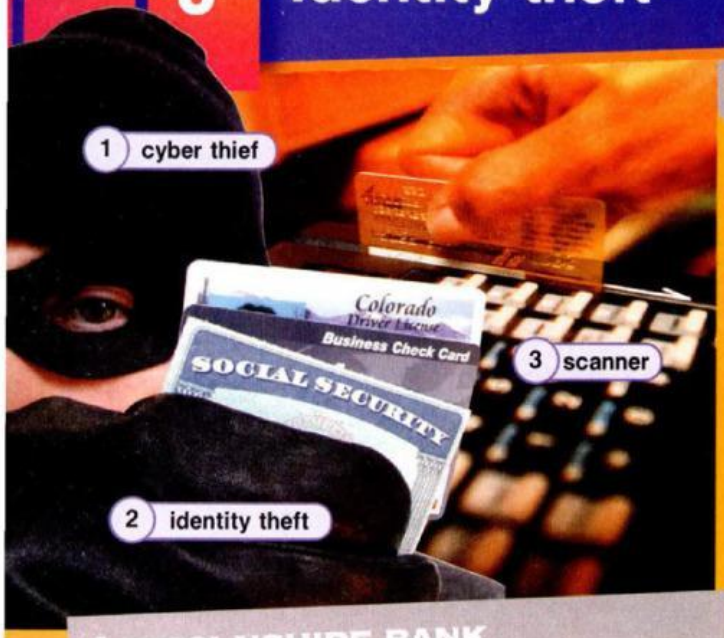
8 Identity theft



Get ready!

1 Before you read the passage, talk about these questions.

1 How does identity theft affect businesses?
2 How can people avoid falling for phishing schemes?

Reading

2 Read the letter from a bank to its customers. Then, mark the following statements as true (T) or false (F).

1 __ Pretexting occurs on telephones.
2 __ Pharming relies on the use of card scanners.
3 __ Trojan horses are spread by pharming sites.

LINCOLNSHIRE BANK
12345 Walker Avenue Albuquerque, NM 87444
505.555.8765

Dear Valued Customer,

Recently, a series of **identity thefts** has affected our customers. Unfortunately, this led to several instances of **fraud** occurring at our bank. The best way to avoid these events is to be informed. Please take a moment to familiarize yourself with some common ways that criminals steal personal information.

Card scanning is one simple form of identity theft. This is when someone uses a card **scanner** to record the information stored on credit or debit cards. Card scanning can be used to collect passport information as well.

Email also presents opportunities for **cyber** thieves. Spam, or unsolicited emails, can contain **malware**. This malicious software includes **spyware**, **Trojan horses**, and **worms** that can infect one's computer and steal information. **Phishing** is also conducted over email. This occurs when thieves trick people into giving them information by pretending to represent a legitimate business.

Pretexting is similar to phishing but is often done over the phone. **Pharming** occurs when a hacker redirects someone to a site operated by them. The site looks legitimate and tricks people into giving away personal information.

If you believe you may be the victim of identity theft, contact us immediately. We will take steps to ensure that your assets are safe.

Vocabulary

3 Write a word that is similar in meaning to the underlined part.

1 I had a lot of <u>malicious software</u> on my old computer.
_ _ l _ _ r _

2 You have a <u>malicious virus that seems beneficial</u>.
_ _ _ _ an _ _ r _ _

3 <u>Tricking people into giving information through email</u> is a serious crime.
p _ _ _ h _ _ g

4 <u>Stealing another's personal information</u> is on the rise.
i _ _ _ _ i _ _ _ h _ f _

5 It's a <u>program that gathers personal information</u>.
_ p _ _ _ _ e

6 <u>Capturing information stored on cards</u> is a new form of stealing.
_ _ _ d _ c _ _ _ _ n _

7 <u>Using a legitimate-looking website to trick people</u> fools many people.
p _ _ _ m _ _ _

4 Fill in the blanks with the correct words from the word bank.

WORD BANK

fraud pretexting cyber worm scanner

1 The man on the phone was part of a _____ scam.
2 I got a _____ in my email and now my computer won't work.
3 The criminal used a _____ to steal the information on her card.
4 The man was arrested and went to jail for committing _____.
5 Avoid _____ crime by being safe on your computer.

5 Listen and read the letter from a bank to its customers again. Why is Lincolnshire Bank contacting its customers?

Listening

6 Listen to a conversation between a customer and a bank employee. Choose the correct answers

1 What is the customer calling about?
A closing her bank account
B reporting a phishing scam
C flagging her account activity
D changing her account information

2 What can be inferred about the woman?
A She receives phishing scams often.
B She has already contacted the police.
C She must call the bank to get money.
D She lost the money in her bank account in the scam.

7 Listen again and complete the conversation.

Employee: Oh! Did it ask you to give away any **1** _____ _____?
Customer: Yeah. It said that the bank **2** _____ _____ _____ my account details.
Employee: Did you email them that information?
Customer: No, I thought I should call the bank first. It seemed **3** _____.
Employee: Yes, Lincolnshire Bank would never ask for your account details via email.
Customer: That's what I thought, but the email **4** _____ _____ because it had the bank logo. It even linked to a site that looked official.
Employee: Well, some of these criminals are **5** _____ _____.

Speaking

8 With a partner, act out the roles below based on Task 7. Then, switch roles.

USE LANGUAGE SUCH AS:

I think I received a phishing scam.
Did you email them that information?
It even linked to a site that looked official.

Student A: You are talking to a bank employee. Ask Student B about:

- phishing scams
- what to do next
- your money's safety

Student B: You are a bank employee. Answer Student A's questions.

Writing

9 You are a bank employee. Use the letter and the conversation from Task 8 to write about identity theft (120-150 words). Talk about:

- *How criminals steal personal information*
- *How customers can protect their assets*

9 Preventative measures

From: **jared.greene@harper.com**
To: **allstaff@harper.com**

Dear Harper Company Staff,

By now, you are all aware of the recent **security** breach. The IT department has traced it to a **bug** in our browsers. This bug created an unwanted **backdoor** in the network, allowing **intruders** in. They installed **keyloggers** that track our passwords.

The IT department removed the keyloggers, and the software supplier is releasing a **patch** that will fix this error. We will inform you when this patch becomes available.

However, this provides a good opportunity to remind you of the measures we must take to make our network safer.

Remember, you must keep the **firewall** settings as strict as possible on your computer. This prevents **attacks** from hackers and keeps certain types of malware out of the system.

Be cautious when downloading files. Perform a virus scan on every email attachment. Also, enable your browsers to block **popups**. Otherwise, spyware can get on to your computer.

Only download company-approved programs to your computer. Unauthorized programs may contain Trojans that can do irreversible damage to our system. Please consult the IT department for a list of **authenticated** programs.

In addition, we will review our **audit logs** from now on. This is to make sure no one violates security **protocol**. Employees violating protocol will receive disciplinary action.

Jared Greene
Manager,
Harper Company

Get ready!

1 Before you read the passage, talk about these questions.

1 How do people keep their computers safe?
2 Why would a company worry about security?

Reading

2 Read the email about safety measures. Then, choose the correct answers.

1 What is the email mainly about?
- **A** improving security at the company
- **B** detecting keylogger programs
- **C** installing a patch on a web browser
- **D** punishing employees for violating security protocol

2 The company will monitor employees by ...
- **A** installing spyware.
- **B** performing virus scans.
- **C** reviewing the audit logs.
- **D** looking for authenticated programs.

3 What can you infer about Harper Company?
- **A** They have authenticated the patch.
- **B** They already have a virus scan program.
- **C** They allow many authenticated programs.
- **D** This is their first security breach.

Vocabulary

3 Match the words (1-8) with the definitions (A-H).

1	__ popup	4	__ audit log	7	__ protocol
2	__ bug	5	__ backdoor	8	__ intruder
3	__ security	6	__ patch		

- **A** set of rules
- **B** error in a program
- **C** unwanted advertisements on a web browser
- **D** someone who accesses a system without permission
- **E** safety of a computer system and its data
- **F** part of a program giving undesired access
- **G** record of who has used a computer and what they've used it for
- **H** code to fix errors in a program

4 Fill in the blanks with the correct words from the word bank.

WORD BANK

authenticate keylogger
attack firewall patch

1 Management has to _____ the program before you download it.
2 A(n) _____ will record your password.
3 Without antivirus software, computers are open to a(n) _____.
4 Put up a(n) _____ to keep hackers out of your computer.
5 Download the _____ to make the program work correctly.

5 Listen and read the email about safety measures again. What should users do when popups appear on a web browser?

Listening

6 Listen to a conversation between two employees at Harper Company. Mark the following statements as true (T) or false (F).

1 __ The antivirus software is causing the employee's problems.
2 __ The browser cannot access any online information.
3 __ The employee's firewall settings are too strict.

7 Listen again and complete the conversation.

Employee 1: None of my programs have online access.
Employee 2: What about **1** _____ _____?
Employee 1: The browser opens, but I can't access any websites. Most importantly, I can't use the email client.
Employee 2: That's a big problem.
Employee 1: I know. I think **2** _____ _____ _____ _____.
Employee 2: Are you sure? The company's **3** _____ _____ _____ is pretty powerful.
Employee 1: I know, and **4** _____ _____ _____ _____ _____.
Employee 2: Oh, the firewall. How high are your settings?
Employee 1: **5** _____ _____ _____ _____.
Employee 2: **6** _____ _____ _____. You need to lower the level if you want your programs to work.

Speaking

8 With a partner, act out the roles below based on Task 7. Then, switch roles.

USE LANGUAGE SUCH AS:

What about your browser?
How high are your settings?
You need to lower the level if you want your programs to work.

Student A: Your computer cannot access the Internet. Talk to Student B about:

- the problem
- what works on the computer
- firewall settings

Student B: You are Student A's coworker. Answer his or her questions.

Writing

9 You work in an IT department. Using the email and conversation from Task 8, write an email to your co-workers about security (120-150 words). Talk about:

- *What security measures there are*
- *What threats there are to computers*
- *How the company plans to monitor its employees on the Internet*