Digital security

1.Security basics

**Security in IT**- is the defence of digital information against internal and external,malicious and accidental threats.

**Physical security** is the protection of the physical parts of the computer from physical actions or disaster.

**Information security** is the measures to prevent,detect and respond to assaults to digital and non-digital information assets.

**Application** security It's a protection of applications from stealing,modifying or deleting.

**Countermeasures** is just a firewalls, patches, encryptions method and authentication.

2.Computer protection and maintenance.

As for computer protection you should never leave your computer unattended in public places, never

turn off or uninstall security tools.

1.Anti-theft protects your devices from physical theft.

2.Cleaning- the best way is to keep your computer clean

3.Troubleshooting- calling an IT specialist to fix something or just to give advice on how to do it.

4.Surge strip is a device that contains electrical outlets that block surges.

5.Restarting your computer helps you when some programs work incorrectly.

6.Antivirus- program, which detects the viruses.

7.UPS helps you to finish your computer with battery backup power during a power outage.

3.Types of password attacks.

1.Brute force attack is a software, which calculates all possible combinations of the words,letters or

even characters.

2.Sniffing is a method,when a hacker tracks all the traffic on the wired or wireless network(but most

popular in wireless) and tries to find sensitive data.

3.Dictionary attack is a method,when hackers guess your password with a dictionary,which contains

thousands of the most commonly used passwords.

4.Keylogger is a software, which records all the keystrokes.

5.Trojans is a program which seems to perform one function,but actually does something else.

4.Password security, authentication.

Authentication- is the way to verify a person's identity. Two factor authentication is a way to increase

security of your data or account by sending verification code after entering the password.

Password security tips:

1. You should avoid personal info such as pets,kids names,birthdays,addresses etc.

2. At least 8 characters.

3. Uppercase,lowercase letters,numbers,characters.

4. Different passwords for different sites.

5. If you have trouble with remembering passwords, use password managers.

5.Malware, types.

Malware- is a type of software that is designed to cause damage to computers and computer systems.

1. Virus- is a program that requires human intervention, infects hosts. There are 2 types of viruses

according to trigger events : time bomb, which activates on a specific date, and logic bomb, which

activates thanks to specific action.

2. Trojan- is a program that seems to perform one task, but actually does something else. It does not

replicate itself, but it spreads only as a payload.

3. Worm is a type of malware, that doesn't require any human intervention,

4. Bot- is a program that performs pre-defined, automated, repetitive tasks.

5. Spyware- type of malware that monitors your online behaviour and sends it to third parties.

6. Keylogger- is a program,which remembers all your keystrokes.

7. Adware- is a software that displays unwanted pop-up ads but it doesn't do any harm to computers.

8. Ransomware- is a software, which limits the user until they pay.

9. Rootkit- is a program that masks itself or other software existence.

10. Bug- is an programmer error in the source code that can lead to unexpected results.

6.Practices to avoid computer infection.

1. Keep software patches and OS service packs up-to-date.

2. Download only from trusted sites and sources.

3. Avoid unsavoury Web-sites.

4. Using antivirus software and scanning files for malware.

5. Use a pop-up blocker to prevent unwanted pop-up ads.

6. Don't click on suspicious links.

7. Antivirus software, techniques.

Antivirus software- is a type of utility software that looks for and eliminates different types of malicious

software that are known at the moment. It is available for all types of computers and devices. Scanners

detect viruses when your computer is already infected, while virus shields in the moment of infection.

Scanning- is a process of searching for malware. There are 2 techniques to look for a virus : a virus

signature- a unique set of commands,that is exploit by malware (database of known virus signature),

heuristic analysis- analysis characteristics and behaviour of files

8. Cyberwarfare attacks, cyber weapon.

Cyberspace- is a virtual world created by computer systems and networks, where everyone can share

and access information, communication, and services globally.

Cyber warfare is the use of technology to conduct attacks on computer systems and networks with the

intention of causing damage, disruption or espionage. Cyber weapons are tools or methods used in

cyber warfare to carry out attacks on targets.

Cyber warfare attacks can take many forms, including malware, viruses, denial-of-service (DoS)

attacks, phishing, and social engineering. These attacks can target government agencies,

businesses, critical infrastructure, and individuals.

9. Social engineering, state of the issue.

Social engineering- it's a manipulation technique to get financial gain.

10. Methods of social engineering.

1. Shouldering- it's when someone watches over your shoulder to get valuable information.

2. Pharming- when someone redirects website traffic to a fraudulent website that collects your data.

3. Phishing- is a tactic that includes deceptive emails to steal information.

4. Baiting- is a tactic used to promise some gain to the victim.

5. Spear phishing- it's like phishing, but is used against individuals.

6. Voice phishing- it is when an attacker uses a telephone line to solicit your card number or other

private information.

7. Tailgating- is a type of social engineering when the hacker does the same activities that you do.

8. Rogue Antivirus- is a type of malware that pretends to be legitimate antivirus software, but it asks for

money to remove viruses and other malware.

11. Protection techniques against phishing, vishing, smishing.

1.Limit Public Information: Limit the amount of personal and sensitive information that is publicly

available, such as on social media, to make it more difficult for attackers to use it in attacks.

2.Verify the Source of any request for sensitive information, whether it comes in the form of an email,

phone call, or text message.

3.Do not click on links or download attachments from unknown sources.

4.Use Anti-Phishing Tools such as web filters and spam blockers, to block phishing emails and prevent

them from reaching employees and individuals.

5.Use encrypted connections, such as HTTPS and VPNs, to protect sensitive information when

accessing websites or transmitting data online.

12.Encryption, its types, usage, importance.

Encryption- is the process of converting plain text to cipher one. Encryption is designed to protect our

data, but it also can be used against us.

There are two many types of encryption :

1.Symmetric encryption uses the same key for both encryption and decryption.

2.Asymmetric encryption uses two keys- a public key and a private key- to encrypt and decrypt

information.The public key can be freely shared, while the private key is available only on your device

and never shared.

Usage: encryption used in secure communication, data storage and digital signatures.

Importance: encryption helps to protect sensitive information from being accessed by unauthorised

parties.

**Digital security**

**Security basics**  
IT security protects digital information from internal/external and accidental/malicious threats.

**Physical security:** protection of computer hardware.

**Information security:** protection of digital and non-digital info.

**Application security:** prevents unauthorized access or changes.

**Countermeasures:** firewalls, patches, encryption, authentication.

**Computer protection and maintenance**

Never leave your computer unattended; don’t disable security tools.

Anti-theft, cleaning, troubleshooting, surge strips, restarting, antivirus, UPS — all help to keep your system safe and running.

**Types of password attacks**

**Brute force:** tries all combinations.

**Sniffing:** captures data on networks.

**Dictionary attack:** uses common passwords.

**Keylogger:** records keystrokes.

**Trojan**: appears safe but steals data.

**Password security and authentication**

**Authentication verifies identity**; two-factor adds extra protection.  
Tips:

1. Avoid personal info.
2. Use 8+ characters with mixed symbols.
3. Use different passwords.
4. Try password managers.

**Malware types**

Virus: needs user action; worm: spreads on its own.

Trojan, bot, spyware, keylogger, adware, ransomware, rootkit, bug — all harm or exploit systems differently.

**Practices to avoid computer infection**

Update software, avoid shady sites, use antivirus and blockers, don’t click unknown links.

**Antivirus software**

Detects/removes malware.

Scanners work after infection, shields prevent it.

Virus signature vs heuristic analysis to detect threats.

**Cyber warfare attacks, cyber weapons**

**Cyberspace:** virtual networked world.

**Cyber warfare:** tech-based attacks using malware, DoS, phishing, etc.

**Cyber weapons**: tools used in such attacks.

**Social Engineering, state of the issue**

Manipulation to gain financial/data advantage.

**Methods of social engineering**

Shouldering, pharming, phishing, baiting, spear phishing, vishing, tailgating, rogue antivirus — trick users into revealing info.

Protection techniques against phishing, Vishing, Smishing

Limit public info, verify sources, don’t click unknown links, use filters and VPNs.

**Encryption, it types, usage, importance**

Converts data to unreadable format.

Symmetric: one key for all.

Asymmetric: public/private key.

Used in secure communication, storage, and digital signatures.

Protects data from unauthorized access.