5 IT security

FOUNDATION: Unauthorized access

Situation: You work in the IT department at Hoffman Auditing, a tax consultancy in Auckland, New Zealand. The company has discovered that several customer accounts have recently been hacked.
→ You write an email to your customers with advice on how to avoid cybercrime.

1 Identifying types of attack

Your department head gives a presentation to the company's senior managers about the hacks.

A 15 Listen to her presentation and match the hacking methods (1–6) with the PowerPoint slides (A–F).

1 phishing
2 worms
3 backdoors
4 man-in-the-middle
5 injection attacks
6 social engineering

- exploits flaws in database
- hides in files that seem normal
- installs software with hidden commands

A 5

- listens to communication between a user and the network
- monitors and records communication
- infects many users that work in cafés and on public Wi-Fi networks

B 4

- pretends to be from a trustworthy organization
- asks the recipient to click on a link
- links to websites that are infected with malware

C 1

- exploits weaknesses in people, not software
- hacker pretends to be a real customer
- persuades users to open an email they've been sent containing malware

D 6

- provides access to a network by bypassing normal authentication
- hides in inactive state and is very difficult to detect
- often starts via a trojan

E 3

- copies itself and spreads to other computers on a network
- sends sensitive documents back to the hackers
- uses network bandwidth to send information

F 2

TOOLBOX

authentication – *Authentifizierung*
to bypass – *umgehen*
to infect – *infizieren*
malware – *Schadprogramm(e)*
recipient – *Empfänger/in*
trojan – *Trojaner*

B 15 Listen again and complete the statements of caution that your manager uses. The first one has been done for you.

1 The findings show that our employees don't seem to *pay attention to* our warnings about cybercrime.
2 We send an information email to our employees each month. I can only repeat what we say there: ___ phishing. beware of
3 Our network monitoring team continues to ___ for worms. keep an eye out for
4 We continually ___ for communications that are going to unidentified locations. watch out
5 Many of our staff work in cafés, even though they have been told to ___ they use secure networks. make sure
6 These are hard to detect, so we ask employees to ___ anything that just doesn't look right. pick up on
7 Our employee training contains lessons on how to ___ social engineering. guard against

Exercising caution
Beware of ...
Guard against ...
Keep an eye out for ...
Pick up on ...

› *Grammar: Imperatives, page 162*

2 Warning employees about cybercrime

The IT department at Hoffman Auditing has created a cybersecurity FAQ page for its employees.

Match the situations (A–G) to the explanations (1–7) on the FAQ page.

Q: What should I do if I receive a suspicious email?

A: Report it as spam to the IT department (phishing@hoffman.co.nz) immediately.

There are many examples of emails that are untrustworthy or suspicious, some of them appear to come from trustworthy organizations. It is important that you watch out for small things that don't seem right. Beware of the following features of emails that are likely to be phishing emails.

Fake emails often ...	Explanations
A ask you for personal information.	1 A trustworthy organization will never threaten you via email.
B have some spelling and grammar mistakes.	2 The expected 'domain name' (i.e. hoffmann) and 'co.nz' are never separated by other words.
C address you as a 'valuable customer'.	3 Hoffman Auditing, for example, uses one logo and colour scheme in emails. Criminals often use badly-copied logos.
D ask you to click on the new 'Hoffman Software' site.	4 A trustworthy company will never ask you for anything personal via email.
E come from domain names such as 'hoffman.confirmdetails.co.nz'.	5 Spam mails are often sent by non-native English speakers. Spelling and grammar are often wrong.
F threaten to punish you if you don't follow a specific action.	6 There is no 'Hoffman Software' site. Criminals use fake company and department names similar to real ones.
G display a logo that is a different colour than normal.	7 A credible company will always refer to you by your first and last name and use your identification number.

3 Warning customers about cybercrime

Your manager asks you to write to Hoffman's customers with tips on how to guard against phishing emails.

Write an email to Hoffman's customers. Make sure you tell them what to do if they receive a suspicious email. Explain some of the things that Hoffman does to minimize the risk to customers.

Use the FAQ page and the language of exercising caution to help you. Make sure you tell them:
- to watch out for cybercrime but not panic
- how to identify a real email from Hoffman
- what to do if they receive a suspicious email that claims to be from Hoffman