

Unit 28	Communication	Vocabulary	Grammar
<i>Is your computer secure?</i>	<i>Discussing different Internet security issues Talking about hackers and their role in Internet security</i>	<i>Types of malware Hacking terms Collocations with the word cyber</i>	<i>conditional sentences</i>

Learning objectives:

- *Learning about the basic ideas related to security and privacy on the internet*
- *Discussing different Internet security issues*
- *Talking about hackers and their role in Internet security*
- *Identifying different types of malware*
- *Learning and using collocations with the word cyber*
- *Revising conditional sentences*

Unit 28

Is Your Computer Secure?

I Warm-up

A Label the pictures using the phrases in the box

Natural disasters	Disgruntled employees	Viruses and bugs
Hackers	Wire tappers, eavesdroppers	



BChoose the best words to go into each of the spaces.

1. A person who illegally accesses somebody else's computer over the internet is called a _____.
a. pirate b. hack c. hacker
2. A website which (in theory) cannot be accessed by a hacker is _____.
a. strong b. secure c. clean
3. A website which can only be viewed by authorised people has _____ access.
a. reduced b. small c. restricted
4. Unwanted advertising emails are popularly known as _____.
a. meatloaf b. spam c. sausages
5. Software which blocks attempts by others to access your computer over the internet is called a _____.
a. firewall b. fire blanket c. fire engine
6. It's essential to _____ your anti-virus protection regularly.
a. up-to-date b. date c. update
7. Anti-virus software can _____ your computer for viruses.
a. detect b. review c. scan
8. Anti-virus software can also _____ viruses on removable media, such as floppy disks.
a. detect b. control c. see
9. When your anti-virus software subscription _____...
a. ends b. stops c. expires
10. ... it's a good idea to _____ it immediately.
a. renew b. renovate c. replace

C Match the malware with the damage. (It's not easy, and the terms are sometimes confused with each other.)

1. virus	a. collects and sends private information from the infected computer to a third party
2. spyware	b. an undesirable program which can replicate itself across a network
3. trojan horse	c. allows a hacker to access private information when he/she wishes
4. keystroke logger or keylogger	d. a program which adds itself to an executable file, and can cause considerable damage to the data on the infected computer
5. worm	e. records characters that are typed into a computer

Computer crimes range from a disgruntled employee who sabotages his former company to a company that hacks into a competitor's computer to steal trade secrets.

Computer security has not kept up with the rapid growth of the computer industry. With more people and more computers, the security problem becomes complex.

B Try to answer these questions:

1. Who are 'hackers'? Brave guys beating the system or computer criminals?
2. What are some common motivations for computer crime?
3. How serious can computer crime be? Have you heard of any incidents of computer crime?

II Reading

A Match the following headlines with the news reports given below.

"Robin Hoods" who cost Microsoft millions go to jail

Hackers score big by thinking small

MAINE MAN SENTENCED TO 6 YEARS FOR EBAY SCAM

Data theft involving four banks could affect 500,000 customers

Electronic account records for some 500,000 banking customers at four different banks were allegedly stolen and sold to collection agencies in a data-theft case that has so far led to criminal charges against nine people, including seven former bank employees.

Police are continuing their investigation into the theft by a crime ring that apparently accessed the data illegally through the former bank employees. The ring had operated for more than four years, with profits reaching several million dollars, the police said.

(Reuters) – A recent computer security breach that left 40 million credit cards vulnerable to fraud shows how online criminals are scoring big by thinking small. Cybercriminals are increasingly crafting more focused attack with a potential for profit as they target one or two companies at a time, rather than blasting out Internet virus attacks across the globe. The payoffs can be enormous. MasterCard International Inc. said that an outsider gained access to as many as 40 million credit and debit cards from a payment processor, having placed a malicious computer script. Targeted attacks have the advantage of being small enough to stay off the radar of Internet security firms that are looking for broader attacks, giving the high-tech criminals the time to research a company thoroughly before trying to penetrate it.

Attackers can then send individual, personalized e-mails to the target company's employees, or pose as IT administrators who need to install a software update. Once in, they can use simple spyware programs to pick up passwords, account numbers and other valuable information.

Three Britons were jailed Friday for being part of a global gang described as "Robin Hoods" who stole expensive software from rich companies and gave it away for free over the Internet.

The group were said to have cost firms such as Microsoft Corp. millions of dollars in profit and enraged its chairman, Bill Gates.

Prosecutors said that these men, motivated by a hatred of software companies, were the key players in international ring called DrinkorDie.com. The gang allowed Internet surfers to download new software for free – often before it came on the market – and made available the Windows 95 OS two weeks before it was released. The group cracked security codes for Norton AntiVirus, Microsoft's word and Excel products and pirated games and design programs.

"They think themselves like latter-day Robin Hoods or sea pirates like Johnny Depp in the film *Pirates of the Caribbean*", said prosecuting lawyer, but, in fact, the gang – which included corporate executives, university administrators and IT managers – were just "plain thieves".

A 21-year-old man was sentenced in U.S. District Court in Maine to more than six years in prison for perpetrating an extensive Internet fraud scheme. Charles Stergios was ordered to pay nearly \$118,000 in restitution to his victims.

Between April 2003 and January 2004, Stergios tried to fraudulently buy and sell merchandise over the Internet through online auction Web site eBay. Stergios engaged in the fraudulent transaction with at least 321 victims. He tried to trick his victims out of around \$420,000 but the actual loss was closer to \$120,000, because some of the transactions weren't completed. In these transactions, Stergios would obtain either valuable merchandise for which he did not pay full value, or he would accept personal or bank checks, or money orders for merchandise that he did not deliver. In addition, he would bid on items such as jewelry, watches and computers, accept delivery of the merchandise, and then pay with a check from a nonexistent account.

III Speaking

III Discussion questions

1. What sort of problems may be caused by hackers and electronic pickpockets? (Refer to the texts for help)
2. What measures should be taken against hacking?
3. How serious do you think the Maine man's crime was?
4. Do you think his punishment was:
 - a. too severe?
 - b. about right?
 - c. not severe enough?
5. Have you heard of any similar incidents of computer hacking?
6. Do you believe the motivation for hacking can be a better understanding of the cyberspace, gaining knowledge, or the thrill of adventure?
7. Can you find parallels between hacking and burglary?
8. Does computer crime sometimes invoke admiring attitudes from the public? Why do stories about computer crime fascinate the general public?
9. Can hacking lead to the improvement of computing and security standards?

IV Word study

A Fill in the blanks with the words from the box

cops crime sitter crooks space phobia

1. The reluctance to report cyber ---- makes it hard to tell how widespread it is, or how much it costs companies.
2. Two years ago, the FBI New York field office set up Criminal Squad 37 — C-37 for short, whose agents are cyber----. They work in cyber---- trying to track cyber----.
3. Cyber---- is a program parents may use to censor the Internet, i.e. restrict what comes in.
4. Cyber----- is fear of computers.

B Fill in the blanks using a word from the list given below.

Security

1. Computer security refers (1)_____ the techniques developed to (2)_____ single computers and network-linked (3)_____ systems from accidental or (4)_____ harm. Such harm includes (5)_____ of computer hardware and (6)_____, physical loss of data, (7)_____ the deliberate invasion of (8)_____ by unauthorized individuals.

These are the words to choose from:

destruction databases protect to
software intentional and computer

2. A password is (1)_____ security measure used to (2)_____ access to computer systems (3)_____ sensitive files. A password (4)_____ a unique string of characters (5)_____ a user types in (6)_____ identification code. The (7)_____ compares the code against (8)_____ stored list of authorized (9)_____ and users. If the (10)_____ is legitimate, the system (11)_____ the user access, at (12)_____ security level has been (13)_____ for the owner of (14)_____ password.

These are the words to choose from:

as and a restrict approved code whatever
is a system allows that the passwords

C Match the clauses in Column A with the clauses in Column B to make logical sentences.

Column A

Column B

If you want to store more information	buy a laptop
If you want to send faxes from your PC	get a bigger hard disk
If you want to stop the computer when it hangs	fit a modem
If you want to make music on your PC	fit a sound card
If you want to take your work away with you hit Control, Alt & Delete	
If you want to protect your data	make a backup

D Working with a partner, write sentences giving advice about computers.

If you want to fight off nasty viruses, e-mail worms, or Trojan horses, you should - shouldn't

- *Keep your antivirus software updated to keep up with new viruses as they emerge*

- *Open cool looking file attachments from persons unknown*
- *Stop spyware and pop-ups*
- *Keep your OS patched*
- *Make a rescue disk*
- *Back up your data files at least weekly*
- *Get a good Internet security suite, combining antivirus, firewall, blockers, spam fighting and other useful apps.*

V Grammar

Conditionals

A Read the following sentences, identify which type each belongs to and supply the correct form of the verbs in brackets.

1. It will not be easy to get through the rest of your life if you (not know) anything about computers.
2. Computers can deal with different kinds of problems if they (be given) the right instructions.
3. If I hadn't been careless, I (not delete) some important files.
4. If you (not install) an antivirus program, a virus may invade your boot sector and destroy your files.
5. If the price of palmtop computers drops next year, I definitely (buy) one.
6. If I knew C++, I (get) a better job.
7. If we (have) access to the Web, we could look up certain information.
8. John: " Your computer is years out of date. Why don't you get rid of it?
Sarah: " Don't be ridiculous! If I (get) rid of it, I (have) to invest \$1000 to buy a new one.
9. If you (want) to gain the maximum use of a PC, you should consider its upgradability.
10. If you intend to run Windows applications, even (not think) of buying a PC with less than 32 MB of RAM.
11. If he had followed his friends' advice, and installed proper software, he (not end) up as Typhoid Mary sending e-mails to everyone in his address book.

12. If you had installed the patch , the Slammer worm (not exploit) the security flaw in your software.

13. If I had made regular backups, I (not suffer) major damage after the latest hacker attack.

14. If you believed every phony warning, you (delete) harmless files as well.??

B Rewrite the following sentences using if.

1. I was careless, so I deleted some important files.

2. I was late for the interview; perhaps that's why they didn't offer me the job.

3. I didn't activate the virus protection program. A virus invaded my boot sector and caused great damage.

4. We didn't buy state-of-the-art equipment, so we couldn't run the latest application programs.

CTranslate the following sentences into English.

1. Da nisu odmah uočili grešku, šteta bi bila ogromna.

2. Ako padne sistem, pozovite dežurnog programera.

3. Da nisam nadgradio opremu, ne bih mogao da koristim nove programe.

4. Ako ne znaš kako da koiristiš računar, možeš slučajno da obrišeš sve fajlove.

5. Kad bismo proširili memoriju, mogli bismo da obradjujemo podatke mnogo brže.

6. Ako želiš da naučiš sve o programiranju, upiši kurs.

7. Ako unaprediš sistem, moći ćeš da radiš sa najnovijim aplikacijama.

8. Kad bi marketing menadžer imao dobar multimedijalni sistem, mogao bi da pripremi efektnije prezentacije.