ENGLISH FOR INFORMATICS 2
BY
ATIQAH NURUL ASRI

MEETING #5

Topic: Computer Threats and Solutions

Material: Module Unit 3: Computer Security, page 27-32

Learning Outcomes:
By the end of the lesson, the students are expected to be able to use appropriate English to:
- identify and explain about computer threats and its prevention and solutions.
- identify and explain kinds of computer crimes.
- make analysis of a computer crime and present it to the class.

Look at the picture. Answer the following questions:

1. Have your computer or system ever been infected by a virus?
2. What did you do?
3. What should other users do to prevent their computer from virus attack?
4. What other security problems may happen to our computer or system?
5. What should we do to secure our computer or system?

Exercise 2: Read the descriptions 1-8. Match the words in the box to the descriptions.

adware	hacker	browser hijacker	malware attack
spyware	Trojan	virus	worm

1. _____ Malicious software that can copy itself and infect the system.
2. _____ A program which is usually free but contains malicious files.
3. _____ A program that automatically plays commercials on a computer.
4. _____ Affects privacy. It does not take control of a computer system, but sends information about the use of a computer system.
5. _____ An effort to gain unauthorized access to a computer.
6. _____ Spreads without the user taking action and usually acts in operation system.
7. _____ A person who on purpose attempts to break into a computer system and use it without the knowledge of the owner.
8. _____ Software that replaces the user's search engine with its own.

Exercise 3: Match the security, solution 1-5 to its purpose a-e.

Exercise 3: Match the security, solution 1-5 to its purpose a-e.

1. a firewall.
2. antivirus software.
3. authentication.
4. username, password, and biometric scanning.
5. encryption.

a. prevents damage that viruses might cause.
b. make sure only authorized people access the network.
c. checks the user is allowed to use system.
d. blocks unauthorized access codes.
e. protects the system from public places.

Exercise 4: You are going to listen to a dialog between Ludek and Ales, an IT expert. Ludek is having a problem with his laptop and ask for Ales' help. Listen it and answer the following questions.

1. Why does Ludek want Ales to check his laptop?
2. Why is Ludek worried that he may lose his project?
3. What does Ales think has happened to Ludek's laptop?
4. Why does he recommend Ludek installs an anti-spyware software?
5. Why is it important to have a network access password?
6. What will Ales do for Ludek?

Do you still remember what Ales told to Ludek about installing anti spyware software? Why did Ales suggest him to do so? Do you remember what type of criminals Ales mentioned?

Are you familiar with the crime? Tell us more about the crime.

What other crimes you know?

What should people do to prevent themselves from the criminals?

Exercise 5: Read the text about Internet Security, Malware: Viruses, Worms, Trojans, and Spyware and Preventative Tips carefully and then answer the questions

Internet Crime

The internet provides a wide variety of opportunities for communication and development, but unfortunately it also has its dark side.

Crackers, or **black-hat hackers**, are computer criminals who use technology to perform a variety of crimes: virus propagation, fraud, intellectual property theft, etc.

Internet-based crimes include **scam**, email fraud to obtain money or valuables, and **phishing**, **bank fraud**, to get banking information such as passwords of Internet bank accounts or credit cash details. Both crimes use emails or websites that look like those of real organizations.

Due to its anonymity, the Internet also provides the right environment for **cyberstalking**, for online **harassment** or **abuse**, mainly in chatrooms or newsgroups.

Piracy, the illegal copying and distribution of copyrighted software, information, music, and video files, is widespread.

But by far the most common type of crime involves **malware**.

Malware: viruses, worms, Trojans, and spyware

Malware (malicious software) is software created to damage or alter the computer data or its operations. These are the main types.

- **Viruses** are programs that spread by attaching themselves to executable files or documents. When the infected program is run, the virus propagates to other files or programs on the computer. Some viruses are designed to work at a particular time or on a specific date, e.g. on Friday 13th. An email virus spreads by sending a copy of itself to everyone in an email address book.
- **Worms** are self-copying programs that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks. Worms are self-contained and don't need to be attached to a document or program the way viruses do.
- **Trojan horse** are malicious programs disguised as innocent-looking files or embedded within legitimate software. Once they are activated, they may affect the computer in a variety of ways: some are just annoying, others are more ominous, creating a backdoor to the computer which can be used to collect stored data. They do not copy themselves or reproduce by infecting other files.
- **Spyware**, software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software. It usually comes hidden in fake freeware or shareware applications downloadable from the internet.

Preventative Tips:

- Do not open attachments from unknown people; always take note of the file extension.
- Run and update antivirus programs, e.g. virus scanners
- Install a firewall, a program designed to prevent spyware from gaining access to the internal network.
- Make backup copies of your files regularly.
- Do not accept files from high-risk sources.
- Use a digital certificate, an electronic way of proving your identity, when you are doing business on the internet. Avoid giving credit card numbers.
- Do not believe everything on the net. Have a suspicious attitude toward its contents.

Taken from Professional English in Use ICT pp.62

Identify the internet crimes sentences 1-6 refer to. Then match them with the advice (a-f).

1. Crackers try to find a way to copy the latest game or computer program.
2. A study has revealed that half a million people will automatically open an email they believe to be from their bank and happily send off all their security details.
3. This software's danger is hidden behind an attractive appearance. That's why it is often wrapped in attractive packages promising photos of celebrities like Anna Kournikova or Jennifer Lopez.
4. There is a particular danger in the internet commerce and emails. Many people believe they have been offered a special gift only to find out later they have been deceived.
5. 'Nimda' spreads by sending infected emails and is also able to infect websites, so when a user visits a compromised website, the browser can infect the computer.
6. Everyday, milions of children spend time in internet chat rooms talking to strangers. But what many of them do not realize is that some of the surfers chatting with them may be sexual predators.

a. People should not buy cracked software and download music illegally from the internet.
b. Be suspicious of wonderful offers. Don't buy if you aren't sure.
c. It's dangerous to give personal information to people you contact in chat rooms.
d. Don't open attachments from people you don't know even if the subject looks attractive.
e. Scan your email and be careful about websites you visit.
f. Check with your bank before sending information.

Exercise 6: Fill in the gaps in these security tips with words from the box

digital certificate	malware	virus	scanner	spyware	firewall	anti-virus

1. Malicious software _____ can be avoided by following some basic rules.
2. Internet users who like cybershopping should get a _____, an electronic identity card.
3. To prevent crackers from breaking into your internal network and obtaining your data, install a _____. It will protect you from _____.
4. If you have been hit by a _____ don't panic! Download a clen-up utility and always remember to use an _____ program, for example a virus _____.