Chapter 5: Internet Security

Topics discussed in this chapter:

- Security and privacy on the Internet
- Safety online for children
- The history of hacking
-Computer crimes

Course objectives

- To grasp the main concepts related to security and privacy on the Internet.
- To discuss controversial issues related to the Internet.

Language

-Grammar: The simple past.
-Vocabulary: Internet security, username, password, firewall, hacker, cracker, cookies, worm, Trojans, spyware, adware, digital certificate, encryption, filtering program, decryption, Internet crime, piracy, plagiarism, malware spreading, phishing, cyberstalking, IP spooying.

Skills

- Listening: In this part, you will learn to choose the most adequate answers to questions about an interview. You will also learn how to complete the interviewer's notes.
-Speaking: In this section, you will discuss Internet issues: computer crimes, personal privacy, infringement of copyright, censorship, etc..
-Reading: This part will help you understand general and specific information about Internet security and privacy on the Internet. It will also allow you to find specific information in a text about the history of hacking.
-Writing; In this section, you will summarize a discussion in a Powerpoint presentation if possible.

English Course, University of M'Sila

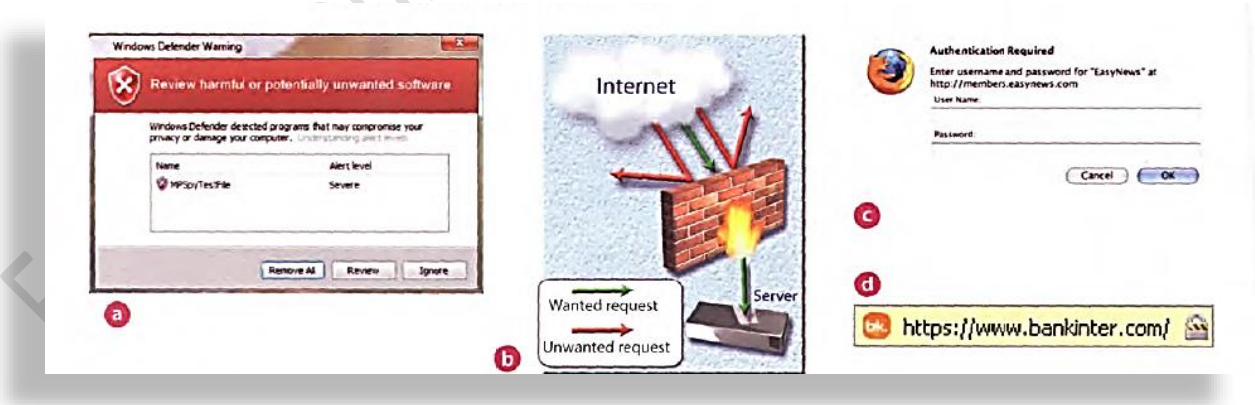
1. Warm up

A. Think about the following questions

1. What is a hacker?
2. How easy do you think is it to infiltrate the Internet and steal sensitive information?
3. What is a spyware?
4. How can you protect your computer from viruses and spyware?

B. Match the following captions (1-4) with the adequate pictures (a-d).

1. A secure website can be recognized in two ways; the address bar shows the letters *https* and a closed padlock or key is displayed at the bottom of the screen.
2. You have to type your username and password to access a locked computer system.
3. The program displays a message when it detects spyware and other unwanted software that may compromise your privacy or damage your computer.
4. Private networks use a software and/or hardware mechanism called a firewall to block unauthorized traffic from the Internet.



2 Security and privacy on the Internet

A. Read the text quickly and see how many of your ideas from 1A Question 3 are mentioned.

B. Read the text more carefully and answer the following questions.

1. Why is security so important on the internet?
2. What security features are offered by Mozilla Firefox?
3. What security protocol is used by banks to make online transactions secure?
4. How can we protect our email and keep it private?
5. What methods are used by companies to make internal networks secure?
6. In what ways can a virus enter a computer system?
7. How does a worm spread itself?

Security and privacy on the Internet

There are many benefits from an open system like the Internet, but one of the risks is that we are often exposed to **hackers**, who break into computer systems just for fun, to steal information, or to spread viruses (see note below). So how do we go about making our online transactions secure?

Security on the Web

Security is crucial when you send confidential information online. Consider, for example, the process of buying a book on the Web. You have to type your credit card number into an order form which passes from computer to computer on its way to the online bookstore. If one of the intermediary computers is infiltrated by hackers, your data can be copied.

To avoid risks, you should set all security alerts to high on your web browser. Mozilla Firefox displays a lock when the website is secure and allows you to disable or delete **cookies** – small files placed on your hard drive by web servers so that they can recognize your PC when you return to their site.

If you use online banking services, make sure they use **digital certificates** – files that are like digital identification cards and that identify users and web servers. Also be sure to use a browser that is compliant with **SSL** (**S**ecure **S**ockets **L**ayer), a protocol which provides secure transactions.

Email privacy

Similarly, as your email travels across the Net, it is copied temporarily onto many computers in between. This means that it can be read by people who illegally enter computer systems.

The only way to protect a message is to put it in a sort of virtual envelope – that is, to encode it with some form of **encryption.** A system designed to send email privately is Pretty Good Privacy, a **freeware** program written by Phil Zimmerman.

Network security

Private networks can be attacked by intruders who attempt to obtain information such as Social Security numbers, bank accounts or research and business reports. To protect crucial data, companies hire security consultants who analyse the risks and provide solutions. The most common methods of protection are **passwords** for access control, **firewalls**, and **encryption** and **decryption** systems. Encryption changes data into a secret code so that only someone with a key can read it. Decryption converts encrypted data back into its original form.

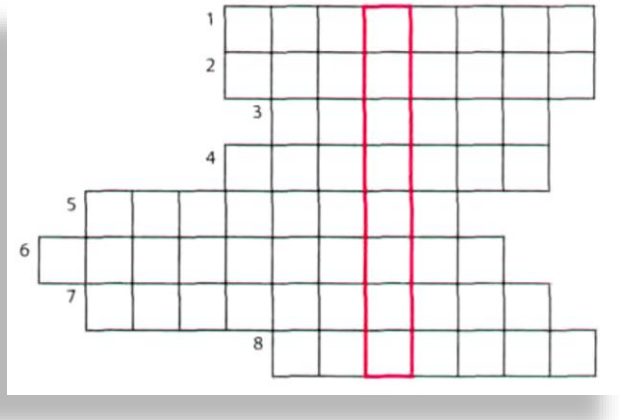
Malware protection

Malware (malicious software) are programs designed to infiltrate or damage your computer, for example **viruses**, **worms**, **Trojans** and **spyware**. A virus can enter a PC via a disc drive – if you insert an infected disc – or via the Internet. A worm is a self-copying program that spreads through email attachments; it replicates itself and sends a copy to everyone in an address book. A Trojan horse is disguised as a useful program; it may affect data security. Spyware collects information from your PC without your consent. Most spyware and adware (software that allows pop-ups – that is, advertisements that suddenly appear on your screen) is included with 'free' downloads.

If you want to protect your PC, don't open email attachments from strangers and take care when downloading files from the Web. Remember to update your **anti-virus software** as often as possible, since new viruses are being created all the time.

Note: Originally, all computer enthusiasts and skilled programmers were known as **hackers**, but during the 1990s, the term hacker became synonymous with **cracker** – a person who uses technology for criminal aims. Nowadays, people often use the word hacker to mean both things. In the computer industry, hackers are known as *white hats* and crackers are called *black hats* or *darkside hackers*.

C. Solve the clues and complete the following puzzle.



1. Users have to enter a…….to gain access to a network.
2. A……protects a company intranet from outside attacks.
3. A…….is a person who uses their computer skills to enter computers and networks illegally.
4. …….can infect your files and corrupt your hard drive.
5. You can download…….from the Net; this type of software is available free of charge but protected by copyright.
6. Encoding data so that unauthorized users can't read it is known as….
7. This company uses …….the techniques to decode (or decipher) secret data.
8. Most…….is designed to obtain personal information without the user's permission.

3 Safety onlinefor children

A. Listen to an interview with Diana Wilson, a member of the Internet Foundation. Which answers (a or b) best describe what she says?

1. Parents should make children aware of
   a. The benefits and risks of the Internet. b. the risks of the Internet.
2. A Web filter program can be used to
   a. Prevent access to the sites with inappropriate content
   b. Rate Web content with labels similar to the way movies are rated)
3. If kids spend too much time online or suffer from Internet addiction, parents should
   a. Stop them using the Internet
   b. b. Look for help from specialists.

English Course, University of M'Sila

B. Listen again and complete the interview

Risks	Solutions
Manipulation of children	There are websites (4) _____ at children.
Invasions of (1) _____	Internet (5) _____ programs let parents block objectionable websites.
Distribution of indecent or (2) _____ material	Websites should (6) _____ their content with a label, from child-friendly to over18 only.
Violence and racist (3) _____	

4 The history of hacking

A. Read Part 1 of the text and answer these questions:

1. Which hacking case inspired the film *War Games*?
2. When did *Captan Zap* hack into the Pentagon?
3. Why was Nicholas Whitely arrested in 1988?
4. How old was the hacker that broke into the U.S. defence computer in 1989?

The history of hacking – Part 1

1971 – John Draper discovered that a whistle offered in boxes of Cap'n Crunch breakfast cereal perfectly generated the 2,600Hz signal used by the AT&T phone company. He started to make free calls. He was arrested in 1972 but wasn't sent to prison.

1974 – Kevin Mitnick, a legend among hackers, began hacking into banking networks and altering the credit reports of his enemies. He didn't expect that his most famous exploit – hacking into the North American Defense Command in Colorado Springs – would inspire the film *War Games* in 1983.

1981 – Ian Murphy, a 23-year-old known as *Captain Zap* on the networks, hacked into the White House and the Pentagon.

1987 – The IBM international network was paralysed by a hacker's Christmas message.

1988 – The Union Bank of Switzerland almost lost £32 million to hackers. Nicholas Whitely was arrested in connection with virus spreading.

1989 – A fifteen-year-old hacker cracked the US defence computer.

1991 – Kevin Poulsen, known as *Dark Dante* on the networks, was accused of stealing military files.

B. Discuss which of the cases in Part 1 you had heard of. Which do you think is the most important?

5. Language work: the past simple

A. Look at the HELP box and then complete Part 2 of the text with the past simple form of the following verbs .

Show spread steal launch attempt overwrite be infect affect

The history of hacking – Part 2

1992 – David L Smith (1) _____ prosecuted for writing the Melissa virus, which was passed in Word files sent via email.

1997 – The German Chaos Computer Club (2) _____ on TV how to obtain money from bank accounts.

2000 – A Russian hacker (3) _____ to extort $100,000 from online music retailer CD Universe.

A Canadian hacker (4) _____ a massive *denial of service* attack against websites like Yahoo! and Amazon.

The *ILoveYou* virus, cleverly disguised as a love letter, (5) _____ so quickly that email had to be shut down in many companies. The worm (6) _____ image and sound files with a copy of itself.

2001 – The *Code Red* worm (7) _____ tens of thousands of machines.

2006 – Hackers (8) _____ the credit card details of almost 20,000 AT&T online customers. However, subscribers to its service (9) (not) _____ .

HELP box

Past simple

- We use the past simple to talk about a complete action or event which happened at a specific time in the past.

  Past ——————|—————— Now
  *He **began** hacking in 1974.*

- We form the past simple of regular verbs by adding **-(e)d** to the infinitive.

  *John Draper **discovered** that a whistle …*

  We form questions and negatives using **did/didn't**.

  *When **did** Captain Zap **hack** into the Pentagon?*
  *He **didn't expect** that his most famous exploit …*

- There are many verbs which are irregular in the past simple.

  *Kevin Mitnick **began** hacking into …*

  For a list of irregular verbs, see page 166.

  We form questions and negatives for irregular verbs in the same way as for regular verbs. The exception is **be** (see below).

  *When **did** Kevin Mitnick **begin** hacking into …?*
  *He **didn't begin** hacking until 1974.*

- We form the past passive with the past simple of **be** + the past participle.

  *IBM international **was paralysed** by hackers.*
  *He **wasn't sent** to prison.*
  *Why **was** Nicholas Whitely **arrested** in 1998?*

B. Read these landmarks in the history of the Internet and prepare at least five questions in the past simple.

Example: What happened in 1960? What did Ray Tomlinson do in 1971?

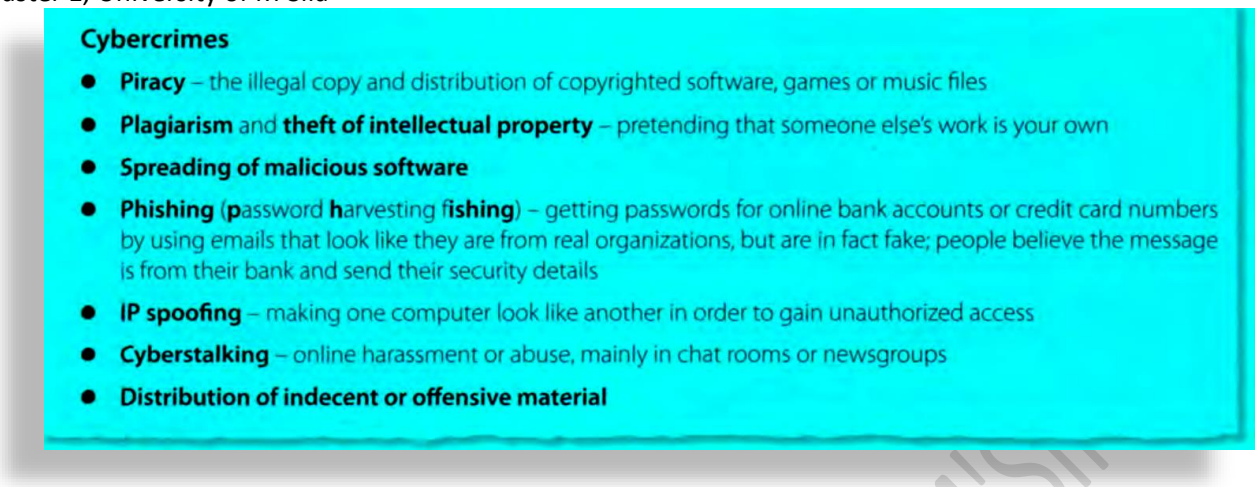
1969 – The US Defense Department establishes ARPANET, a network connecting research centres.
1971 – Ray Tomlinson of BBN invents an email program to send messages across a network. The @ sign is chosen for its *at* meaning.
1981 – IBM sells the first IBM PC. BITNET provides email and file transfers to universities.
1982 – TCP/IP is adopted as the standard language of the Internet.
1988 – Jarkko Oikarinen develops the system known as Internet Relay Chat (IRC).
1991 – CERN (*Conseil Européen pour la Recherche Nucléaire*) creates the World Wide Web.
1998 – The Internet 2 network is born. It can handle data and video at high speed but is not a public network.
1999 – Online banking, e-commerce and MP3 music become popular.
2001 – Napster, whose software allows users to share downloaded music, maintains that it does not perpetrate or encourage music piracy. However, a judge rules that Napster's technology is an infringement of music copyright.
2004 – Network Solutions begins offering 100-year domain registration.
2006 – Americans spend over $100 billion shopping online.

6. Internet Issues

A. Look at the list of cybercrimes and discuss think about these questions

1. Which crimes are the most dangerous?
2. Is it fair or unfair to pay the songs, fideos, books ornarticles that you download? Should copyright infringement be allowed online?
3. What measures can be taken by governments to stop cybercrime?
4. Do you think governments have the right to censor material on the Internet?
5. Personal information such as our address, safety, and civil and criminal records is held in databases by marketing companies. Is our privacy in danger?

English Course, Universi



Cybercrimes

- **Piracy** – the illegal copy and distribution of copyrighted software, games or music files
- **Plagiarism** and **theft of intellectual property** – pretending that someone else's work is your own
- **Spreading of malicious software**
- **Phishing** (**p**assword **h**arvesting f**ishing**) – getting passwords for online bank accounts or credit card numbers by using emails that look like they are from real organizations, but are in fact fake; people believe the message is from their bank and send their security details
- **IP spoofing** – making one computer look like another in order to gain unauthorized access
- **Cyberstalking** – online harassment or abuse, mainly in chat rooms or newsgroups
- **Distribution of indecent or offensive material**

B. Write a summary of your discussion on PowerPoint presentation.

English Course, University of M'Sila