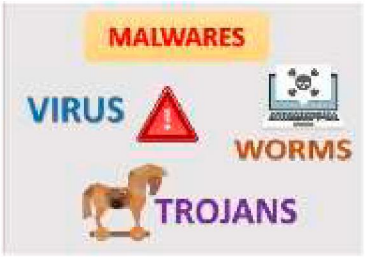
Likely targets of cyber weapons are electronic national defence systems, hospitals, water supplies, fully-automated transportation control systems, air traffic controls, electricity grid management, systems communication and data networks. In general, cyber weapons could hit every critical infrastructure and vital systems of any country.

One of the most dangerous effects of the use of a cyber weapon is the difficulty to predict its diffusion since cyber space has no boundaries. This means that cyber weapons could hit in unpredictable ways other systems and networks that are not considered targets. In extreme cases, there is a possibility that it attacks the systems of host nation in a sort of "boomerang effect". Besides, the presence of cyber weapons in cyberspace could open up the possibility of reverse engineering of its source code by ill-intentioned individuals. Foreign governments, cyber terrorists, hacktivists and cyber criminals could be able to detect, isolate and analyse the agents, designing and spreading new cyber threats that are difficult to mitigate.

4. Cyberattacks are one of the biggest dangers in the world of IT. Give your arguments why it is so. Work in group of three or four people.

V. Conclusion Worksheet

Imagine that you want to enter someone's computer system. List as many ways or techniques as possible that you can use to gain access. Consider what harm can be caused by your actions. Consider the following techniques. Work with a groupmate. Then report your ideas to the group.



- ✓ using keylogging software
- ✓ using Trojans
- ✓ using email worms
- ✓ using spyware
- ✓ using ransomware

VI. Web Search

Explore the resources in the list to obtain additional information on security software and its components. Report your findings to the group.

https://www.welivesecurity.com/category/malware/

https://www.techopedia.com/definition/4536/security-software

https://www.techtarget.com/searchsecurity/definition/malware

VII. Revision Point

1. Read the abstract "Heuristic Analysis" and translate it into Belarusian or Russian. Use a dictionary if necessary.

Heuristic Analysis

Antivirus software can use techniques called heuristic analysis to detect malware by analysing the characteristics and behaviour of suspicious files. These techniques are especially useful for detecting new malware for which signatures have yet to be collected and added to the virus database. One method of heuristic analysis allows the suspicious file to run in a guarded environment called a sandbox. If the file exhibits malicious behaviour, it's treated like a virus and quarantined or deleted. A second method involves inspecting the contents of a suspicious file for commands that carry out destructive or surveillance activities. Heuristic based antivirus tools use a number of different scanning techniques, including file analysis when the scanning software will closely inspect a file to determine its purpose, destination and intent; file emulation, also known as dynamic scanning or sandbox testing, file emulation tests a file in a controlled virtual environment to see what happens; genetic signature detection designed to locate different variations of a virus.

2. Do the quiz.

1. What is used to find out browsing habits, keystrokes, or passwords for the purposes of identity theft?	a) Trojan horse b) adware	c) virus d) spyware
2. When a computer starts performing repetitive tasks it can be due to …	a) rootkit b) spyware	c) a bot d) spam
3. How is a worm different from a virus?	a) It does more harm b) It can't spread without a user doing sth c) It can spread without a user doing sth d) It doesn't do any harm	

4. What most defines a computer virus?	a) It crashes computers b) It can spy on what you do c) It can copy and spread itself d) It cannot be fixed
5. Trojan is a virus that …	a) is easy to detect due to its suspicious signs b) can multiply quickly into copies of itself c) is similar to human viruses d) is difficult to detect because it replicates itself as a safe program
6. It is a set of software tools that enable an unauthorised user to gain control of a computer system without being detected	a) ransomware b) Trojan horse c) rootkit d) adware
7. It generates revenue for its developers by automatically generating adverts on your screen, usually within a web browser	a) spyware b) ransomware c) rootkit d) adware

3. Choose the options from the ones given in italics to make true statements.

Nowadays, it is a big challenge to protect our *sensitive/available* data from unwanted and unauthorised sources. There are various tools and devices that can provide different *security/danger* levels and help keep our *private/public* data secure. One such tool is a firewall that *prevents/encourages unauthorised/legitimate* access and keeps our computers and data safe and secure.

A firewall can be defined as a special type of network security device or a software program that *monitors/ignores* and filters incoming and outgoing network traffic based on a *defined/undefined* set of security rules. It acts as a barrier between internal private networks and external sources such as the public Internet. The primary purpose of a firewall is to allow *non-threatening/damaging* traffic and prevent *malicious/ridiculous* or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users *block/open* malicious software from accessing the Internet on infected computers.

4. Get ready to speak on the topics below and assess your performance according to the following scale.

Comprehensive	Rather confident	Limited

- Malware, types, ways to be infected.
- Practices to avoid computer infection.
- Antivirus software, techniques.
- Cyberwarfare attacks, cyber weapon.

Lesson 3: Social Engineering

Aim	Objectives
Master communication skills and competences in social engineering methods and protection procedures in the sphere of IT	At the end of this lesson, students will be able to: • define the concept of social engineering • describe the main methods of social engineering • list measures of protection against social engineering scam • explain how encryption work • discuss and present findings in pairs and small groups • write a summary based on different media

I. Lead-in

1. What is social engineering in terms of IT? Consider the three definitions and choose the appropriate one.

A. It refers to applying engineering approach and innovation to the field of social relations

B. It refers to the ethical issues which arise in the process of interaction between people and different devices

C. It is a manipulation technique that exploits human errors to gain private information, access, or valuables

2. Share your opinion on the statement. Justify your point of view.

Security is all about knowing who and what to trust. Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value.

II. Vocabulary Focus

1. Consider the facts about social engineering. Work out the meaning of the words in bold. Then make a list of key terms and collocations related to the topic.

In the context of cyber security, social engineering is a **deceptive** practice that **exploits** human psychology.

Its goal is to **induce** victims to interact with a digital device and get financial **gain** or cause service **disruption**.

The types of information these **scammers** are seeking can **vary**.

When individuals are targeted, the criminals are trying to **trick** you **into** giving them your **credentials**, bank information or access your computer.

Social engineer is a **judgement-neutral** term for a person who **devises** and carries out an **exploit**.

The **bait** that is set forth in various such exploits is based on one or more **incentives** designed to **compel** individuals to participate in the **scam**.

Social engineering attacks **prey on** human **vulnerabilities**, for example, **gullibility**, curiosity, greed. None of us is **infallible**.

2. Match the words in Column A with their synonyms in Column B.

A.	B.
deceptive	javelin, pike
spear	fake, false
bait	reward
gain	catch, take
solicitation	misleading
fraudulent	simulate, pretend
spoof	decoy
nab	extortion

3. Match the most common methods of social engineering on the left with the definitions.

1. Shouldering (shoulder surfing) 2. Pharming 3. Phishing 4. Baiting 5. Spear Phishing 6. Vishing 7. Tailgating 8. Rogue Antivirus	a) This tactic includes deceptive emails to steal information. b) A spoofed email is used to carry out targeted attacks against individuals or businesses. c) It's an online and physical social engineering attack that promises the victim some gain. d) Victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed. e) It relies on human trust to give the criminal physical access to a secure building or area. f) It redirects website traffic to fraudulent websites that distribute malware, collect personal data, sell counterfeit products, and perpetrate other scams. g) It occurs when someone surreptitiously watches over your shoulder to nab valuable information. h) It is voice solicitation over the phone (voice+phishing)

4. Complete the passage about one more type of social engineering with the words in the box. What is it? How does it work?

convince; targeted; spoofing; perpetrate; baiting; relies; solicitation; quo

A quid pro 1) _____ attack is a low-level form of 2) _____ hacking that 3) _____on human trust. It is also known as a "something-for-something attack". It is a case of 4) _____, as attackers 5) _____ victims to get a service or benefit and the latter performs specific tasks or gives out information or access. An example would be a case of voice 6) _____ when an attacker calls your phone 7) _____ to be from one of your service providers' technical support representatives. They will offer you some assistance that is used to 8) _____ a scam.

5. Before watching the video from "Security Awareness" series look at the picture on the right and say what is going on in the office today. Predict what can go wrong this time. Work out the meaning of the words and phrases below.

- ✓ on behalf of
- ✓ a cyber vigilance and security award
- ✓ to run an influencer blog
- ✓ an engraving
- ✓ a plaque

6. Savvy cybercriminals know that social engineering works best when focusing on human emotions. Watch the video "Security Awareness: Episode 6" [43] and identify the type of social engineering in Task 3 it illustrates. Then choose which emotions/traits have been exploited from the ones given in the box.

helpfulness; curiosity; fear; gullibility; urgency; greed

7. Look through the examples of social engineering attacks and decide which emotion/trait from the ones listed in Task 6 is exploited in each case.

A. You receive a voicemail that says you're under investigation for tax fraud, and that you must call immediately to prevent arrest and criminal investigation

B. Imagine if you could simply transfer $10 to an investor and see this grow into $10,000 without any effort on your behalf. A carefully worded baiting email tells victims to provide their bank account information and the funds will be transferred

C. Cybercriminals pay attention to events capturing a lot of news coverage. For example, after the second Boeing MAX8 plane crash, cybercriminals sent emails with attachments that claimed to include leaked data about the crash. In reality, the attachment installed a version of the worm RAT on the victim's computer

D. Cybercriminals target two or three employees in the company with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database urgently stressing that the manager needs it to make sure everyone gets paid on time

E. You receive an email from an online shop that you frequently buy from telling you that they need to confirm your credit card information to protect your account. The email language urges you to respond quickly, or your credit card information can be stolen

8. Use the ideas to make questions that can be asked considering the main issues of this section. Then discuss these questions in groups of three or four people.

- ✓ Spread of social engineering.
- ✓ Types of social engineering attacks.
- ✓ Red flags of such scams.
- ✓ Typical victims of phishing, vishing, smishing.
- ✓ Emotions being exploited in such attacks.

III. Language Box

1. Watch the video "Hack Attack – Vishing" [34] which shows a sample vishing call from the inside and answer the questions.

a) What does a deceptive scammer use to perpetrate a scam?
b) Why is voice solicitation so quick and successful?
c) What red flags can indicate that it's a fraudulent phone call?
d) What information was compromised?
e) What further actions should be taken to protect information after being compromised?

2. Aside from knowing how social engineering works and looking for red flags, there are some ways how you can protect yourself from such scams. Distribute the tips below between the two categories.

Protection against phishing

Protection against vishing

a) Be cautious about all communications you receive. If it appears to be a suspicious one, do not respond. Delete it.
b) Don't pick up the phone, simply let it go to voicemail. Caller IDs can be faked, which means you might not know who's calling. Later decide whether to call back.

c) Don't press buttons or respond to prompts. Scammers often use these tricks to identify potential targets for more robocalls. And the record of your voice can be used to navigate voice-automated phone menus.
d) Don't enter personal information in a pop-up screen. Legitimate companies and organisations don't ask for personal information via pop-up screens.
e) Do not click on any links listed in the email message, and do not open any attachments contained in a suspicious email.
f) Install a special spam filter on your email application and your web browser. These filters will not keep out all fraudulent messages, but they will reduce their number.
g) Hang up. The moment you suspect it's a fraudulent phone call, don't feel obliged to carry on a polite conversation. Simply hang up and block the number.
h) Verify the caller's identity. If the person provides a call-back number, it may be part of the scam, so don't use it.

3. Explain the words in bold. Use the following facts and work out the definition of what smishing is. Keep in mind it is a portmanteau word.

a) As users grow more **overwhelmed** by constant emails and suspicious of spam, text messages have become a more attractive attack vector.
b) In addition, people are often less **watchful** for suspicious messages on their phones than on their computers.
c) Smishers may try to convince you to give up a username password **combo** or other confidential information and use it for **nefarious** purposes later.
d) Bank's mission is one of the most **lucrative** and common types of this category of attack.
e) A smishing scam can convince users to download an app **purporting** to be from the nation's postal service.
f) Attackers can **plunder** your bank account, install malware on your phone that gains access to your finances or your location information, or trick you into spending money needlessly.

portmanteau word
[pɔːt'mæn.təʊ ˌwɜːd] –
a word formed by
combining two other words

4. Watch the video "What Is Smishing?" [56]. Write down what the following words, collocations and figures refer to:

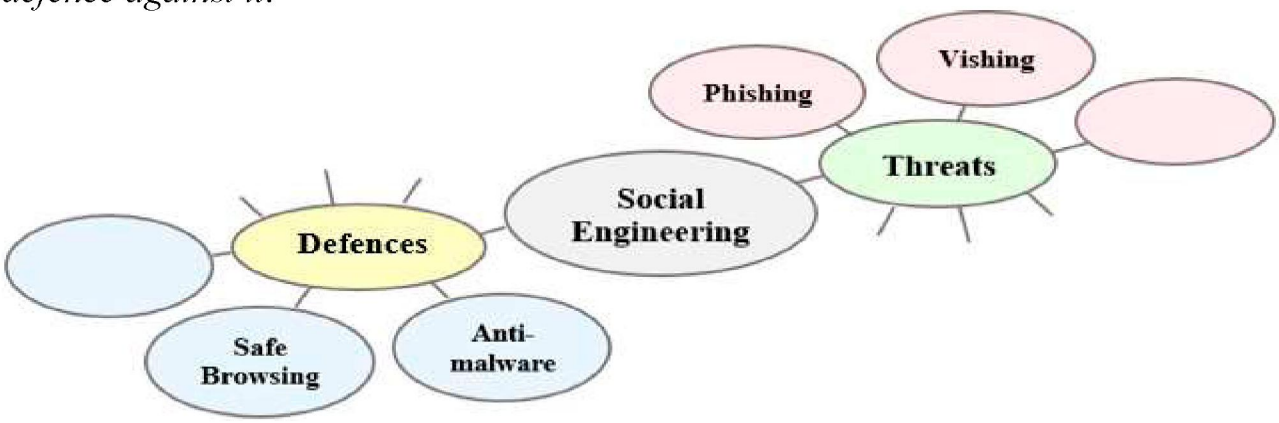
a) misleading text messages;
b) since the 1990s;
c) 98 % and 45 %;
d) 20 % and 6 %;
e) intimate relationships;
f) credentials;
g) the Czech Republic;
h) a few hundred dollars;
i) clergyman.

5. Watch the video again and provide the following information.

a) Give a proper definition to smishing.
b) Explain why it is becoming so widely spread today.
c) Name its main categories.
d) List the emotions that are mainly exploited.

6. Work out a list of measures how to be protected from smishing. Work in groups of three or four people. Then report your ideas to the rest of the group.

7. Use the information from this section and your background knowledge to complete the concept map. Then get ready to speak about social engineering, its threats and defence against it.

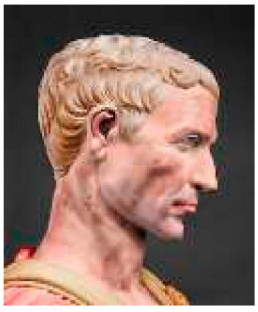


8. Interview some of your groupmates to elicit responses on the following questions. Then share the most interesting information gathered with the group.

a) Why do scammers use social engineering rather than hacking?
b) Why are people so gullible?
c) How can we avoid taking the bait and becoming victims of such scams?

IV. Decision Bank

1. Since ancient times people have been trying to protect sensitive information. Do you recognise the person in the picture? How is he related to the issues of cyber security? Can you break the cipher and read the secret message below? Is it a hard cipher to break?



Secret Message

c	v	v	c	e	m	c	v	f	c	y	p

Original Message

2. Choose the options from the ones given in italics to make true statements. Watch the video "How Encryption Works" [35], check your ideas and get ready to explain how encryption functions.

encryption – the process of converting plain text to cipher text

a) Keeping your text messages protected against *eavesdroppers/interlocutors* has become a major issue today.
b) Your text messages are protected using *end-to-end/open* encryption.
c) Your phone has two *versatile/unique* keys that encrypt and decrypt messages.
d) Two people use the other person's public key combined with their own private key to create a *permanent/temporary* shared key.
e) They then use the shared key to encrypt messages to each other and their public keys are used to confirm that those shared keys are *fake/authentic*.
f) Some people believe that tech and telecom companies should provide what's called *backdoor/doorway* access to these encrypted messages.
g) The first type of backdoor is a list of *public/private* keys that allow the company access to encrypted messages.
h) But if the list of private keys is hacked or compromised, every person's private key is up for *leaves/grabs*.
i) The second type of backdoor is for tech companies to *deliberately/unintentionally* build a weakness or flaw into the encryption formula.
j) At the core of this whole debate is the very *simple/thorny* issue of personal privacy versus national security.

3. Watch the video again and complete the ideas.

1. The government says it occasionally needs access to some of these messages … .
2. End-to-end encryption happens whenever you send … from your smartphone.
3. Your public key is shared with other people, and it's used as … .
4. Your private key is only on your device and … .
5. When two people want to securely chat they use a combination of … .
6. The shared keys are being … constantly which ensures that people's conversation cannot be decrypted in the future.
7. The first type of backdoor access to the encrypted messages is a list of private keys that allow the company … .
8. The second type of backdoor is for tech companies to … into the encryption formula.

4. Read the article "Why Encryption Matters" published on the NortonLifeLock and decide whether the sentences in italics render the main or additional information. Give your view on the issues discussed in the article. Address the key ideas below.

Encryption for Internet privacy	Cybercrime as a big business	Encryption to commit cybercrime	Protection from ransomware

Why Encryption Matters

Written by Dan Rafter
Updated on Jun 12, 2023

Encryption helps protect your online privacy by turning personal information into "for your eyes only" messages intended only for the parties that need them and no one else. You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.

Cybercrime is a global business, often run by multinational outfits. Many of the large-scale data breaches that you may have heard about in the news demonstrate that cybercriminals are often out to steal personal information for financial gain.

Encryption is designed to protect your data, but it can also be used against you. Targeted ransomware is a cybercrime that can impact organisations of all sizes, including government offices. Ransomware can also target individual computer users. Attackers deploy ransomware to encrypt the various devices, including computers and servers, of victims. *The attackers often demand a ransom before they will provide a key to decrypt the encrypted data.* The goal is to persuade victims to pay out as a way to recover access to their important files, data, video and images. *Ransomware attacks against government agencies can shut down services, making it hard to get a permit, obtain a marriage licence, or pay a tax bill, for instance.*

But ransomware attacks can also happen to you. *Here are some tips to help protect your devices from ransomware attacks and the risk of having your data inaccessible.*

Install and use trusted security software on all your devices, including your mobile phone. Keep your security software up to date. It can help protect your devices from cyberattacks. Update your operating system and other software. This can patch security vulnerabilities. *Avoid reflexively opening email attachments.* Why? Email is one of the principal methods for delivering ransomware. Be wary of any email attachment that advises you to enable macros to view its content. *If you enable macros, macro malware can infect multiple files.* Back up your data to an external hard drive. If you're the victim of a ransomware attack, you'll likely be able to restore your files once the malware has been cleaned up. Consider using cloud services. This can help mitigate a ransomware infection, since many cloud services retain previous versions of files, allowing you to "roll back" to the unencrypted form. Don't pay the ransom. You could pay a ransom in hopes of getting your files back, but you might not get them back. *There's no guarantee the cybercriminal will release your data.*

Encryption is essential to help protect your sensitive personal information. But in the case of ransomware attacks, it can be used against you.

V. Conclusion Worksheet

Split into teams. Roll the dice in turns – use the one online https://freeonlinedice.com – and play the game. Appoint your lecturer to judge you. Every wrong answer returns your team to Start. The first team to reach Finish are the winners.

The *Can you … ?* Game

START	1. define social engineering (SE)?	2. name the goal of SE?	3. name the weakest link in the security chain?
7. list vulnerabilities scammers exploit? (at least 4)	6. name the methods of SE? (at least 5)	5. describe what the bait can be?	4. explain what a social engineer does?
8. explain what shouldering is?	9. explain what pharming is?	10. explain what phishing is?	11. explain what baiting is?
15. explain what rogue antivirus is?	14. explain what tailgating is?	13. explain what vishing is?	12. explain what spear phishing is?
16. explain what quid pro quo is?	17. explain what smishing is?	18. name the red flags of phishing? (at least 5)	19. list he ways of protection against phishing? (at least 3)
23. explain the difference between public and private keys?	22. define encryption?	21. recall the first person who encrypted a message?	20. list he ways of protection against vishing? (at least 3)
24. explain what symmetric encryption means?	25. explain what asymmetric encryption means?	26. prove why encryption matters?	FINISH

VI. Web Search

Explore the resources in the list to obtain additional information on social engineering and encryption. Report your findings in writing.

https://theconversation.com/us/search?q=social+engineering

https://www.welivesecurity.com/ category/cybersecurity/

https://theconversation.com/us/topics/encryption-241

VII. Revision Point

1. Use the key vocabulary of this lesson and find the terms that match the definitions.

1. It involves an attacker directly targeting a specific organisation or person with tailored phishing communications.
2. It's a type of social engineering attack where a scammer uses a false promise to lure a victim into a trap.
3. It is a form of cyberattack that sends you to a fake website that looks like the real thing.
4. Such attack describes a situation where the attacker can physically view the device screen and keypad to obtain personal information.
5. It is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information.
6. It happens when someone sneaks into a restricted area by using someone else.
7. It's a type of malware that pretends to have found an infection on the victim's computer.

2. Use the opposite words to the ones given in italics to correct the information.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other 1) *cipher text* messages. The simplest method uses the 2) *asymmetric* or secret key system. Here, data is 3) *decrypted* using a secret key, and then both the encoded message and secret key are sent to the 4) *sender* for decryption. But, if the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the 5) *symmetric* or 6) *private* key system. In this case, every user has two keys: one public and one private. Senders 7) *offer* the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's 8) *public* key will decode it.

3. Render the article "Think Before You Scan" published on WeLiveSecurity by ESET orally. Record your speech and send it to your groupmate for assessment according to the checklist below. Your overall mark will be provided at the end of the table.

Think Before You Scan
How fraudsters can exploit QR codes to steal money

Cecilia Pastorino
Updated May 4, 2023

QR codes are having a moment. The humble squares may have been around since 1994, but it wasn't until the COVID-19 era that they became a truly household name. These days, you can spot them all over the place, with the codes put to use for everything from displaying restaurant menus to facilitating contactless transactions to being built into contact tracing apps. Much like any other popular technology, however, the widespread use of QR codes has also caught the attention of scammers, who have co-opted them for nefarious purposes.

Short for "Quick Response", a QR code is a type of machine-scannable barcode that, as implied by its name, is designed to be read and interpreted instantly by a digital device. A QR code can store up to 4,296 alphanumeric characters, although the commonly used ones tend to contain fewer characters and so allow for easy decoding by a smartphone's camera.

The text strings that are encoded within a QR code may contain a variety of data. The action prompted by reading a QR code depends on the application that is interacting with said code. The codes may be used to open a website, download a file, add a contact, connect to a Wi-Fi network, and even make payments.

It can redirect you to a malicious website to steal sensitive information. Phishing attacks don't spread only by emails, instant messages, or text. Just as attackers can use malicious ads and other techniques to direct victims to fraudulent sites, they can do the same with QR codes. This is especially a concern if the codes are put up in adverts in busy areas or near banks or other financial institutions.

QR code can download a malicious file on your device. Many bars and restaurants use QR codes to download a PDF-format menu or install an app enabling patrons to place an order. Attackers could easily tamper with the QR code to try to trick the potential victim into downloading a malicious PDF file or a rogue mobile app.

QR codes can trigger actions directly on your device. However, there are some basic actions that any basic QR reader is capable of interpreting. These include connecting the device to a Wi-Fi network, sending an email or SMS message with a predefined text, or saving contact information on the device.

Most financial apps today allow making payments through QR codes that contain data belonging to the recipient of the money. However, attackers could modify these QR codes with their own data and receive payments into their accounts. It could also generate codes with money collection requests to deceive buyers.

Many QR codes are used as a certificate to verify a person's information, such as their ID or vaccine pass. In these cases, the QR codes may contain information that

is as sensitive as the information contained in their ID or medical records, which an attacker could easily obtain by scanning the QR code.

In most scenarios, the attacker will need to generate a malicious QR code that will replace the original one. In other words, the attacks involve social engineering and rely on duping the victim into taking an ill-fated action.

Here's what to consider before scanning a QR code. Before scanning a QR code, check that it has not been tampered with; for example, verify that it doesn't cover up another QR code. Refrain from scanning randomly found QR codes or codes in unsolicited messages. Be very careful when it comes to using a QR code to pay a bill or conduct another kind of financial transaction. Consider using another payment option. Disable the option to perform automatic actions when scanning a QR code, such as visiting a website, downloading a file, or connecting to a Wi-Fi network. After scanning, look at the URL to check that it's legitimate. Do not share QR codes containing sensitive information. When generating a QR code, use a reputable service. Such a service can also verify that the QR is genuine and performs the desired action. Keep your apps up-to-date and use security software.

Summary checklist	*Yes*	*Undecided*	*No*
1. The origin of the publication was mentioned			
2. The date of the column was provided			
3. The style of the script was defined and justified			
4. The genre of the post was indicated and justified			
5. The author of the article was called			
6. The title of the post was given			
7. The main idea of the article was identified			
8. The important points were included			
9. The unnecessary details were left out			
10. The personal opinion/impression of the article was given			
11. The personal view on the topic/problem was provided			
12. The summary included own vocabulary not citations			
13. The summary was full of varied grammar structures			
The overall mark (excellent/good/satisfactory/below average/bad)			

4. Get ready to speak on the topics below and assess your performance according to the following scale.

Comprehensive	Rather confident	Limited

- Social engineering, state of the issue.
- Methods of social engineering.
- Protection techniques against phishing, vishing, smishing.
- Encryption, its types, usage, importance.

Wordlist

Topic: Digital Security

Adware *n*	Replicate *v*
Appealing *adj*	Rootkit *n*
Assault *n, v*	Scam *n, v*
Attachment *n*	Scan *n, v*
Authentication *n*	Shield *n, v*
Baiting *n*	Shouldering *n*
Bot *n*	Smishing *n*
Compel *v*	Sniffing *n*
Compromise *v*	Spoof *n, v*
Confirm *v*	Spyware *n*
Conventional *adj*	Surreptitiously *adv*
Countermeasure *n*	Suspect *n, v*
Credentials *n, pl*	Tailgating *n*
Current *n, adj*	Trick (into) *v*
Cyberspace *n*	Unaware *adj*
Deceptive *adj*	Unintentional *adj*
Devastating *adj*	Unleash *v*
Disruption *n*	Virus *n*
Encryption *n*	Vishing *n*
Espionage *n*	Worm *n, v*
Exploit *n, v*	
Fraud *n*	*Collocations:*
Fraudulent *adj*	
Gain *n, v*	Be on the lookout
Hacktivist *n*	Brute force attack
Hijack *n, v*	Collateral damages
Inadvertently *adv*	Cyber weapon
Induce *v*	Denial of service
Infallible *adj*	Dictionary attack
Intercept *v*	Heuristic analyses
Keylogger *n*	Identity theft
Leakage *n*	Password manager
Lucrative *adj*	Pop-up ads
Lurk *v*	Power surge
Malicious *adj*	Private key
Malware *n*	Public key
Mitigate *v*	Quid pro quo
Nefarious *adj*	Retinal pattern
Notorious *adj*	Rogue antivirus
Outlet *n*	Spear phishing
Overhaul *n, v*	Surge strip/suppressor
Payload *n*	Third party
Penetration *n*	Trigger event
Pharming *n*	Trojan horse
Phishing *n*	Verification code
Precaution *n*	Virus signature
Prey (on) *v*	Voice solicitation
Ransomware *n*	

List of Abbreviations

ADSL – Asymmetric Digital Subscriber Line
AI – Artificial Intelligence
ALU – Arithmetic Logic Unit
API – Application Programming Interface
AR – Augmented Reality
ATM – Automated teller machine (Cash-point)
BIOS – Basic Input Output System
BSoD – Black screen of death
CPU – Central Processing Unit
CU – Control Unit
DDoS - Distributed denial-of-service
DIMM – Dual in-line memory modules
DL – Deep learning
DNS – Domain Name Server
DoS – Denial of service
dp – dot pitch
DSL – Digital subscriber line
DSS – Decision support system
FTP – File Transfer Protocol
GSM – Global System for Mobile Communication (Groupe Spécial Mobile)
GUI – Graphical User Interface
HDD – Hard Disk Drive
HTML – Hypertext Markup Language
HTTP – Hypertext Transfer Protocol
ICT – Information and Communications Technology/Technologies
ID – Identity document
InfoSec – Information security
IoT – Internet of Things
IRC – Internet Relay Chat
IS – Information System
ISP – Internet Service Provider
LAN – Local Area Network
MAN – Metropolitan Area Network
MIS – Management information system
ML – Machine learning
OOP – Object-oriented programming
PAN – Personal Area Network
PC – Personal computer
PDA – Personal digital assistant
PIN – Personal identification number
POP – Post Office Protocol
P2P – Peer-to-peer
P2P – Point-to-point
QoS – Quality of service
RAM – Random Access Memory

ROM – Read Only Memory
RSS – Really Simple Syndication
SDLC – System development life cycle
SDSL – Symmetric Digital Subscriber Line
SMTP – Simple Mail Transfer Protocol
SSD – Solid State Drive
STOP – Security Tracking of Office Property
SU – System Unit
TCP/IP – Transmission Control Protocol/Internet Protocol
TelNet – Telecommunication Network
TPS – Transaction processing systems
UDP – User Datagram Protocol
UID – Unique identifier
URL – Uniform Resource Locator
USB – Universal Serial Bus
VoIP – Voice over Internet Protocol
VR – Virtual Reality
WAN – Wide Area Network
WAP – Wireless access point
Wi-Fi – Wireless Fidelity
WWW – World Wide Web
XML – Extensible Markup Language