**Topic 9 Digital security**

***Security basics.***

Digital security is the protection of digital information from internal and external malicious threats. This protection includes detecting, preventing, and responding to threats through security policies, software tools, and IT services.

There are two main types of digital security. Physical security is the protection of personnel, equipment, software, networks, and data from physical actions, intrusions, and other events that may harm an organization. An example of a common physical security threat is an attacker who infiltrates an organization and uses a USB drive to copy and delete sensitive data or physically deliver malware directly to systems. Information security is the protection of any data by using and creating certain programs, encryption, and the like.

***Password security.***

A password is a series of characters that verifies a user ID. Password security is the most common protection of any data from hackers. But such protection is not reliable, since it is necessary to set passwords according to certain rules, if they are not followed, then there will be no point in using this type of digital security protection.

***Hardware security.***

Hardware security is a discipline that includes hardware design, access control, secure computing, secure storage of keys and passwords, code authentication, and the like.

***Malware.***

Malware (malicious software) is software created to damage or change the computer data or its operations.

These are main types of malware:

Viruses are programs that spread by attaching themselves to executable files or documents. Any code that is designed to hide the existence of processes and privileges is referred to as a rootkit. Worms are self-copying programs that can move from one computer to another without human help, by exploiting security flaws in computer networks. Trojan horses are malicious programs disguised as innocent-looking files or embedded within legitimate software. Spyware, software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software

***Social engineering.***

Social engineering is the psychological manipulation of people to perform actions or disclose confidential information. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into disclosing data, distributing malware, or providing access to restricted systems. Attacks can occur online, in person, and through other interactions.

As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware. Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Pretexting- Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task. As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

***Encryption.***

Encryption is the basic building block of data security. Encryption transforms a message or data file in such a way that its contents are hidden from unauthorized readers. An original message or file that has not yet been encrypted is referred to as plaintext or cleartext. An encrypted message or file is referred to as ciphertext. The process of converting plaintext into ciphertext is called encryption. The reverse process—converting ciphertext into plaintext—is called decryption.