8 IT security and safety

Briefing

This unit focuses on security threats, solutions and procedures, as well as workstation health and safety. It also looks at reporting security incidents and reviewing security.

Security solutions

Here the focus is on **security threats to IT systems** and what can be done to deal with these threats. As such, it relates to and develops the focus on **transaction security** in Unit 4. **Adware** refers to programs that automatically download and/or display advertisements on the computer. **Spyware** is software that can send information about the use of a computer system. **Malware**, from the words *malicious* and *software*, is a general term that refers to programs designed to gain access to a computer without the user's authorisation or knowledge. One example is **worms**, programs that spread to other computers without the user taking action. Another example is **Trojans**, which are programs that pretend to be useful, encouraging a user to download and/or use them but that in fact damage the system. **Viruses** copy themselves into other programs and cause system problems. A **browser hijacker** is software that replaces the user's search engine with its own. Another security threat mentioned is **piggybacking**, which is using someone else's wireless internet connection without their permission in order to access the internet.

Solutions mentioned include **biometric scanning** (for example, using thumb prints to identify people) and **antivirus software**, which is designed to protect computers from cyber attack.

In addition, there is a communicative focus on expressing probability (for example, *You **might** have a virus on your computer*.).

Workstation health and safety

This section deals with how you should sit at your computer as well as giving instructions on health and safety. Students will need to know these words: *eye*, *forearm*, *hand*, *foot*, *back*, *shoulder*, *thigh*. **Reflected glare** is the light emitted from the computer screen.

There is also a focus on computer dos and don'ts (for example, connecting peripherals before turning your computer on or off).

Scandisk is a utility that checks and repairs file systems. **Power surges** are when there is an unexpected increase in power (for example, as a result of electric storms). **Unauthorised software** is software the organisation has not given permission to use.

Security procedures

This section focuses on the kind of rules and recommendations that employees are likely to be asked to follow in a large organisation to meet security requirements. **Data transfer** means the moving of information (for example, from an office computer to a home one). **Security incidents** are events that threaten security. A **security breach** is when someone accesses a computer system illegally or without permission.

There is also a focus on *mustn't*, *shouldn't* and *not be allowed/permitted* to express prohibition.

Reporting incidents

Here the objective is to teach students how to write a short report on a security incident. The incidents reported are changing printer settings, downloading a movie at work, installing unauthorised software and a teacher accessing a database to change a student's grade. **P2P** (Peer-to-Peer or Person-to-Person) software allows people to share computer resources with each other but is often used for things such as illegal file sharing.

Business matters

In this section, students have to review and report on a computer set-up in an office, both in terms of health and safety and computer security. The safety focus is on things like having cables correctly positioned, having the right sort of office furniture and the dangers of putting food and drink on workstations.

A **DSL** (Digital Subscriber Line) modem provides the connection from a computer to the internet.

Further reading

Use the following keywords to search the internet for websites which give more in-depth information about the topics covered in this unit: hacker, viruses, worms, computer health and safety.

Teacher's notes

Before you start the unit

Review the content of Unit 7. Ask students to give you a list of typical computer faults and write them on the board. Then ask students to work in pairs and roleplay conversations where Student A explains the fault and Student B tries to provide a solution (for example, *'My printer isn't working.' 'Have you checked the connection?'*).

Security solutions

Speaking

1 Do the activity with books closed as many terms students suggest may be in Exercise 2. In addition to the terms in the reading text, students may suggest some of the following: *zombies*, *phishing*, *viral websites*, *bluesnarfing*.

Reading

2 Pre-teach the following words and phrases: *malicious*, *infect*, *spread*, *replace*, *gain unauthorised access* and *commercials*. Then go through the eight descriptions to check that students understand them. Finally, ask them to match the words to the descriptions.

1 virus **2** spyware **3** worm **4** hacker
5 browser hijacker **6** malware attack
7 adware **8** Trojan

Speaking

3 If students have not experienced a computer security threat themselves, ask them to talk about stories of computer attacks they have heard from friends and colleagues or read about in newspapers. Ask students to use the terms from Exercises 1 and 2. You could also point out that the present perfect can be used to talk about experiences (for example, *I've had a virus on my laptop.*) If you asked students to find a news story about a threat to IT security that involved a virus, you could ask them to share what they found out at this point.

4 Ask students to discuss solutions to the problems they identified in Exercise 3. Students may suggest some of the following solutions:

- Download software from a verified source.
- Check your system on a regular basis.
- Make sure your antivirus is updated daily.
- Always check external drives for viruses before transferring files.
- Make sure incoming email is always scanned for malware.
- Don't purchase things online through unknown or unverified websites.
- Don't share your passwords with anyone.
- Follow IT security and safety procedures at work.

Vocabulary

5 Go through the security solutions on the left and see if students can provide explanations of the terms themselves before doing the matching activity. After checking the answers, go through the words and phrases to practise the stressed syllables (1 ***fire****wall*; 2 ***an****tivirus* ***soft****ware*; 3 *authenti****ca****tion*; 4 ***u****sername*, ***pass****word and bio****me****tric* ***sca****nning*; 5 *en****cryp****tion*).

2 a **3** c **4** b **5** d

Listening

6 ▶ 48 Play the recording straight through once to give students the opportunity to get a general understanding of the conversation. Ask them what Ludek's problem is (*His laptop is not working.*), then play the recording again. You could pause it in the middle if you think students won't have enough time to write in their answers.

1 Because nothing seems to work.
2 Because he hasn't backed it up.
3 He thinks the computer has (spyware or some other) malware on it.
4 Because an antivirus program may not catch everything.
5 Because it will protect the computer from hackers and piggybackers.
6 He will scan Ludek's system with his anti-spyware software.

Ask students to go to page 77 so they can read through the dialogue while listening a third time. As revision, ask them to underline the ways Ales gives advice (*You should install a good spyware doctor program. And why don't you protect your WLAN access with a password?*). Deal with vocabulary difficulties and point out the use of different tenses.

Language

Explain the use of *may*/*might* (*not*) in contexts that students will immediately understand. Make sure they are able to pronounce *might* correctly. Elicit some example sentences to check students understand the verbs' usage; this could be talking about the weather or a future football match, for example.

Speaking

7 Tell students that this discussion reviews the use of *should* for asking for and giving advice and also gives them the opportunity to use *may* and *might* in the context of protecting their computer. Write the problems identified in the reading in Exercise 2 on the board. Make sure both students in each pair get the opportunity to play the part of both the non-IT expert and the expert.

Workstation health and safety

Speaking

1 Ask students to look at the illustration on the page but with the advice in Exercise 2 covered. Students may suggest some of the following problems: headaches, sore eyes, back pain, a stiff neck, pain in the arms and fingers (an example of RSI, which stands for Repetitive Strain Injury). You may also want to teach the relevant parts of the body: *feet*, (*fore*)*arms*, *hands*, *back*, *fingers*, *eyes*, *shoulders*, *neck*, *thighs*, *legs.*

Vocabulary

2 Ask students to read the advice and deal with any vocabulary questions they may have. Then ask them to match the phrases with the correct part of the illustration in pairs.

1 d **2** e **3** h **4** f **5** b **6** g **7** c **8** a

Speaking

3 After students have discussed the three questions in pairs, ask them to report back to the whole class on what they said.

4 Ask students to make recommendations using *Make sure …* and the advice in Exercise 2 (for example, *Make sure your feet are flat on the floor. Make sure your shoulders are relaxed.*

Reading

5 Pre-teach the words *power surges*, *cleaner* and *polish.* Ask students to read through the rules in pairs. While they discuss the list of rules, go round the class and deal with any vocabulary problems individually. Note that Scandisk is a utility for Windows that checks and repairs files.

Vocabulary

6 Tell students that this activity practises and checks some key verb–noun collocations. They can do the activity in pairs or individually.

2 d **3** c **4** a/b **5** a/b

Speaking

7 Ask students to think of and write at least four rules for computer use. They may suggest some of the following ideas:

- Take a break every thirty minutes.
- Don't let your computer get too hot.
- Use cleaning tools appropriate for computers.
- Wipe your screen with a damp cloth only.
- Ask IT support for assistance before opening a computer.
- Follow maintenance recommendations.
- Secure all cables.

8 Ask students to refer to Exercises 2 and 5 when they answer the question.

Extra activity

Ask students to write and design (and if possible, illustrate) an A4 poster giving the most important health and safety points in their school, college or company.

Security procedures

Speaking

1 Ask students to do this activity in pairs and then to share their ideas with the class. Students may suggest some of the following security procedures, which have featured in one way or another in this unit and earlier ones: installing anti-virus software, creating a firewall, using passwords, backing up files. They may also suggest new procedures like reporting incidents, which is mentioned in Exercise 2.

Reading

2 Encourage students to do the matching activity without trying to understand every word in the text. When they have finished, deal with any vocabulary difficulties but, again, encourage students not to worry about every single word. Point out that *current* in the first paragraph means *up-to-date* in this context.

1 Safety security requirements **2** Password recommendations **3** Email and network usage **4** Data transfer and backup **5** Reporting IT security incidents

Vocabulary

3 Tell students that this activity practises some key verb–noun collocations. Encourage them to record word combinations such as these, not just individual words, when they record vocabulary.

2 b **3** c **4** a **5** f **6** e

Speaking

4 Ask students to discuss the two questions in pairs and to make sure they use the superlative form (for example, *The most* (or *least*) *important thing is only installing software that management has approved.*) Remind students to use the present simple to talk about habits (for example, *People sometimes do not report incidents.*).

Language

Read through the explanations and examples with the class. *Mustn't* and *shouldn't* have already been introduced in the course, so focus in particular on the new language, which is *you aren't allowed to …* and *you aren't permitted to … .* Do not teach the formation of the passive form – just teach these two items as set phrases. Point out that *you* refers to people in general.

Listening

5 ▶ 49 Play the recording and ask students to just listen. Point out the contracted forms. Then play the recording again and ask students to repeat the sentences.

Speaking

6 Tell students that they can refer back to the text in Exercise 2 on page 64 and to the text in Exercise 5 on page 63 for help with this activity. If students are from one school, college or company, you may want to research ahead what the local rules and recommendations are so that you can provide cues to the discussion if students have difficulty.

Writing

7 Ask students to do this activity in small groups. Alternatively, if time is short, set this activity as homework.

Extra activity

Ask students to use what they have written to create a leaflet giving the most important regulations in their school, college or company.

Reporting incidents

Speaking

1 Discuss the question as a class with books closed or with the reports from Exercise 2 covered. If students do not have experience of reporting an incident, ask them to suggest the kind of incidents that people should report. You could also ask them to think of situations where they did not report something they should have reported.

Reading

2 Ask students to read the reports and say if any of them refer to incidents that are similar to what you talked about in Exercise 1.

Speaking

3 To help students with the discussion, write *I think* on the board, followed by two example sentences to show that it can come at the beginning or end of the sentence (for example, ***I think*** *the teacher incident is the most serious one. The printer settings change is the least important incident,* ***I think***.). Stronger students may be able to justify their opinions using *because.*

Writing

4 Ask students to do this activity in pairs or small groups. The idea is to write a more detailed version of one of the reports in Exercise 2. Tell students that they should write two or three sentences giving a brief description of the incident, adding any extra information if necessary, and two or three sentences with recommendations on what action the IT department should take.

Extra activity

With a stronger class, ask students to swap reports and respond to them as the IT supervisor. They should respond stating if they agree or disagree with what has been written. If computers and email are available, the initial reports and replies from the IT supervisor could be sent via email.

Business matters

Reading

1 Before students do the activity, ask them to look at the two illustrations and identify one problem in each. This will give them a clear idea of what they are supposed to do. Then ask them to make notes on network security and health and safety problems.

Suggested answers
Network security: firewall? anti-virus/anti-spam software? email and web browser filter? back up for data or cloud storage? filtering software? username and password protection?
Health and safety in the workplace: inappropriate seating (no chairs with back support), food on tables, cups on the table with a spill, cup on a computer, hanging cables from the ceiling, kettle on the table, fan on the floor, untidy coffee table with food and CDs together, dartboard in dangerous position near filing cabinet

Speaking

2 Give students at least ten minutes to prepare and rehearse their presentations in their pairs, then ask them to present their recommendations to another pair or to small groups. Tell them that the presentations should not be longer than one minute for each part.

Write these phrases on the board to help students with their presentations: *We recommend …; QuickFix should …; First of all, …; Secondly, …; Finally, … .*