

7 Working online

Starting point

1 Which online mobile devices do you have with you all the time?

2 How important is it for you to be online 24/7?

3 How do you feel when you can't access the Internet and go online? Give reasons for your answer.

Working with words | Online security

1 Work with a partner and discuss these questions.

1 How secure is your computer and data?
2 How do you protect your documents and data?
3 What makes a password weak or strong?



2 Read this article. What is the writer's main purpose?

- To report examples of cybercrime in businesses.
- To convince businesses to invest in online security.
- To explain that online security is important for businesses.

How safe is your business?

Spamhaus is an international non-profit organization based in Switzerland. One day, without warning, the Spamhaus servers were compromised and the website was down for nearly a week. The organization had become another victim of a cyberattack.

For Spamhaus, the attack was especially bad because the organization manages databases of spammers and blacklisted users for business corporations, governments and Internet providers. In other words, Spamhaus had a special understanding of online security. But even it couldn't prevent the cybercriminals.

It's a warning to all organizations and businesses that they are vulnerable to such attacks. And yet, in a recent survey by Deloitte of almost 2,000 executives, 79% were not confident about their company's level of online protection but only 58% planned to increase spending on their cybersecurity. This is a surprisingly low figure considering the risks.

Hackers can spend an average of 243 days on the victim's network before the company realizes there's a problem.

According to a recent study by Mandiant, a provider of corporate cybersecurity systems, there are three reasons for the lack of spending. Firstly, hackers can spend an average of 243 days on the victim's network before the company realizes there's a problem. Secondly, cybersecurity is cost-saving but not money-making, so investors are less interested in paying for it. And finally, many companies feel that if they follow basic procedures such as regularly changing passwords and encrypting files, then they are safe and don't need to invest in more security. They'd prefer to wait and see.

Unfortunately, as businesses become more and more reliant on the Internet, how can businesses afford not to spend more on cybersecurity?

3 The writer thinks we should spend more money on online security. Discuss these questions with a partner.

1 How does the writer support this view in the article?
2 Do you agree? Do you think this is true for your company? Why/Why not?

4 Match these words from the article in **2** to definitions 1–8.

compromised *was down* *hacker* *encrypt* *prevent* *vulnerable* *network* *victim*

1 when a protected thing is no longer secure *compromised*
2 stopped working _____
3 person or organization who is attacked as a result of a crime _____
4 stop something from happening _____
5 weak or easily attacked _____
6 person who secretly looks at and changes information on a computer system _____
7 connected computers and devices for sharing information _____
8 make computer data impossible to read unless the user has a password _____

5 Have you or anyone you know ever been a victim of cybercrime? What happened? Why wasn't the data or identity secure?

6 ▶7.1 Listen to three people talking about online security. Match each person to the type of online security a–c.

Speaker 1: ___
Speaker 2: ___
Speaker 3: ___

a Regularly changing your log in details
b Making copies of documents and other data
c Checking for viruses

7 ▶7.1 Listen again. Match verbs 1–7 with nouns a–g.

1 upgrade	a data
2 back up	b files
3 encrypt	c documents
4 create	d scans
5 open	e attachments
6 share	f software
7 run	g a new password

8 Work with a partner. Make and ask each other questions with 'How often do you …?' and a verb and noun from **7**. Answer the questions and give reasons.

Example: ***A*** *How often do you upgrade your software?*
B *About once every three years because new software is expensive.*

» For more exercises, go to **Practice file 7** on page 118.

9 Work with a partner. Discuss and write a list of guidelines for people working online at your company.

Example: *To prevent hackers, create a new password once every three months.*

