**Lesson 1**

Security, in information technology (IT), is the defense of digital information against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to this threats.  
  
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.  
  
In the context of digital security, user authentication is any technique used to verify 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. Strong password is long and hard to remember, it consists of numbers, upper and lowercase letters and other symbols.  
  
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 also uses password-cracking software but its range is much more extensive than the dictionary attack. Because it uses all possible combinations of letters to find a password, a brute force attack can run for days to crack some passwords. A dictionary attack helps hackers guess your password by stepping through a dictionary containing thousands of the most commonly used passwords. 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.  
  
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 malware 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 e-mail attachments software downloads, and even files.  
  
Do not share your password with anyone. Avoid writing down a password. Memorise it. You should often change passwords. The more passwords and user IDs you have, the more difficult they become to remember. Your computer's operating system, Web browser, or other software might include a password manager to help you keep security of user IDs and passwords.

**Lesson 2**

Malware is any software designed to gain unauthorized access to the computing resources of the computer itself or to information stored on the computer.

There are a lot of types of malware nowadays, lets list some of them.

First of all it is virus. The main feature of computer virus that it is spread and replicated by itself. Virus also able to infect your PC.

The next one is Trojan horse. This malware is designed to seems to perform one task, but in fact perform other tasks.

Worm can be used to cause damage for big componies. It spread by network, infect it and replicate itself.

Bot is necessary to perform repetitive tasks, but it can be not a malware targeted.

Spyware. It is a program that aims to gather information about a person and send it to another entity in a way that harms the user.

Keylogger - a program that records every keystroke made by a computer user to gain fraudulent access to passwords.

Adware - software that displays unwanted pesky pop-up ads which can appear on your computer.

Ransomware - malware that prevents or limits users from accessing their system.

Rootkit - a program that masks its existence or the existence of other software.

There are many ways to get infected with malware.

The first way is through the mail. Malware authors often try to fraudulently download malicious files. This can be an email with an attached file, which is described as a delivery notification. If you are not sure that you know the sender, or something seems suspicious, do not open the letter.

The next popular way is through external media. Many malicious programs spread by infecting removable media, such as USB flash memory devices or external hard drives. Malware can be installed automatically when the infected media is connected to the computer. If you find a USB device that was lost do not connect it to a computer with important data. Sometimes attackers intentionally leave infected USB devices in public places, hoping that someone will find them and connect them to a computer.

Another way is to install malware along with other programs. Some malicious programs may be installed simultaneously with other downloaded programs. Such programs include software from third-party websites or files transmitted through peer-to-peer networks. By the way, programs for generating software keys (key generators) often install malware in parallel. To avoid installing malware or potentially unwanted programs Download the software only from the official website of its supplier.

And the last way is through websites. When trying to go to a website, it may try to exploit vulnerabilities in the web browser to infect the computer with malware. That is why it is very important to keep all the software, especially the web browser, up to date and remove the unused program.

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.

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.

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.

Information and Communication Technology (ICT) has created a virtual world with no boundaries and with people who engaged in the exploitation of the cyberspace for illegal activities. This virtual world is called "cyberspace". It can creates a lot of cyber threats for example espionage, theft of technology, financial frauds an so on. That’s why there are a lot of cyber weapons types nowadays. They can be classified into 4 pints. Precision that means the capability to target only a specific objective. Intrusion – level of penetration inside the target. Visibility – capability to remain undetected and ease of implementation that means resources are needed to develop a cyber weapon. All of this are needed to cause damage for hospitals, water supply, power grids and so on. Cyber weapon gets more and more attention for a bad reason. It is very attractive because it replays real weapon. It is less expensive and perform attack at the speed of light. The most dangerous effect is its unpredictable damage to other systems that are not considered targets.

**Lesson 3**

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.  
  
Phishing - This tactic includes deceptive emails to steal information.  
  
Pharming - It redirects Web site traffic to fraudulent Web sites that distribute malware, collect personal data, sell counterfeit products, and perpetrate other scams.  
  
Vishing – It is when someone calls you and represents him self as a bank worker