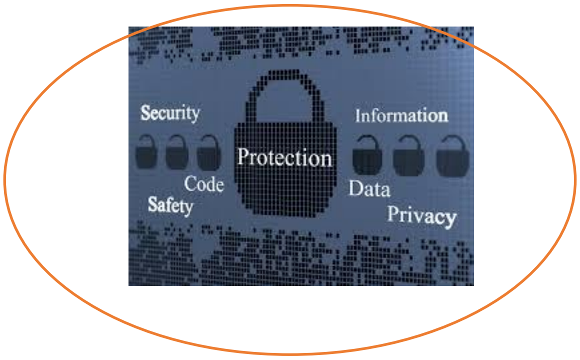
UNIT 3
COMPUTER SECURITY



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.
- understand the use of past simple.
- create an infographic about computer security.

3.1. Computer Threats and Safety

Exercise 1: Work in pairs. Discuss what kinds of computer threats you know and how to prevent as well as to solve them.

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

adware
spyware
hacker
Trojan
browser hijacker
virus
malware attack
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.

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: Listen to this dialogue and answer the questions. Ludek has asked his IT expert friend, Ales, for help.

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?

Exercise 5: Read the following texts about ***Internet Security, Malware: Viruses, Worms, Trojans, and Spyware*** and ***Preventative Tips***.

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.

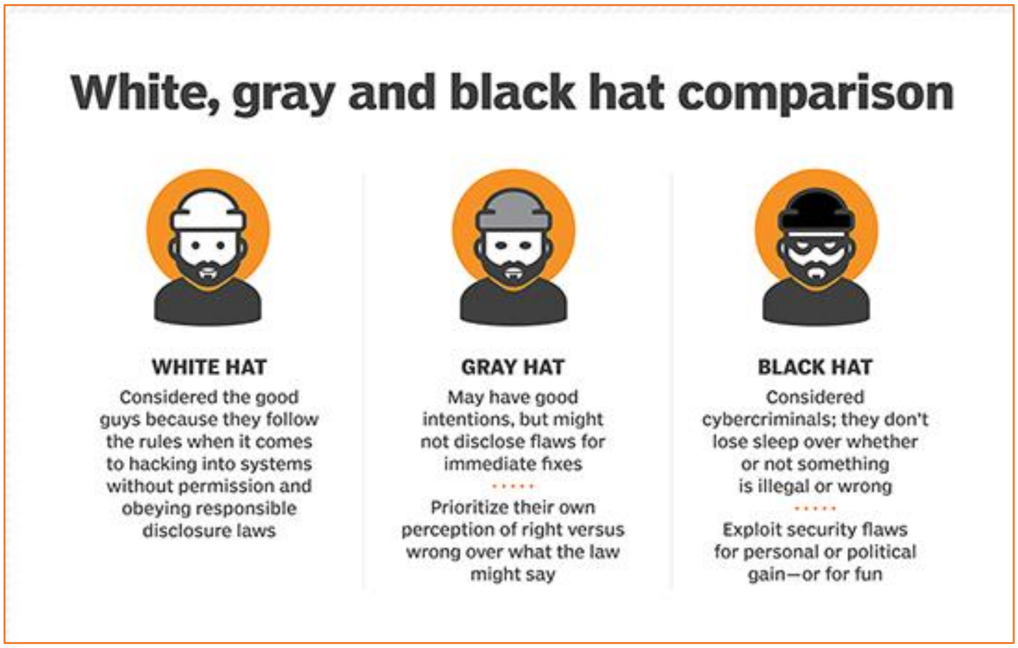
digital certificate   malware   virus   scanner   spyware   firewall   anti-virus

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 _______.

Exercise 7: In pairs, please discuss the following questions.

1. What do you do to prevent computer infections?
2. Do you keep your virus protection updated? The internet has lots of websites where you can get free advice and sofware. What should you di to improve your computer security?

Exercise 8: Study the following comparison about types of hackers. Discuss with your friend about the comparison and your opinion about them.



White, gray and black hat comparison

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

Exploit security flaws for personal or political gain—or for fun

3.2. Grammar Study

Exercise 9: Read Part 1 of the ***History of Hacking*** below and answer the questions.

1. Which hacking case inspired the film *War Games*?

2. When did *Captain Zap* hack into Pentagon?

3. Why was Nicholas Whitely arrested in 1988?

4. How old was the hacker that broke into the US 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 T&T phone company. He started to make free calls. He was arrested in 1972 but wasn’t sent to prison.

1974 Kevin Mitnik, a legend among hackers, began hacking into banking networks and altering the credit reports of his enemies. He did’nt 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 Chrismas message.

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

1989 A 15-year-old hacker cracked the US defence computer.

1991 Kevin Poulsen, knows as dark dante on the networks, was accused of stealing military files.

Taken from Infotect English for Computer Users, pp.96

Past Simple

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

He began hacking in 1974.

- We form the past simple of regular verbs (V2) by adding (-**ed**) to the basic form of the verb (V1).

John Draper discovered that a whistle in boxes of Cap'n Crunch breakfast cereal perfectly generated the 2,600Hz signal used by T&T phone company.

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

Kevin Mitnik began hacking into banking networks and altering the credit reports of his enemies.

begin – began

- 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 hacking would inspire a producer to make a movie.

- We form the past passive with the past simple of **be + the past participle (V3).**

He was arrested in 1972 but wasn't sent to prison.
The IBM international network was paralysed by a hacker's Chrismas message.

Exercise 10: Read Part 2 of the ***History of Hacking*** below and fill in the table using the correct simple past forms of the verbs in the box.

show spread steal launch attempt overwrite be infect affect

In 1992, David L Smith _______ (1) prosecuted for writing the Melissa virus, which was passed in Word files sent via email. In 1997 the German Chaos Computer Club _____ (2) on TV how to obtain money from bank accounts. In 2000, a Russian hacker _____ (3) to extort $100,000 from online music retailer CD Universe. A Canadian hacker _____ (4) a massive denial service attack againts websites like Yahoo! And Amazon. 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. In 2001, the Code Red Worm _____ (7) tens of thousands of machines. In 2006, hackers ____ (8) the credit cards details for almost 20,000 AT&T online customers, However, subscribers to its service (not) _____* (9).

**passive form*

Exercise 11: In small groups, look at the list of cybercrimes below and discuss these following questions. Write a summary of your discussion in Power Point and present it to the rest of the class.

1. Which crime is the most dangerous?
2. It is fair or unfair to pay for the songs, videos, or articles that you download? Should copyright violation be allowed online?
3. What laws can be taken by government to stop cybercrimes?
4. Do you think governments have the right to censor material on the internet?

5. Personal information such as our address, salary, and civil and criminal records is held in databases by marketing companies. Is our privacy in danger?

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** (Password Harvesting Fishing) getting password for online bank accounts or credit card numbers by using email that look like they are from real organizations, but they are in fact fake; people believe the message is from their bank and security details.
- **IP Spoofing** – making one computer look like another in order to gain unauthorized access.
- **Cyberstalking** – online harassment or abuse, mainly in chatrooms or newsgroups.
- **Distribution of indecent or offensive material.**

Taken from Infotech English for Computer Users pp.98

Exercise 12: Work in pairs. Find an article from newspaper about a computer crime in Indonesia and match it with the Information and Electronic Transactions (English Version of UU ITE), discuss, and make an analysis by answering these following questions.

1. From the news, identify: a. The doers/criminals

   b. The crime committed

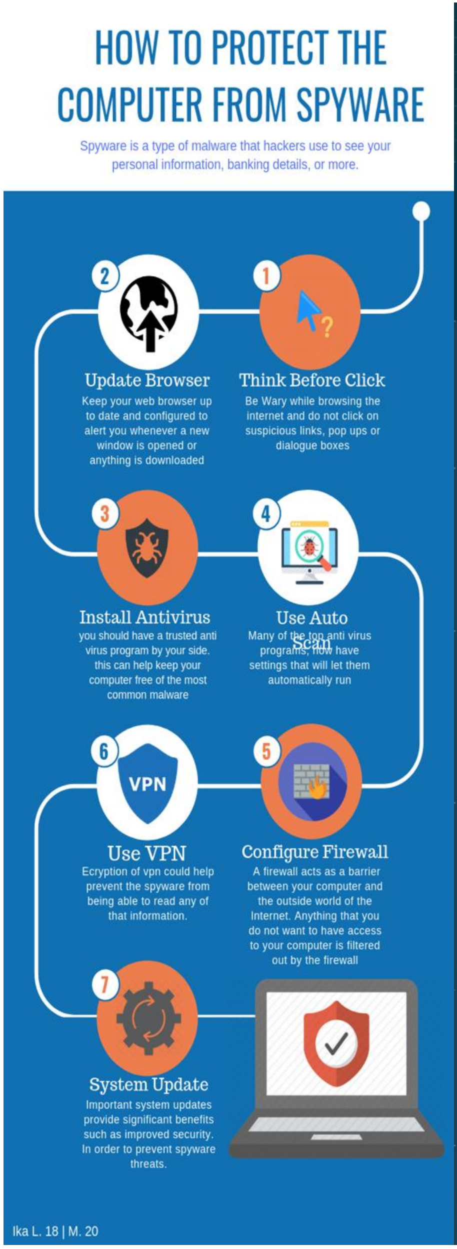
   c. The punishment

2. Do you think the punishment fit the crime? Why? Why not?
3. What should people do to prevent themselves from being the victims of such crime?
4. In what articles and law did the suspect violate the crime?

Exercise 13: Work with your group. Create an infographic dealing with the computer security, especially on the following topics:

- How to prevent malware attack
- Crackers vs Hackers
- Spyware vs Malware
- How to protect the computer from spyware
- How to solve Phishing
- How to solve an attack from Trojan virus

Here is the example of the infographics.



HOW TO PROTECT THE COMPUTER FROM SPYWARE

Spyware is a type of malware that hackers use to see your personal information, banking details, or more.

1 **Think Before Click**
Be Wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes

2 **Update Browser**
Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded

3 **Install Antivirus**
you should have a trusted anti virus program by your side. this can help keep your computer free of the most common malware

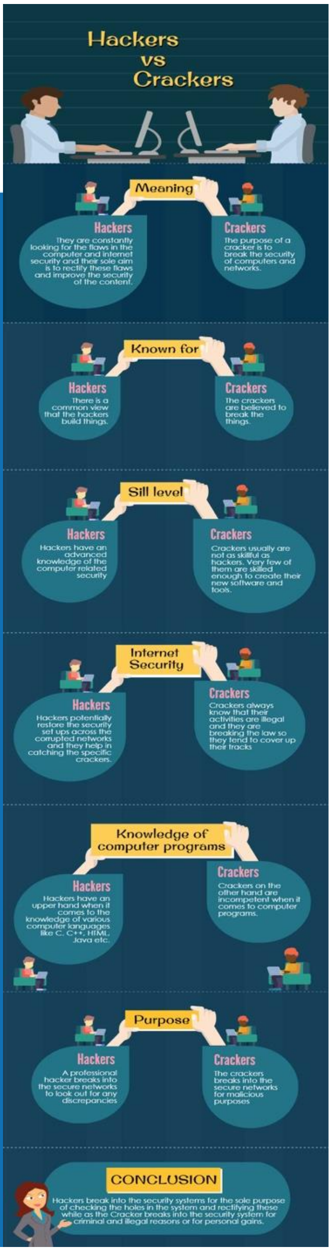
4 **Use Auto Scan**
Many of the top anti virus programs, now have settings that will let them automatically run

5 **Configure Firewall**
A firewall acts as a barrier between your computer and the outside world of the Internet. Anything that you do not want to have access to your computer is filtered out by the firewall

6 **Use VPN**
Ecryption of vpn could help prevent the spyware from being able to read any of that information.

7 **System Update**
Important system updates provide significant benefits such as improved security. In order to prevent spyware threats.

Ika L. 18 | M. 20



Hackers vs Crackers

Meaning

Hackers: They are constantly looking for the flaws in the computer and internet security and their sole aim is to rectify these flaws and improve the security of the content.

Crackers: The purpose of a cracker is to break the security of computers and networks.

Known for

Hackers: There is a common view that the hackers build things.

Crackers: The crackers are believed to break the things.

Sill level

Hackers: Hackers have an advanced knowledge of the computer related security

Crackers: Crackers usually are not as skillful as hackers. Very few of them are skilled enough to create their new software and tools.

Internet Security

Hackers: Hackers potentially restore the security set ups across the corrupted networks and they help in catching the specific crackers.

Crackers: Crackers always know that their activities are illegal and they are breaking the law so they tend to cover up their tracks

Knowledge of computer programs

Hackers: Hackers have an upper hand when it comes to the knowledge of various computer languages like C, C++, HTML, Java etc.

Crackers: Crackers on the other hand are incompetent when it comes to computer programs.

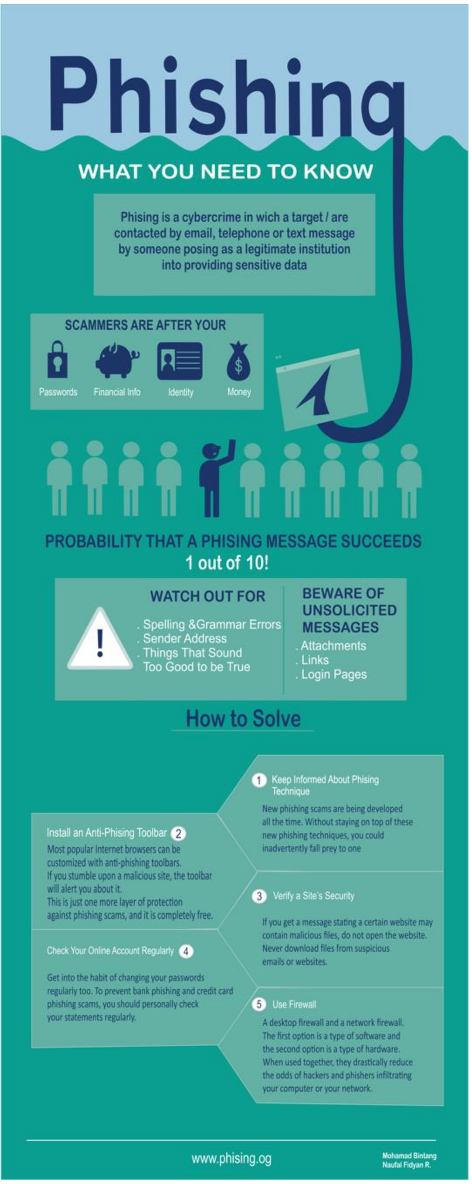
Purpose

Hackers: A professional hacker breaks into the secure networks to look out for any discrepancies

Crackers: The crackers breaks into the secure networks for malicious purposes

CONCLUSION

Hackers break into the security systems for the sole purpose of checking the holes in the system and rectifying these while as the Cracker breaks into the security system for criminal and illegal reasons or for personal gains.



Phishing

WHAT YOU NEED TO KNOW

Phising is a cybercrime in wich a target / are contacted by email, telephone or text message by someone posing as a legitimate institution into providing sensitive data

SCAMMERS ARE AFTER YOUR

Passwords · Financial Info · Identity · Money

PROBABILITY THAT A PHISING MESSAGE SUCCEEDS
1 out of 10!

WATCH OUT FOR
. Spelling &Grammar Errors
. Sender Address
. Things That Sound Too Good to be True

BEWARE OF UNSOLICITED MESSAGES
. Attachments
. Links
. Login Pages

How to Solve

1 Keep Informed About Phising Technique
New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one

2 Install an Anti-Phising Toolbar
Most popular Internet browsers can be customized with anti-phishing toolbars. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

3 Verify a Site's Security
If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites.

4 Check Your Online Account Regularly
Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly.

5 Use Firewall
A desktop firewall and a network firewall. The first option is a type of software and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

www.phising.og

Mohamad Bintang
Naufal Fidyan R.