15 Internet crime and Data Security

Topic

Security and privacy on the Internet, computer crimes

Learning objectives

Students will be able:

- To explain why security is important
- To understand the basic ideas related to security and privacy on the Internet
- To name threats to the systems and applications software
- To define various types of malware
- To list precautions against spreading malware
- To acquire vocabulary related to computer crimes

Key words

firewall, hacker, cracker, cookies, virus, worm, Trojans, spyware, adware, digital certificate, encryption, decryption, Internet crime, piracy, plagiarism, malware, cyberstalking, IP spoofing, phishing, virus scanner, antivirus program

Internet crime

Despite many benefits the Internet brings some risks. One of them are the **hackers**, people who break into computer systems just for fun, to steal information or to spread viruses.

Crackers are computer criminals who commit a variety of crimes – virus propagation, fraud, intellectual property theft, etc.

Scam is a kind of email fraud to obtain money.

Phishing (password harvesting fishing) – getting password for an online bank account or a credit card number by using emails which look as if they were from a real organization. In fact they are fakes but people often send their security details because they believe that the email is from their bank. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

Piracy – the unauthorized copying of software. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues or even sell them.

Plagiarism and **theft of intellectual property** – pretending that someone else´s work is your own.

Spreading of malicious software means distributing programs that can reproduce themselves and are written with the purpose of causing damage or causing the computer to behave in an unusual way.

IP spoofing – making a computer look like another in order to gain unauthorised access.

Cyberstalking – a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyberstalker targets a specific victim with often threatening messages.

Distribution of indecent or offensive material

The most common type of crime involves **malware**

Malware

means malicious software – software created to damage or alter data.

Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you better protect your computer from their often damaging effects.

- **A computer virus** attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but **it actually cannot infect your computer unless you run or open the malicious program**. It is important to note that a **virus cannot be spread without a human action,** for example by sharing infecting files or sending emails with viruses as attachments in the email.
- **A worm** is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the **capability to travel without any human action**. The biggest danger with a worm is its capability to replicate itself on your system. One example would be a worm sending a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, etc. Due to the copying nature of a worm and its

capability to travel across networks the end result in most cases is that the worm consumes too much system memory, causing Web servers, network servers and individual computers to stop responding.

- **A Trojan Horse** at first glance appears to be useful software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans neither reproduce by infecting other files nor self-replicate.
- **A blended threat** is a more sophisticated attack that combines some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat.
- **Spyware** is software designed to collect information for commercial or criminal purposes. It usually comes hidden in fake freeware or shareware applications downloaded from the Internet. It can gather information about e-mail addresses and even passwords and credit card numbers. Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another recipient.

Security measures

There is a variety of security measures which can be used to protect both hardware and software.

1. **Controlling physical access** to hardware and software.
2. **Backing up** data and programs regularly
3. **Implementing network controls,** for example
    - Using **passwords** to control access to a network system.
    - Installing a **firewall** - a system that controls data going into and out of a network which prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. For individual home users, the most popular firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access to your computer, and usually provides additional protection against the most common Trojan programs or e-

mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network.
    - **Encrypting data** – putting data to a form that only authorised users can understand.
    - Using **signature verification** or **biometric authentication** (a fingerprint reader or an eye scanner).
4. Protecting against natural disasters by installing **uninterruptible power supplies** (battery backup systems providing power to a computer when the normal electricity source fails) and **surge protection** (electronic devices protecting the equipment from damage in case of a sudden surge in a power supply).
5. Protecting against viruses by using **antivirus programs** – programs able to detect, identify and remove viruses from a computer system – and downloading updates frequently to ensure your software has the latest fixes for new viruses, worms, and Trojan horses. Make sure your anti-virus program has the capability to scan e-mail and files as they are downloaded from the Internet.
6. Ensuring that all **software** is **free of viruses before it is installed**. Particular care should be taken when using free software and shareware (software that is free to try out but must be paid for when it is used after the trial period.

Vocabulary

	Definition	**Translation**
adware	software devised to display advertisement, can include spyware	adware
authentication	verifying the identity of a user logging onto a network	ověření, potvrzení pravosti
biometric authentication	identification based on physical features - fingerprints, voice scan, etc.	biometrické ověření
cookies	small files used by web servers to know if you have visited their site	cookies
cracker	someone who breaks into the PC system to steal data, propagate a virus, etc.	cracker
cyberstalking	online harassment or abuse, mainly in chat rooms	stalking, obtěžování přes internet
decryption	the process of decoding secret data	dekódování
digital certificate	a file that identifies the user or a web server	digitální certifikát
encryption	the process of saving and transmitting data in encoded form	kódování, šifrování

firewall	a software or hardware device that allows limited access to an internal network from the Net	firewall
fraud	something intended to deceive	podvod
hacker	someone who invades a privacy of a network	hacker
Internet crime	crimes perpetrated over the Net	internetová kriminalita
IP spoofing	making a computer look like another one to gain unauthorized access	
malware	malicious software created to damage computer data	zákeřný software
password	a secret word which must be entered before access is given	heslo
phishing	getting passwords of online bank accounts or credit card numbers using fake emails	podvodné online vylákání a zneužití osobních údajů
piracy	the illegal copying and distribution of copyrighted programs and files	pirátství
plagiarism	pretending that someone else´s work is your own.	plagiátorství
spyware	software that collects information from your PC without your consent	spyware
Trojan	malicious software disguised as a useful program	trojský kůň
username	the name you identify yourself when you log onto a computer system or a network	uživatelské jméno
virus	a piece of software which attaches itself to a file and spreads to the system files	virus
virus scanner	a type of antivirus program that searches a system for virus signatures	
worm	a self-copying program that replicates itself and spreads through email	worm, druh viru

Summary

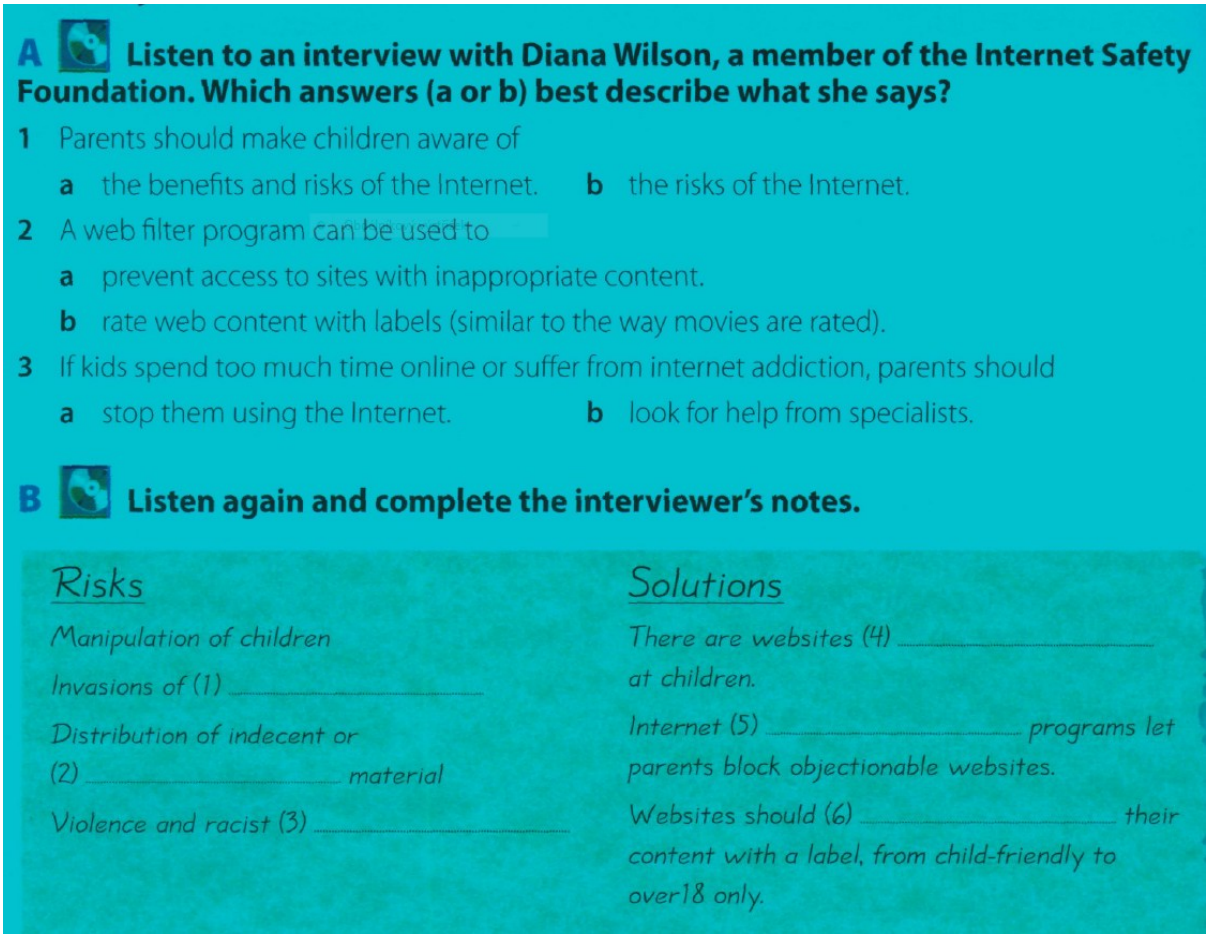
Despite many benefits the Internet brings some risks, for example phishing, piracy, plagiarism, spreading malicious software, cyberstalking, spreading offensive material, etc.

The most common type of crime involves malware (malicious software) – viruses, worms and Trojan Horses.

There is a variety of security measures which can be used to protect both hardware and software, for example: Controlling physical access to hardware and software, backing up data and programs, using passwords to control access to a network system, installing a firewall, encrypting data, using signature verification or biometric authentication, using antivirus programs and downloading updates, ensuring that all software is free of viruses before it is installed.

Tasks and Questions

1. **Listening: Infotech p. 96**



A **Listen to an interview with Diana Wilson, a member of the Internet Safety 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 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** look for help from specialists.

B **Listen again and complete the interviewer's notes.**

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) _____	

2. **Complete this product description of an internet security program. Type in the missing words using the mixed-up letters in brackets.**

EFG (1)_____ [inta-riuvs] software is the only program you need for complete protection from online threats.

EFG scans all incoming and outgoing email attachments, helping to protect your PC against (2) _____ [rivessu] , (3) _____ [romsw] , (4) _____ [Torsjan] and other types of (5))_____ [lawmare] . A (6) _____ [lawlrife] shields your system from attack by (7) _____ [reschak] , while the program can also detect if a website's (8) _____ [igidlat ercteacfiti] is out-of-date or suspicious, allowing you to carry out financial transactions online with total security.

In addition to all of the above, the EFG Professional Edition also comes with email (9) _____ [crynetipon] and the EFG (10)_____ [rawsyep] scanner, helping you to keep your system free of unwanted advertising and (11) _____ [socoiek] .

EFG Basic is available to download as (12)_____ [warfeeer] by clicking here. Alternatively, you can purchase the EFG Professional Edition for only £29.95. Click here to visit our (13) _____ [rescue witebes] or pay using PayPal by clicking here.

3. Decide what kind of cybercrime is described.

1 In July 2001, the online file-sharing network *Napster* shut its website following legal action from several major record labels.

2 In late 2006, a computer worm took control of hundreds of pages on MySpace and changed links to direct surfers to websites designed to steal their login details.

3 The first well-known worm was the *Internet Worm* of 1988, which infected SunOS and VAX BSD systems.

4 A 2007 study found that 28% of female internet users had experienced online harassment. In 84% of cases, the incidents happened in a chat room.

5 In 2008, author J K Rowling said that a company trying to publish an online Harry Potter encyclopaedia had 'stolen her words'.

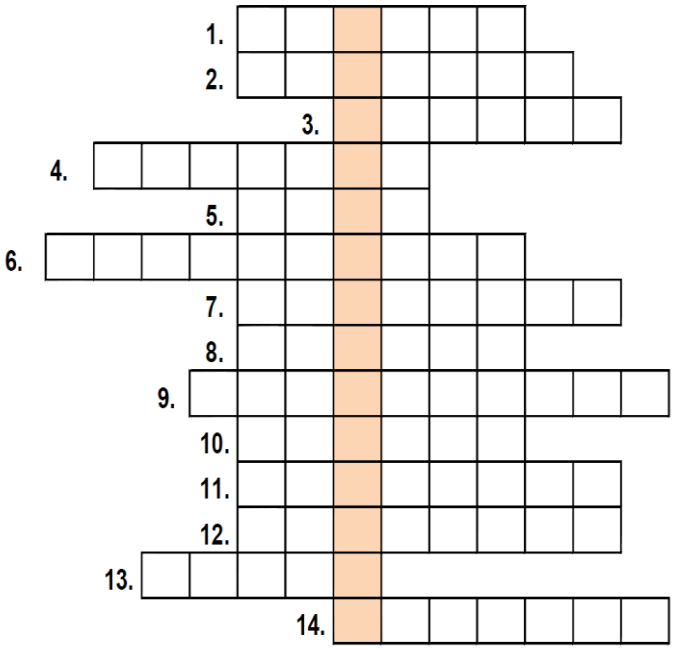
http://www.cambridge.org/servlet/file/store7/item620178/version1/Infotech4ed_WS_U19InternetSecurity.pdf

4. Match the word with its definition.

1. Phishing	a) pretending that someone else´s work is your own
2. Plagiarism	b) a kind of malware which cannot be spread without a human action
3. Cyberstalking	c) a kind of malware which has the capability to spread without any human action
4. Spyware	d) getting security details of online bank accounts using fake emails
5. Piracy	e) someone who invades a privacy of a network just for fun
6. Worm	f) someone who invades computers for criminal purposes
7. Hacker	g) online harassment or abuse
8. Cracker	h) the unauthorized copying of software
9. Virus	i) a software or hardware device that allows limited access to an internal network from the Net
10. Firewall	j) software that collects information from your PC without your consent

11. Complete the puzzle: solution = another dangerous type of Internet crime

1. someone who invades a network for fun
2. software that collects information from your PC without your consent
3. to make a copy of the data in case the original data is lost or damaged
4. someone who breaks into the PC for criminal aims
5. a self-copying program that replicates itself
6. saving and transmitting data in encoded form
7. the name you identify yourself when you log onto a network
8. the illegal copying and distribution of copyrighted programs
9. decoding secret data
10. malicious software disguised as a useful program
11. software or hardware protecting a computer network from intruders
12. getting passwords or credit card numbers using fake emails
13. a piece of software which attaches itself to a file and spreads
14. malicious software created to damage computer data



5) In groups discuss the following issues:

- What type of cybercrime do you consider to be the most dangerous and why?
- Downloading songs films and copyright infringement; government measures to stop it
- Privacy on the Internet
- Social networks and security
- Censorship on the Internet

6) Writing: A magazine article

Write a short article to a magazine in which you give advice on how to prevent from Internet crime.

*Use **imperatives***
***Never** open….*

*Use **should / shouldn´t** + infinitive*
*You **should install** the …*
*You **shouldn´t open** …*
It is a good idea to…

Questions

1. What is the difference between a hacker and a cracker?
2. What is phishing?

3. What is piracy?
4. What is plagiarism?
5. What is cyberstalking?
6. What is malware? Give examples.
7. Name as many types of Internet crime as possible.
8. What is the difference between a worm and a virus?
9. What is a Trojan horse?
10. What is spyware?
11. How can you prevent from Internet crime – give examples.
12. What is a firewall?
13. What is a password?
14. What is encrypting and decrypting?
15. What is biometric authentication?
16. What is an antivirus program?

Literatura