IT security and safety
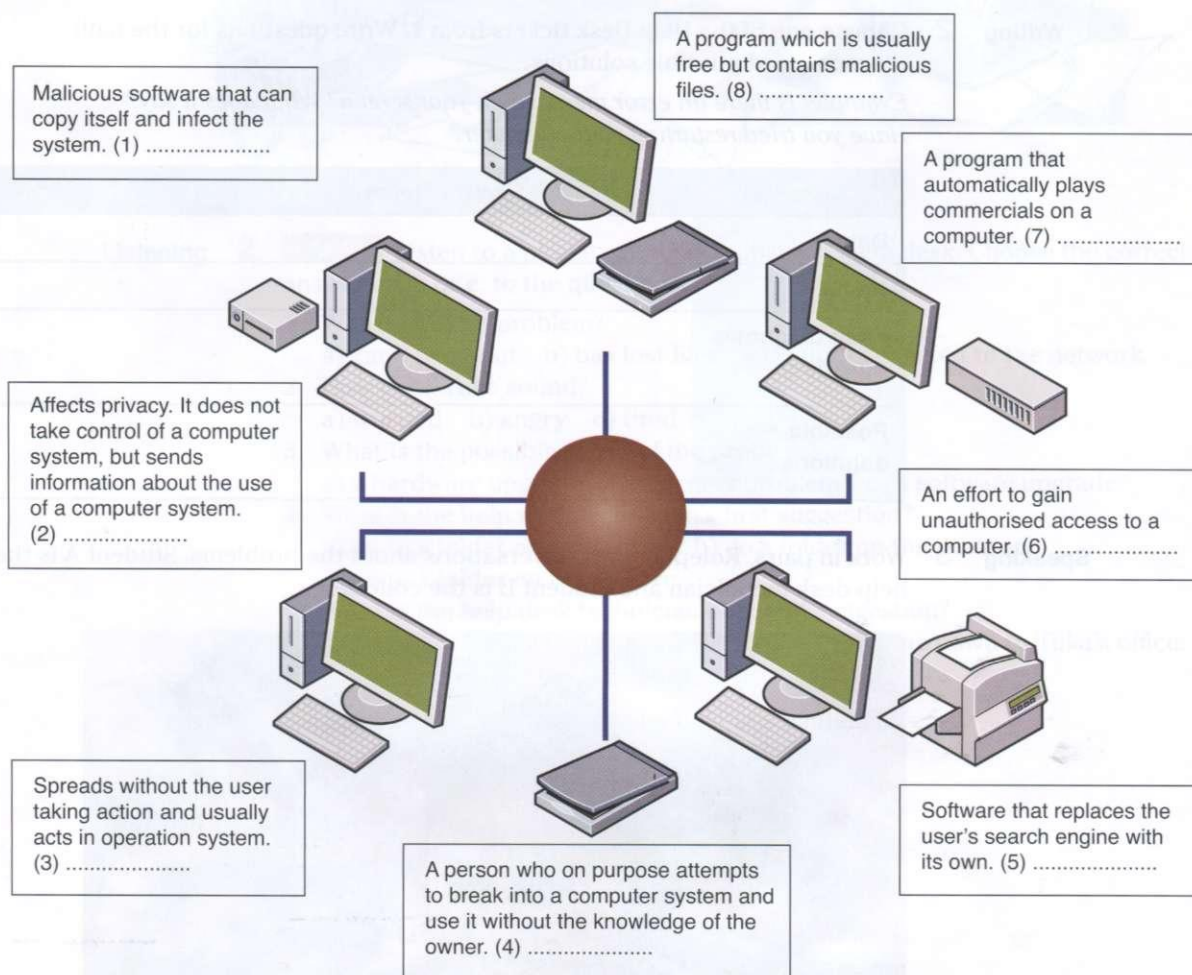
- talk about security solutions
- express possibility and prohibition
- report events and incidents
- recommend improvement actions

Security solutions

Speaking **1** Work in pairs. Make a list of all the different words about security threats and attacks you can think of.

Reading **2** Read the descriptions 1–8. Match the words in the box to the descriptions.

> adware   hacker   browser hijacker   malware attack   spyware
> Trojan   virus   worm

Malicious software that can copy itself and infect the system. (1) ....

A program which is usually free but contains malicious files. (8) ....

A program that automatically plays commercials on a computer. (7) ....

Affects privacy. It does not take control of a computer system, but sends information about the use of a computer system. (2) ....

An effort to gain unauthorised access to a computer. (6) ....

Spreads without the user taking action and usually acts in operation system. (3) ....

A person who on purpose attempts to break into a computer system and use it without the knowledge of the owner. (4) ....

Software that replaces the user's search engine with its own. (5) ....

Speaking **3** Have you ever had a computer security threat? Has anyone ever hacked into your computer system? Use the words and phrases in 2 to describe what happened.

4 Work in small groups. Discuss what you can do to stop these problems.

Vocabulary **5** 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 authorised people access the network
c) checks the user is allowed to use system
d) blocks unauthorised access codes
e) protects the system from public access

Listening **6** 🎵 48 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?

Language

Expressing possibility

We use **may/might** + infinitive without *to* to talk about things that are possible now or in the future.	*You **may** have a virus on your computer.*
	*The program **might** not run properly.*

Speaking **7** Work in pairs. Practise giving advice to a non-IT expert on protecting their computer.

Example:
Non-IT expert: What should I do to stop … ?
*Expert: You should … . It may/might … .*

Workstation health and safety

Speaking **1** Work in pairs. Make a list of computer health and safety problems. Compare your list with another pair.

Vocabulary **2** Label this diagram with the advice 1–8.

1 There should be clearance under the work surface.
2 You should have your feet flat on the floor.
3 Make sure your forearms and hands are in a straight line.
4 Your lower back should be supported.
5 Your screen should be positioned to avoid reflected glare.
6 Keep your shoulders relaxed.
7 You should have your thighs tilted slightly.
8 Make sure the top of the screen is at or slightly below eye level.

a) ☐   b) ☐   g) ☐   h) ☐   f) ☐   c) ☐   d) ☐   e) ☐
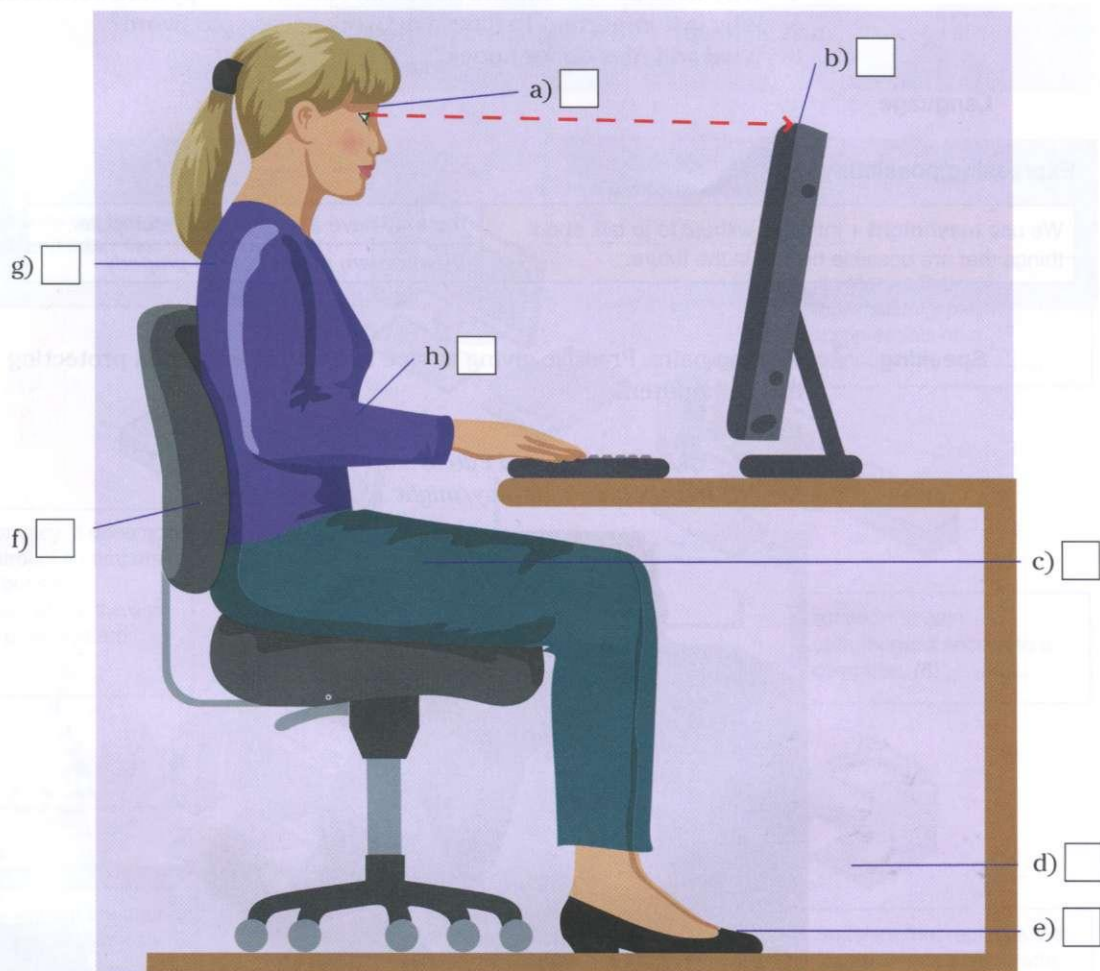
Speaking **3** Work in pairs. Answer these questions about the advice in 2.

1 Do you always follow the advice?
2 What other things can you recommend for good computer use?
3 Have you had (or given) computer use training?

4 Work in pairs. Practise giving instructions to each other.

Example: Make sure you … .

Reading　**5**　Read this list of rules for using a company computer. Which ones do you follow? Why?

COMPUTER DOS AND DON'TS

Things you should do:
– Run Scandisk regularly to check and repair your file systems.
– Connect all peripherals before you switch the computer on.
– Keep your keyboard and screen clean.
– Keep CDs and DVDs in covers and hold them by the edge when using.
– Always shut down your laptop computer first if you need to move it.
– Secure your hardware from sudden power surges.

Things you should not do:
– Do not disconnect the keyboard, mouse, monitor, printer or any peripheral if the PC is on.
– Don't eat food or drink near the keyboard and computer. Don't blow smoke over your PC.
– Don't move or lift your desktop computer when it's on. Don't drop your laptop.
– Don't clean your hardware with a household polish or cleaner.
– Don't turn your computer off for lunch breaks.
– Don't load unauthorised software.

Vocabulary　**6**　Match the verb 1–5 with the noun a–e.

1	switch/turn off	a) software
2	eat	b) software
3	connect	c) peripherals
4	load	d) food
5	run	e) the computer

Speaking　**7**　Work in pairs. Discuss what other rules you can add to the two lists in 5. Compare your list with another pair.

8　What is the most important rule you can give about computer use? Work in pairs. Practise giving advice to each other.

Example: Always … ./You should … .

Security procedures

Speaking **1** What security procedures are you familiar with? Make a list and share it with the group.

Reading **2** Read this text on security and match the headings in the box with the paragraphs 1–5.

Data transfer and backup	Email and network usage
Password recommendations	Reporting IT security incidents
Safety security requirements	

Systems and network security

All employees must follow security and safety procedures approved by the management.

1 _____

Only install and use software that the management has approved. Install the latest antivirus and antispyware tools.

Keep current with security software updates and patches.

Follow office health and safety standards.

2 _____

Choose a password that is difficult to guess: use between 6 and 8 characters, have letters in upper and lower case and intermix letters, numbers, and punctuation marks. Keep your password private. Change your password every 9 weeks.

3 _____

Configure your email software to use secure protocols. Use company official e-mail software only. Always double check that you are sending your message to the right recipient. Do not send sensitive data over the network. Use mail encryption to send sensitive data. Do not download unknown files or files for private use, such as movies and music.

4 _____

Transfer files via a secure connection. Back up files regularly on the server in your homefolder. Do not use external drives.

5 _____

Employees must notify their supervisor or IT help desk about any damage, misuse, irregularities or security breaches.

Vocabulary **3** Match the verb 1–6 with the noun a–f.

1	transfer	a) protocols
2	install	b) software
3	follow	c) procedures
4	use	d) files
5	notify	e) an incident
6	report	f) a supervisor

Speaking **4** What are the most important procedures to follow in the document in 2?
Which procedures do people sometimes not follow?

Language

Expressing prohibition

a rule or requirement (We use these when it is necessary not to do this or to tell someone not to do something.)	You **mustn't** give your password to anyone.
	You **aren't allowed/permitted** to share your password with anyone.
a strong recommendation (We use this to give advice.)	You **shouldn't** use your date of birth in your password. (It is not a good idea to do this)

Listening **5** 🎧 **49** Listen and repeat these sentences.

1 You mustn't put your cup of coffee on the computer.
2 You mustn't work without breaks.
3 You aren't allowed to smoke in the office.
4 We aren't allowed to send private emails.
5 You shouldn't eat lunch at your desk.

Speaking **6** Work in small groups. Talk about the computer regulations in your company or college. Use *you mustn't*, *you aren't allowed to* and *you shouldn't*.

Writing **7** Write a document listing the regulations you talked about in 7. Use these headings.

Personal use of computers

Health and safety

Security

Reporting problems

Reporting incidents

Speaking **1** Have you ever reported a security incident? What was it about?

Reading **2** Read these five IT incidents in a company.

A

Incident report

Date: 02.05

Report for: Miley O'Hara

Report prepared by: Ann Greshon

Incident: teacher, has accessed the database to change student's grade

Recommendations:

C

Incident report

Date:

Report for:

Report prepared by:

Incident: employee's children have installed games on company's laptop

Recommendations:

B

Incident: employee has changed the printer settings

Recommendations:

E

Incident report

Date:

Report for:

Report prepared by:

Incident:

Incident: employee has downloaded a movie

Recommendations:

Incident: employee has installed P2P software

Recommendations:

Speaking **3** Work in pairs. Grade the incidents: 1 = the least serious. 5 = the most serious. Then compare your grades in small groups.

Writing **4** Write a short report to the IT supervisor on the most serious incident. You will need to give recommendations on how to deal with the incident.

Incident report

Date:

Business matters

Reading **1** Work in pairs. You are systems safety coordinators. You have already completed two inspections of the IT systems in QuickFix Ltd. The first inspection was about network security and the second about health and safety in a workplace. Your investigation shows that the company has very poor security and safety systems. Look at the pictures and make notes.
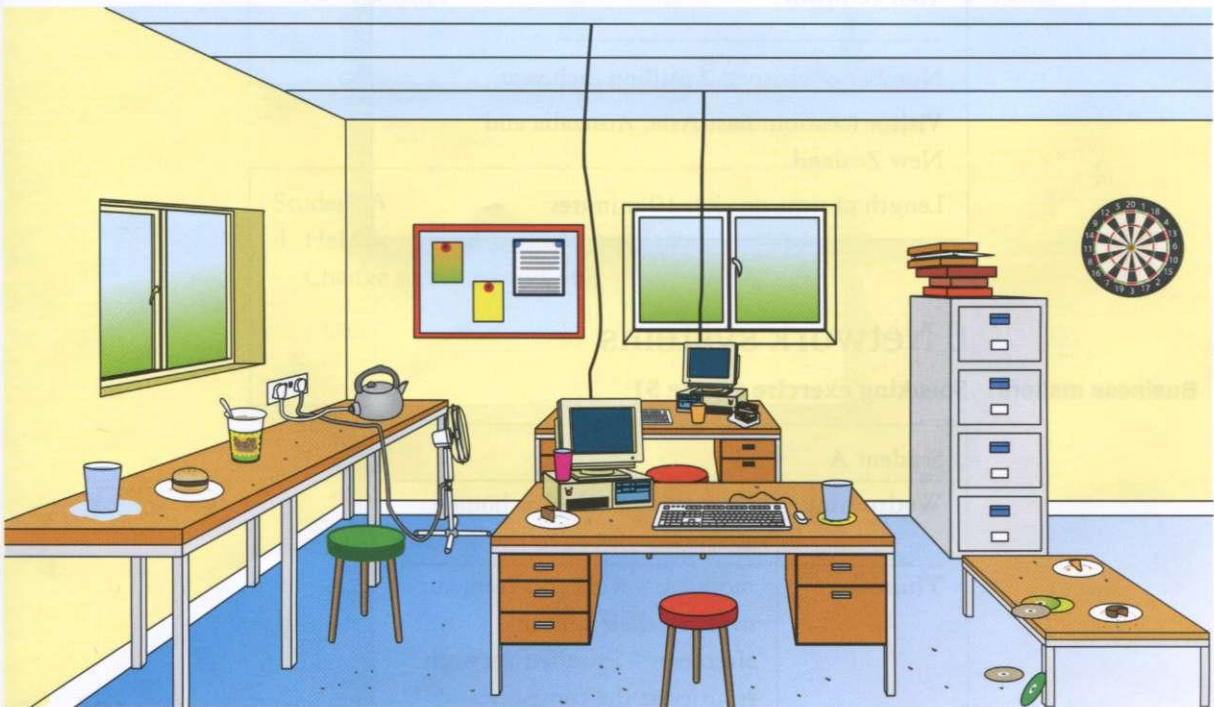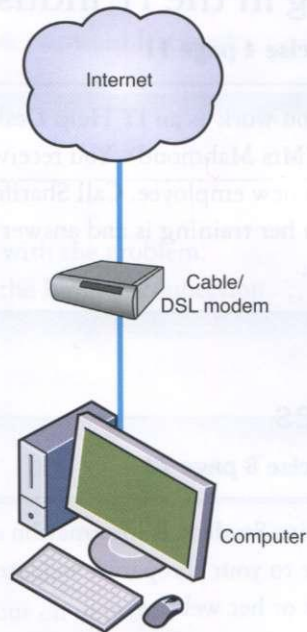
Speaking **2** Based on the information in the pictures and your notes, present your report after the inspections. Student A: talk about health and safety in the workplace. Student B: talk about network security.