

Unit 2

COMPUTER AND INTERNET SECURITY

In this unit you will

- ▶ learn and practice vocabulary for online threats and security issues
- ▶ discuss ways of staying safe online



File
Encryption
Program

COMPUTER
SECURITY

STRONG
PASSWORDS

FIREWALL
PROGRAM

BACKUPS

spyware

spam

phishing

data

security

malware

virus

attack

virus detected

virus alert!

Part 1: Cybercrime

1a Class Discussion

- ▶ What are the different dangers of using the Internet?
- ▶ What different kinds of cybercrime (computer crime) do you know?

'Hacking is breaking into a computer system.'

Hacking

A hacker is a person who breaks codes and passwords to gain **unauthorised entry** to computer systems. Hackers can do a lot of damage if they **break into a computer system**. **Stand-alone** computers are usually safe as there is no connection for the hackers to break into. Computers which are part of networks or those with **external links** such as attached modems are in danger from hackers. Many hackers often don't **intend** to damage or steal data, they just enjoy breaking into a system. But other hackers might want to **commit fraud**, **steal valuable data** or to damage or delete data to **harm** a company. Phishing "Phishing" is a form of **Internet fraud** where **criminals** aim to steal valuable information such as credit cards, social security numbers, user IDs and passwords for bank accounts. They set up a **fake website** which looks **identical** to a legitimate company such as a bank or **insurance company**. They then send e-mails or instant messages to people to **trick** them into logging into the site and giving their **account details** and **security codes**.

Copied from <http://www.teachict.com/glossary/P/phishing.htm>



1b Guess the meaning

Guess the Turkish meanings of the **highlighted** words in the text and match them with the following equivalents:

- | | | |
|--------------------------|--------------------|-----------------------|
| sahte web sitesi | dış bağlantılar | aynı |
| izinsiz giriş | güvenlik şifreleri | |
| | tek başına | dolandırıcılık yapmak |
| Internet dolandırıcılığı | yasal şirket | zarar vermek |
| | kandırmak | suçlular |
| niyetli olmak | hesap detayları | |
| değerli verileri çalmak | değerli bilgiler | |



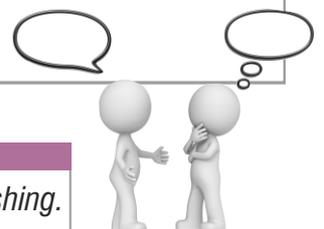
1c Check your understanding

Answer the following questions according to the text.

1. Which one can hackers break into more easily - laptops or networked computers? Why?
2. Is a laptop safer with or without a modem?
3. Why do hackers hack?
4. What kind of valuable information can criminals steal online?
5. How do criminals steal people's valuable information through Phishing?

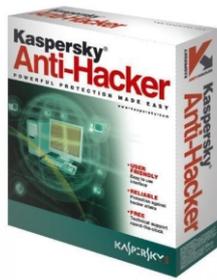
1d Brainstorm

First in pairs and then as whole class, brainstorm for ideas as how to prevent hacking and phishing.



1e Class discussion

- ▶ What is an anti-hacker?
- ▶ Where can you get it?
- ▶ Have you ever used a similar software?



Can a Computer be Protected from Hacking?

Just as in the real world, there is no guaranteed way to stop someone breaking into a building (you can make it very difficult, but every security system has its **weaknesses**), there is also no guaranteed way to stop someone breaking into a computer system. However, you can make it **difficult** enough so that a hacker **moves on** and looks for an easier **target**.

You should:

- ▶ Use **strong passwords** to protect your user login account
- ▶ **Never reveal** your login password to anyone else
- ▶ Place a **firewall** between your computer and any network
- ▶ **Disconnect** from networks when you are not using them
- ▶ **Encrypt** any sensitive information (just in case they get in)

Copied from <<http://www.igcseict.info/theory/6/hack/index.html>>

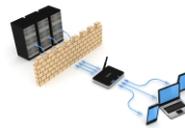
1f Match

Read the text and

1. Match the following with the **highlighted** words in the text.

- | | | |
|------------------------|--------------------------|---------|
| a) goes somewhere else | b) code | c) tell |
| d) break connection | e) opposite of strengths | |
| f) security wall | g) someone to attack | |

2. Match the following pictures with 4 of the suggestions in the text:



1g Check your comprehension

1. According to the text, how is breaking into a computer system similar to breaking into a house?
2. What does a hacker do when it is too difficult to hack into one system?
3. How can you protect your user login account?
4. How can you protect your computer from networks?
5. How can you protect important information?

1h Encryption Game

Using the information in the paragraph, encrypt the following text messages. Your key is **3 (three)**.

- see you later thank you it's late we'll talk tomorrow I have to go

Encryption

Here's a simple encryption system for text messages: change each letter in your message to an X number of letters later in the alphabet. The X number of spaces you move down the alphabet for each letter is the secret key. If the key is two, A becomes C, B becomes D, C becomes E, etc. Using that encryption system, the plaintext message "HELLO" would become "JGNNQ"

Part 2: Malware

2a Class Discussion

- ▶ What do you do if you get a Virus Alert on your computer?
- ▶ What different types of malware do you know?
- ▶ How can a computer or a network be protected from malware?



'Malware means malicious software (kötü amaçlı yazılım).'

2b Check the meaning

Use your glossary to find the meanings of the **highlighted** words in the text.

What is Malware?

Malware is a general term used to describe all of the **harmful** program codes including viruses, spyware, worms, Trojans, or anything that is **designed** to **perform malicious operations** on a computer. They can **log** your **key strokes** secretly (keylogger) or they may **spy** on which sites you are visiting without you knowing (Adware) in order to target **advertises** towards you.

Malware types that hide themselves include Trojan horses and Rootkits. These **disguise** themselves and computer users do not easily recognize them as threats.

2c True (T) or False (F)

Decide if the following statements are True or False according to the text.

1. Trojans are not malware.
2. All malware can do bad things on your computer.
3. A keylogger malware records your keyboard actions.
4. Adware steals your passwords.
5. If you play online games and you have adware in your computer, you can get game advertisements on other websites as well.
6. You can easily see Trojans and Rootkits on your computer.

2d Group Discussion

Trojan malware was named for the fabled "Trojan Horse". Read the story of the Trojan Horse below and then discuss in your groups why this malware was named Trojan. You can also watch a clip from the movie Troy with Brad Pitt:

<http://www.youtube.com/watch?v=YbiR6IMf5KQ>

Story of the Trojan Horse

Almost 3000 years ago, the Greeks fought a battle with the Trojans (people of Troy) but could not get inside the tall strong walls around the city. So the Greeks thought that if they could not win the battle with their physical strength they should win it with their brains. They thought of a smart trick. They started building a wooden horse. The Trojans kept wondering why the Greeks were building a horse. Some laughed and some were puzzled. Then one day when they saw the Greek armies sailing away, they got confused. Soon in few days, all the warships, army tents and armies disappeared. The only thing that remained were the 80 feet tall strange wooden horse.

Some Trojans wanted to burn the horse but the King was too proud of defeating the Greeks and ordered to bring the horse inside the city walls as a symbol of their victory. After pulling the horse inside they partied and danced all night. Then they went to sleep. It was now that the Greeks played the rest of their trick. A very brave Greek soldier named Odysseus hid around thirty strong soldiers inside the hollow wooden horse. The soldiers stepped out in the dark and signaled their warships hiding around a nearby island. Then they opened the Trojan city gates and the Greek army swarmed in.

dapted from <<http://kinooze.com/2012/09/08/the-trojan-horse/>>



Part 3: Internet Safety

3a Class Discussion

- ▶ What is Internet scam?
- ▶ What does the sentence in the image mean?
- ▶ What kind of things sound too good to be true?
- ▶ Have you ever received scam e-mails? What did they say?
- ▶ Have you ever had problems with people online?



3b Read and discuss

Below is a scam e-mail. Read and decide why it is scam.

CONGRATULATIONS!! YOUR EMAIL WON OUR LOTTERY

Dear Winner,

We happily announce to you the draw (#103) of the ACCULOTTO ONLINE INTERNATIONAL E-MAIL LOTTERY held on 17 Feb. 2007. You are among the hundred people who were selected this year to claim the sum of \$1.100,00(one million one hundred thousand dollars). Please note that your lucky winning number falls within our representative office in Africa In view of this, \$1.100,00(one million one hundred thousand dollars) will be released to you by any of our payment offices in Africa. Our agent will send your money as soon as you contact him. To claim your money, please contact our agent through the e-mail below with your information: 1) name, 2) occupation, 3) age, 4) sex, 5) nationality, 6) phone number and address

Dr Allan Smith

Email: agent_allan_smith@yahoo.com.mx

3c Check the meaning



Use your glossary to check the meanings of the **highlighted** words in the following text.

Stay safe online

The Internet is a valuable and fun resource for entertainment, making friends and learning. Social networking sites, such as Facebook, MySpace, Bebo and Twitter have become increasingly popular in recent years.

But if you use the internet, you could be at risk of **illegal activity** or **abuse** - be it **bullying**, **fraud** or something more serious. Unlike seeing someone face to face, people aren't always what they first seem on the Internet.

The Internet offers you a lot of freedom and this can lead some people to behave in ways they would not behave in **public**. For example, they might say things in a chat room they would never say face to face. Therefore, it is important to learn how to stay safe online.

Some Golden Rules

- ▶ Don't give out personal information such as your address or phone number.
- ▶ Don't open emails or attachments from people you don't know.
- ▶ Don't become online 'friends' with people you don't know.
- ▶ Never arrange to meet someone in person who you've met online.
- ▶ If anything you see or read online worries you, tell someone about it.

Adapted from <http://safe.met.police.uk/internet_safety/get_the_facts.html>

3d Read and answer

1. What is the Internet good for?
2. What are the risks of using the Internet?
3. What can people do online which they might not do in public?
4. Which golden rules from the text can be used with the e-mail above?

3e Group work

As a group write up a list of tips to help young people stay safe on social networking sites. The group with most ideas wins.

Part 4 Choosing Passwords

4a Class Discussion

- ▶ What do you have passwords for?
- ▶ Do you use the same password for everything?
- ▶ Are your username and password the same or different?
- ▶ How do you choose your passwords?
- ▶ Do you think your passwords are strong?
- ▶ What tips do you have for choosing a strong password?

Log in

Username: *****
Password: *****

4b Check the meaning

Skim the text **Choosing the Best Passwords** and use your glossary to check the meanings of the **highlighted** words in the text.

4c Match

Match the following passwords and PIN numbers with the phrases:

- | | |
|------------------|---|
| 1) ali@2237442 | a) all uppercase letters |
| 2) 44444444 | b) combination of upper and lower case letters |
| 3) HUSEYIN | c) combination of numbers, symbols and lower case letters |
| 4) 13579 | d) ascending numbers |
| 5) KArAogLanOGIU | e) descending numbers |
| 6) 123456 | f) numerical sequence |
| 7) 147*0 | g) duplicated number |
| 8) 97642 | h) easily recognizable keypad pattern |



Picture A: a phone keypad

Choosing the Best Passwords - Dos and Don'ts

Do:

- ▶ Always use a password.
- ▶ Choose a password with a combination of **upper and lower case letters**, numbers and keyboard symbols such as @ # \$ % ^ & * () _ +. For example, **SP1D3Rm@n** is a variation of **spiderman**, with upper and lower case letters, numbers, and symbols. However, be aware that some of the symbols may be difficult to enter on **foreign keyboards**.
- ▶ Choose a password containing at least eight characters. Longer passwords are harder for criminals to guess or break.

Don't:

use the following as passwords:

- ▶ Your **username**, actual name or business name.
- ▶ Family members' or pets' names.
- ▶ Your or family birthdays.
- ▶ Favourite football team or other words easy to work out with a little background knowledge.
- ▶ The word 'password'.
- ▶ **Numerical sequences**
- ▶ A **commonplace** dictionary word, which could be cracked by common hacking programs
- ▶ When choosing numerical passcodes or PINs, do not use **ascending** or **descending** numbers, **duplicated** numbers or easily **recognizable** keypad patterns such as 14789 or 2580 (see Picture A).

4d Analyze

Read the text with your partner and decide if the following passwords are strong or weak. Put them under the right column below. Then join the class to explain your decisions.

- | | |
|----------------|---------------|
| a) 26Nisan1990 | b) bukalemun |
| c) A1TC ^ n | d) wordpass |
| e) B3y@RmUdU | f) Cem12345 |
| g) 891011 | h) F3n3rB@hc3 |



4e Improve the passwords

Work with your partner to improve the following passwords.

karagozlum Galatasaray serce
Haspolat Musti1996 babutsa

