Internet safety

Warm up

1. Discuss the quote: "A hacker to me is someone creative who doe s wonderful things" - Tim Berners-Lee.
2. Has your computer ever been infected by malicious software? If so, which and how did you get rid of it?
3. Which types of malware are most dangerous? Why?

Reading

As more and more technology is integrated into everyday life, it is necessary to be aware of many negative effects of the Internet that can cause personal and professional harm, and may be leading to an erosion of morals, ethics, and basic principles. The Internet's vast reach, constantly changing technologies, and growing social nature have made users vulnerable to identity theft including scam (email fraud to obtain money or valuables), plagiarism (theft of intellectual property), privacy violations, such cyberbullying (including slander or libel) addiction (involving online gambling, gaming and shopping, and compulsive surfing on the Web), sexual exploitation (including child pornography) and lack of face-to-face communication.

The Internet also exerts negative effects on business. Piracy, the illegal copying and distribution of copyrighted software, information, music and video files, is widespread. The popularity of file swapping networks, where people are able to illegally download music and films onto their home computers for free, has caused sales of music CDs to drop.

Crackers, or black-hat hackers, are computer criminals who use technology to perform a variety of internet-based crimes. The most common type of crime involves malware.

1. What are some examples of online risks mentioned in the passage, and how do they affect users?
2. What negative effects does the Internet have on businesses, according to the passage?
3. How does piracy and illegal file sharing affect industries such as music and film?
4. Who are crackers, and what types of crimes do they commit?

Malware

Malware (short for malicious software) is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software. It is software created by crackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware includes computer viruses, spyware, worms, Trojan horses, adware, phishing, pharming, and most rootkits.

1. **Match these different types of malware (A - K) with the descriptions (1 -11)**

a) Clickjacking	1. A self-replicating program that adds itself to an executable file. It is designed to infect a computer by rapidly spreading from one file to another and causing great harm to the data

			on the infected computer
b)	Worm	2.	A standalone malware computer program that replicates itself in order to spread to other computers using a computer network relying on security failures. Unlike a virus, it does not need to attach itself to an existing program.
c)	Pharming	3.	monitors a user's location and aims to gather information about a person or organization without their knowledge and may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge
d)	Spyware	4.	a type of malware containing malicious code that, when executed, carries out actions typically causing loss or theft of data, and possible system harm. It tricks the user into allowing the program access to their computer, usually through a download or email attachment.
e)	Mousetrapping	5.	a form of malware that presents unwanted advertisements to the user of a compute
f)	Phishing	6.	attempting to acquire information, such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Such e-mails may contain links to websites that are infected with malware.
g)	Adware	7.	A technique used to redirect a legitimate website's traffic to another illegitimate website in order to gain access to a user's banking information such as passwords of Internet bank accounts or credit card details. It has become of major concern to businesses hosting e-commerce and online banking websites.
h)	Rootkit	8.	Software used by a hacker to gain constant administrator-level access to a computer or network. It is typically installed through a stolen password or by exploiting system vulnerabilities without the victim's consent or knowledge. It is activated each time the victim's system boots up
i)	Trojan horse	9.	occurs when malware or spyware replaces your browser's home page with its own in order to force more hits to a particular website.
j)	Browser hijacking	10.	A technique that tricks users into clicking on a malicious link by adding the link to a transparent layer over what appears to be a legitimate web page.
k)	Virus	11.	keeps visitors from leaving a website by locking them into a window, opening multiple windows on the desktop, or re-launching their website in a window that cannot be closed.

2. Identify the Internet crimes the sentences 1- 6 refer to. Then match them with the advice A - F below.

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 security details.

3. This software's danger is hidden behind an attractive appearance. That's why it is often wrapped in attractive package s promising photos of celebrities.
4. There is a particular danger in 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 ' spread s by sending infected emails and is also able to infect websites, so when a user visits a compromise d website, the browser can infect the computer.
6. Every day, millions of children spend time in Internet chat rooms talking to strangers. But what many of them don't realize is that some of the surfers chatting with them may be sexual predators.

Tips:

A. People shouldn't buy cracked software or 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 which websites you visit.
F. Check with your bank before sending information

Vocabulary practice
Complete the crossword puzzle with different kinds of malware.
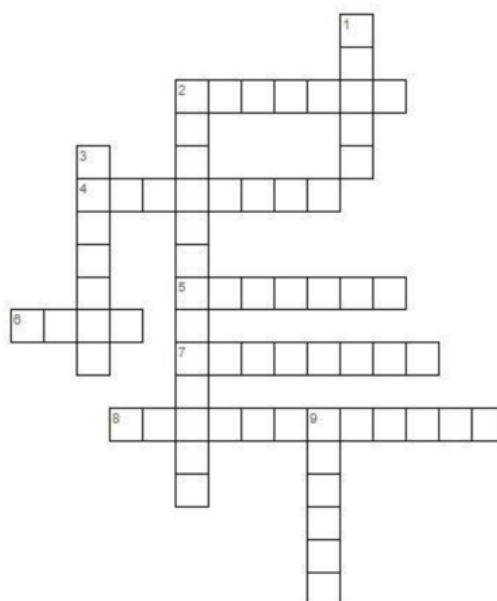
ACROSS	DOWN
2/ is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software	1/ adds itself to an executable file and can cause considerable damage to the data on the infected computer
4/ attempts to acquire information, such as usernames , passwords , and credit card details by masquerading as a trustworthy entity in an electronic communication	2/ keeps visitors from leaving a website by locking them into a window
5/ is installed through a stolen password or by	3/ collects and sends private information from

exploiting system vulnerabilities in order to gain constant administrator-level access to a computer or network	the infected computer to the third party
6/ replicates itself across a network and usually performs malicious actions; it doe s not need to attach itself to an existing program	4/ presents unwanted advertisements embedded in the application
7/ redirects a legitimate website's traffic to another illegitimate website in order to gain access to a user's personal information	
8/ tricks users into clicking on a malicious link by adding the link to a transparent layer over what appear s to be a legitimate we b page	

Speaking

In groups, discuss the following questions.

Which cybercrime from the list below is the most dangerous? Give reasons for your choice.

- piracy
- plagiarism
- cyberstalking
- phishing
- spreading of malware
- distribution of indecent or offensive material
- Is it fair or unfair to pay for the songs, videos, books or articles that you download? Should copyright infringement be allowed online?