Unit 19 Internet security

1 On alert

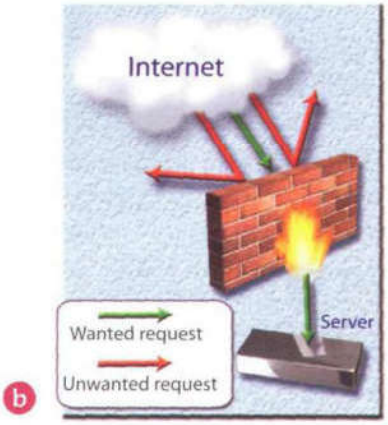
A **In pairs, discuss these questions.**

1 What is a hacker?
2 How easy do you think it is to infiltrate the Internet and steal sensitive information?
3 How can you protect your computer from viruses and spyware?

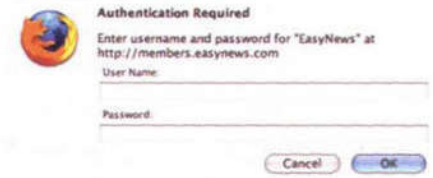
B **Match the captions (1–4) with the pictures (a–d).**

1 A secure website can be recognized in two ways: the address bar shows the letters *https* and a closed padlock or key is displayed at the bottom of the screen.
2 You have to type your username and password to access a locked computer system.
3 This program displays a message when it detects spyware and other unwanted software that may compromise your privacy or damage your computer.
4 Private networks use a software and/or hardware mechanism called a firewall to block unauthorized traffic from the Internet.

a



b



c

d

2 Security and privacy on the Internet

A **Read the text quickly and see how many of your ideas from 1A Question 3 are mentioned.**

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

1 Why is security so important on the Internet?
2 What security features are offered by Mozilla Firefox?
3 What security protocol is used by banks to make online transactions secure?
4 How can we protect our email and keep it private?
5 What methods are used by companies to make internal networks secure?
6 In what ways can a virus enter a computer system?
7 How does a worm spread itself?

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** (**S**ecure **S**ockets **L**ayer), 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.

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.

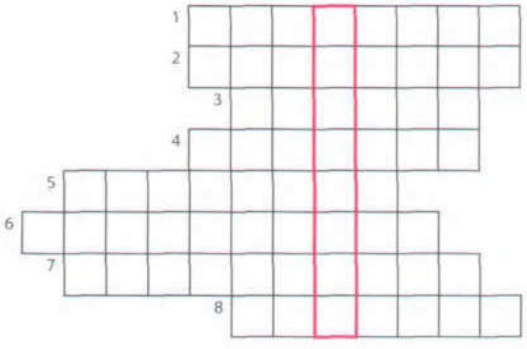
Malware protection

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*.

C Solve the clues and complete the puzzle.



1 Users have to enter a _____ to gain access to a network.

2 A _____ protects a company intranet from outside attacks.

3 A _____ is a person who uses their computer skills to enter computers and networks illegally.

4 _____ can infect your files and corrupt your hard drive.

5 You can download _____ from the Net; this type of software is available free of charge but protected by copyright.

6 Encoding data so that unauthorized users can't read it is known as _____.

7 This company uses _____ techniques to decode (or decipher) secret data.

8 Most _____ is designed to obtain personal information without the user's permission.