

# UNIT 8

Internet security

# 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 passwords for online bank accounts or credit card numbers by using emails that look like they are from real organizations, but are in fact fake; people believe the message is from their bank and send their security details
- **IP spoofing** - making one computer look like another in order to gain unauthorized access
- **Cyberstalking** - online harassment or abuse, mainly in chat rooms or newsgroups
- **Distribution of indecent or offensive material**



## **Hacker** /'hækə/ *n*

Some one who invades a network's privacy. Originally, all computer enthusiasts and skilled programmers were known as **hackers**, but during the 1990s, the term hacker became synonymous with **cracker**, a person who breaks security on computers. Today, people often use the word hacker to mean both things. In the computer industry, hackers are known as *white hats* and crackers are called *black hats* or *darkside hackers*.

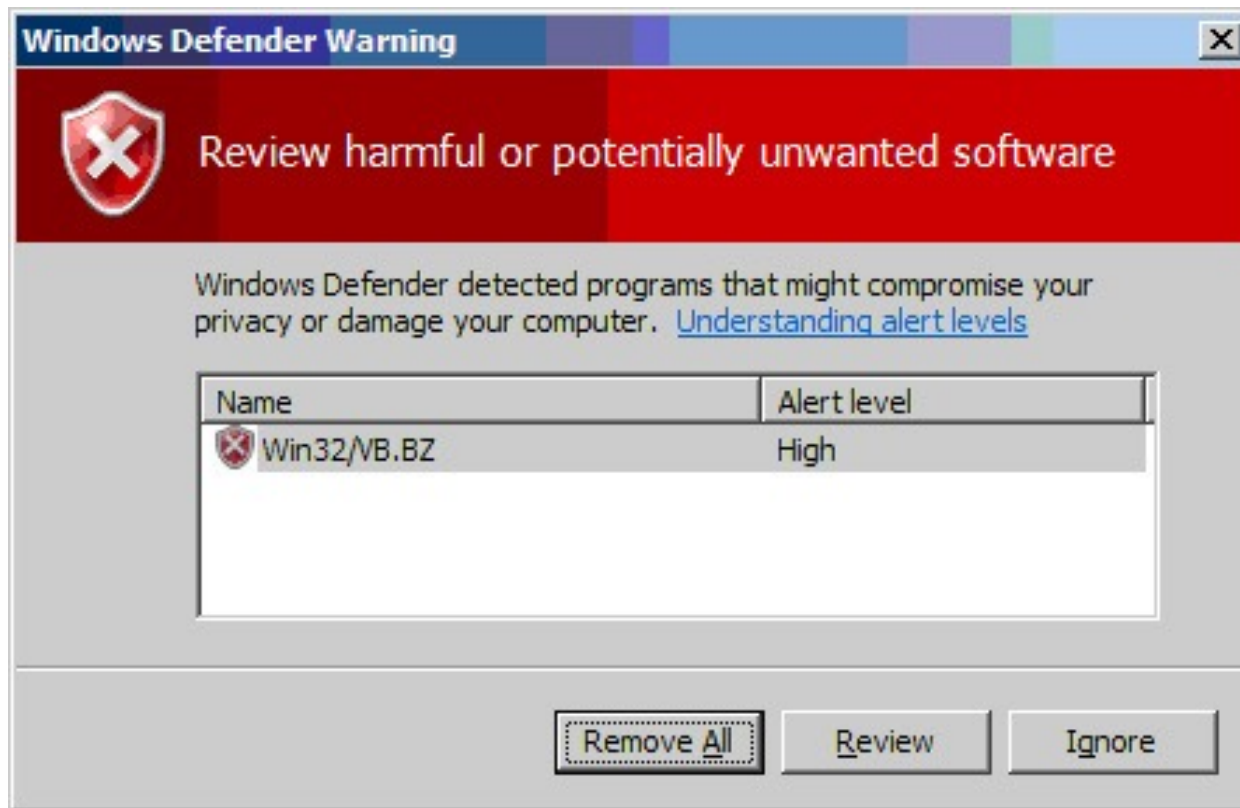
## **Virus** /'vaɪrəs/ *n*

A piece of software which attaches itself to a file. Once you run an infected program, the virus quickly spreads to the system files and other software. Some viruses can destroy the contents of hard disk.



**B** Match the captions (1 -4)with the pictures(a-d).

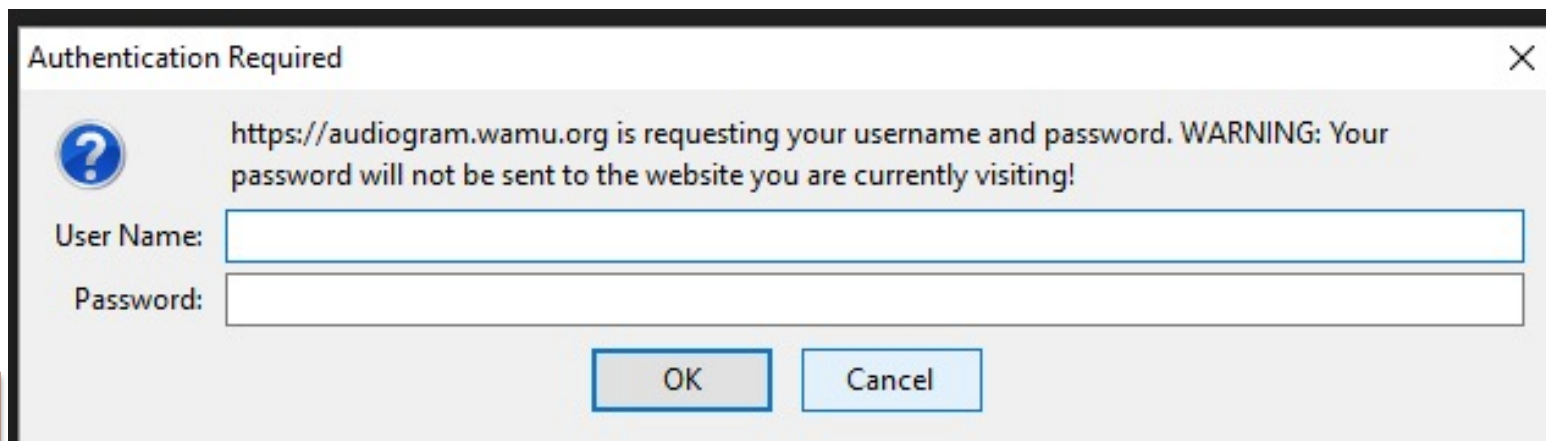
**a**



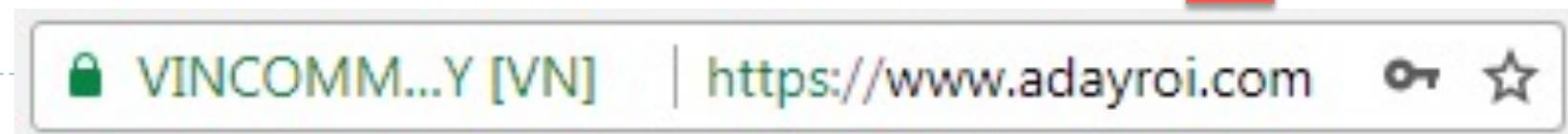
**b**



**c**



**d**



# Security and privacy on the Internet

There are many benefits from an open system like the Internet, but one of the risks is that we are often exposed to hackers, who break into computer systems just for fun, to steal information, or to spread viruses (see note below). So how do we go about making our online transactions secure?

## Security on the Web

Security is crucial when you send confidential information online. Consider, for example, the process of buying a book on the Web. You have to type your credit card number into an order form which passes from computer to computer on its way to the online bookstore. If one of the intermediary computers is infiltrated by hackers, your data can be copied.

To avoid risks, you should set all security alerts to high on your web browser. Mozilla Firefox displays a lock when the website is secure and allows you to disable or delete cookies - small files placed on your hard drive by web servers so that they can recognize your PC when you return to their site.

If you use online banking services, make sure they use digital certificates - files that are like digital identification cards and that identify users and web servers. Also be sure to use a browser that is compliant with SSL (Secure Sockets Layer), a protocol which provides secure transactions.

## Email privacy

Similarly, as your email travels across the Net, it is copied temporarily onto many computers in between. This means that it can be read by people who illegally enter computer systems.

The only way to protect a message is to put it in a sort of virtual envelope - that is, to encode it with some form of encryption. A system designed to send email privately is Pretty Good Privacy, a freeware program written by Phil Zimmerman.



# Security and privacy on the Internet

## Network security

Private networks can be attacked by intruders who attempt to obtain information such as Social Security numbers, bank accounts or research and business reports. To protect crucial data, companies hire security consultants who analyse the risks and provide solutions. The most common methods of protection are passwords for access control, firewalls, and encryption and decryption systems. Encryption changes data into a secret code so that only someone with a key can read it. Decryption converts encrypted data back into its original form.


## Malware protection

Malware (malicious software) are programs designed to infiltrate or damage your computer, for example viruses, worms, Trojans and spyware. A virus can enter a PC via a disc drive – if you insert an infected disc - or via the Internet. A worm is a self-copying program that spreads through email attachments; it replicates itself and sends a copy to everyone in an address book. A Trojan horse is disguised as a useful program; it may affect data security. Spyware collects information from your PC without your consent. Most spyware and adware (software that allows pop-ups - that is, advertisements that suddenly appear on your screen) is included with 'free' downloads.

If you want to protect your PC, don't open email attachments from strangers and take care when downloading files from the Web. Remember to update your anti-virus software as often as possible, since new viruses are being created all the time.

**Note:** Originally, all computer enthusiasts and skilled programmers were known as **hackers**, but during the 1990s, the term hacker became synonymous with **cracker** - a person who uses technology for criminal aims. Nowadays, people often use the word hacker to mean both things. In the computer industry, hackers are known as *white hats* and crackers are called *black hats* or *darkside hackers*.

## B Read the text more carefully and answer these questions.

1. Why is security so important on the Internet?
    - Because the Internet is an open system and we are exposed to hackers who break into computer systems to steal or destroy data. Security is crucial when we send confidential information such as credit card numbers.
  2. What security features are offered by Mozilla Firefox?
    - Mozilla Firefox displays a lock when the website is secure and allows you to disable or delete cookies.
  3. What security protocol is used by banks to make online transactions secure?
    - Bank use SSL (Secure Sockets Layer), a protocol which provides secure transactions.
  4. How can we protect our email and keep it private?
    - We can encode our email using an encryption program like Pretty Good Privacy.
  5. What methods are used by companies to make internal networks secure?
    - The most common methods to protect private networks are passwords for access control, firewalls, and encryption & decryption systems
  6. In what ways can a virus enter a computer system?
    - A virus can enter a PC via an infected disc or via the Internet.
  7. How does a worm spread itself?
    - A worm spreads through email attachments; it replicates itself and sends a copy to everyone in an email address book.
- 

C Solve the clues and complete the puzzle.

				1	P	A	S	S	W	O	R	D
				2	F	I	R	E	W	A	L	L
				3	H	A	C	K	E	R		
				4	V	I	R	U	S	E	S	
	5	F	R	E	E	W	A	R	E			
6	E	N	C	R	Y	P	T	I	O	N		
	7	D	E	C	R	Y	P	T	I	O	N	
				8	S	P	Y	W	A	R	E	



# 4 The history of hacking

## **A Read Part 1 of the text and answer these questions.**

- 1 Which hacking case inspired the film *War Games*?
- 2 When did *Captain Zap* hack into the 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 the AT&T phone company. He started to make free calls. He was arrested in 1972 but wasn't sent to prison.
- 1974** – Kevin Mitnick, a legend among hackers, began hacking into banking networks and altering the credit reports of his enemies. He didn't 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 Christmas message.
- 1988** – The Union Bank of Switzerland almost lost £32 million to hackers. Nicholas Whitely was arrested in connection with virus spreading.
- 1989** – A fifteen-year-old hacker cracked the US defence computer.
- 1991** – Kevin Poulsen, known as *Dark Dante* on the networks, was accused of stealing military files.

# The past simple

---

- ▶ Quá khứ đơn: để nói về một hành động hoàn chỉnh hoặc sự kiện đã xảy ra vào một thời điểm cụ thể trong quá khứ.

- ▶ Động từ thường chia thì quá khứ đơn = infinitive + **-(e)d**

*John Draper **discovered** that a whistle...*

- ▶ Câu hỏi và phủ định sử dụng **did/didn't**

*When **did** Captain Zap **hack** into the Pentagon?*

*He **didn't expect** that his most famous exploit...*

- ▶ Động từ bất quy tắc

*Kevin Mitnick **began** hacking into...*

*When **did** Kevin Mitnick **begin** hacking into ...?*

*He **didn't begin** hacking until 1974.*

- ▶ Quá khứ bị động = quá khứ đơn của be + quá khứ phân từ.

*IBM international network **was paralysed** by hackers.*

*He **wasn't sent** to prison.*

*Why **was** Nicholas Whitely **arrested** in 1998?*



Complete Part 2 of the text with the past simple form of the verbs in the box.

show	spread	steal	launch	attempt	overwrite	be	infect	affect
------	--------	-------	--------	---------	-----------	----	--------	--------

### The history of hacking – Part 2

- 1992** – David L Smith (1) was prosecuted for writing the Melissa virus, which was passed in Word files sent via email.
- 1997** – The German Chaos Computer Club (2) showed on TV how to obtain money from bank accounts.
- 2000** – A Russian hacker (3) attempted to extort \$100,000 from online music retailer CD Universe.  
A Canadian hacker (4) launched a massive *denial of service* attack against websites like Yahoo! and Amazon.  
The *ILoveYou* virus, cleverly disguised as a love letter, (5) spread so quickly that email had to be shut down in many companies. The worm (6) overwrote image and sound files with a copy of itself.
- 2001** – The *Code Red* worm (7) infected tens of thousands of machines.
- 2006** – Hackers (8) stole the credit card details of almost 20,000 AT&T online customers.  
However, subscribers to its service (9) (not) affected.

# B Read these landmarks in the history of the Internet

---

**1969** - The US Defense Department establishes ARPANET, a network connecting research centres.

**1971** - Ray Tomlinson of BBN invents an email program to send messages across a network. The @ sign is chosen for its *at* meaning.

**1981** - IBM sells the first IBM PC. BITNET provides email and file transfers to universities

**1982** - TCP/IP is adopted as the standard language of the Internet.

**1988** - Jarkko Oikarinen develops the system known as Internet Relay Chat (IRC).

**1991** - CERN (*Conseil Europeen pour la Recherche Nucleaire*) creates the World Wide Web

**1998** - The Internet 2 network is born. It can handle data and video at high speed but is not a public network.

**1999** - Online banking, e-commerce and MP3 music become popular.

**2001** - Napster, whose software allows users to share downloaded music, maintains that it does not perpetrate or encourage music piracy. However, a judge rules that Napster's technology is an infringement of music copyright.

**2004** - Network Solutions begins offering 100-year domain registration.

**2006** - Americans spend over \$100 billion shopping online.

---

