
Login
xxxxxx
Password
****_




depositphotos



Hackers and Viruses / Identity Theft

Units 7 & 8

MISSION STATEMENT

1. How do computer viruses impact business?

2. What should people do when their computers are infected?



Vocabulary

3 Match the words (1-7) with the definitions (A-G).

1 E piggyback
2 G hacker
3 F host
4 D overwriting virus
5 A anti-antivirus virus
6 C resident extension
7 B virus

A a virus that attacks anti-virus software
B a program file that installs itself without permission
C an add-on that makes a computer virus part of the host computer's operating system
D a virus that copies its code over and destroys the files of the original data
E to gain unauthorized access to a computer system by using the owner's connection
F a computer system that has a virus attached to it
G a person who illegally exploits computer hardware and software

LINCOLNSHIRE BANK

LOCAL MAN ARRESTED ON Hacking Charges

(Wilmington) – Donald Greene has been arrested by Interpol on computer hacking charges. Interpol claims that Greene, a computer **hacker**, planted **viruses** on unwitting **host** computers. It is thought that Greene used a method called "**piggybacking**" to gain access to computers when their owners **logged in**. This gave him access to the computer's protective firewall and allowed him to disable it.

Interpol says that Greene has done over $50 million in damage. Most of this damage was done when he used **overwriting viruses** to overwrite and destroy files on government computer systems. But Greene targeted home computers, too. For these, anti-virus software was unable to stop Greene's viruses because he included **anti-antivirus viruses** with them. These viruses essentially shut down anti-virus software. Greene is also alleged to have used **resident viruses**. These viruses **imbed** themselves in a file or disk drive. When **resident extensions** are included with them, they become a part of the computer's operating system. This makes them nearly impossible to get rid of. As with all viruses, Greene's viruses are said to have **replicated** themselves quickly to **infect** multiple computers.

6 infect

2 Read the newspaper article. Then, choose the right answers.

1 What is the article mainly about?

A new types of computer virus
B a man who is investigating viruses
C the capture of a man who used viruses
D a way to protect computers from viruses

2 Which type of virus was the most harmful?

A overwriting viruses
B anti-antivirus viruses
C resident extensions
D resident viruses

3 What can be inferred about resident viruses?

A They can disable firewalls.
B They aid hackers with piggybacking.
C They do less damage than anti-antivirus viruses.
D They do not always include resident extensions.

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

1 Email is used to contaminate computers with viruses.
i _ _ _ c _

2 Enter identification that allows one to use a computer first.
l _ _ _ n

3 Some viruses can make copies of themselves. r _ _ _ i _ _ t _

4 If the virus becomes a part of something else, it will be hard to delete. _ m _ _ _ s

5 Viruses that become part of files but do nothing until activated can go unnoticed for months.
r _ _ _ d _ _ t _ _ r _ s _ _

Listening

6 Listen to a conversation between an employee and his manager. Mark the following statements as true (T) or false (F).

1 T The manager read the newspaper article.

2 F Overwriting viruses destroyed the manager's files.

3 F The manager decides to purchase new anti-virus software.

7 Listen again and complete the conversation.

Employee: Have you seen this article in today's paper? The one about the **1** _____?

Manager: Yes, I have. What about it?

Employee: Well, I think the IT department needs to **2** _____ _____ _____.

Manager: Do you think our company is vulnerable to these types of attacks?

Employee: Definitely. The overwriting viruses he used could do incredible damage.

Manager: I see. How much damage are we talking about?

Employee: Greene did millions of dollars' worth of damage by **3** _____ _____. That could happen to us.

Manager: Something like that would **4** _____ _____ _____.

Employee: Exactly. I think these **5** _____ _____ and resident extensions are a problem, too.

Manager: Why's that?

Employee: Well, these types of viruses **6** _____ _____ in files and disk drives.

Speaking

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

USE LANGUAGE SUCH AS:

Have you seen this article in today's paper?

How much damage are we talking about?

Something like that would ruin the company.

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

- viruses
- potential damage

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



Write a letter

Writing

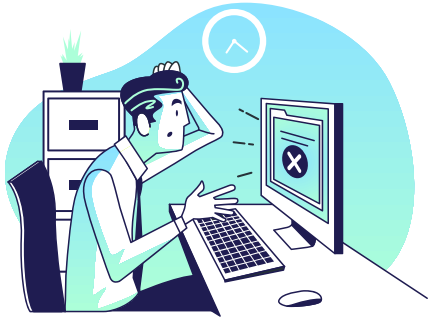
9 You are worried about computer security at work. Use the article and the conversation from Task 8 to write an email to your manager about (120–150 words). Talk about:

- *Why you are concerned about computer viruses*
- *Which types of computer viruses are most dangerous*
- *How computer viruses could harm the company*




Identity
Theft

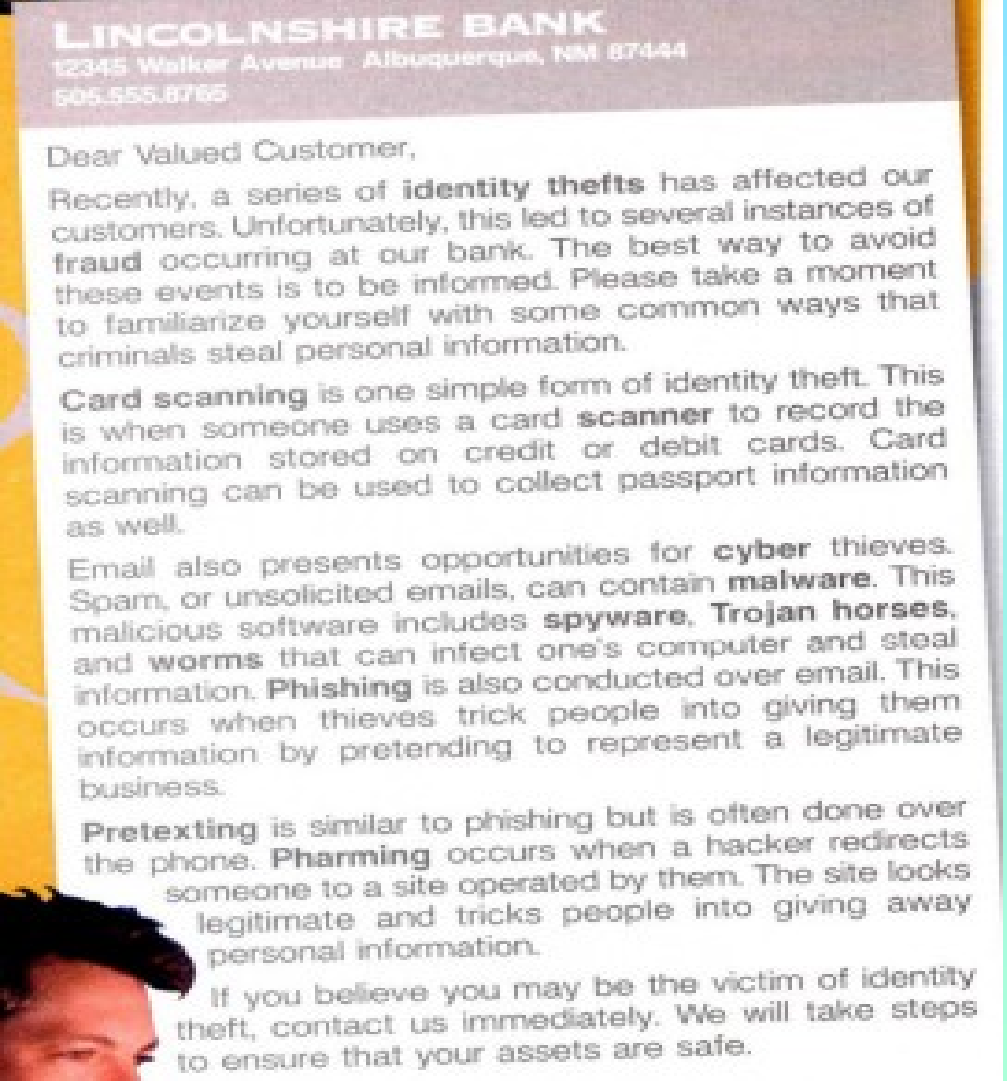
Discuss the questions



1. How does identity theft affect businesses?



2. How can people avoid falling for phishing schemes?



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.

Reading

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

1 T Pretexting occurs on telephones.

2 F Pharming relies on the use of card scanners.

3 F Trojan horses are spread by pharming sites.

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 pretexting scam.

2 I got a worm in my email and now my computer won't work.

3 The criminal used a scanner to steal the information on her card.

4 The man was arrested and went to jail for committing fraud.

5 Avoid cyber crime by being safe on your computer.

Vocabulary

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

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

2 You have a malicious virus that seems beneficial.
_ _ _ _ an _ _ r _ _

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

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

5 It's a program that gathers personal information.
_ p _ _ _ _ e

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

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



ing

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.

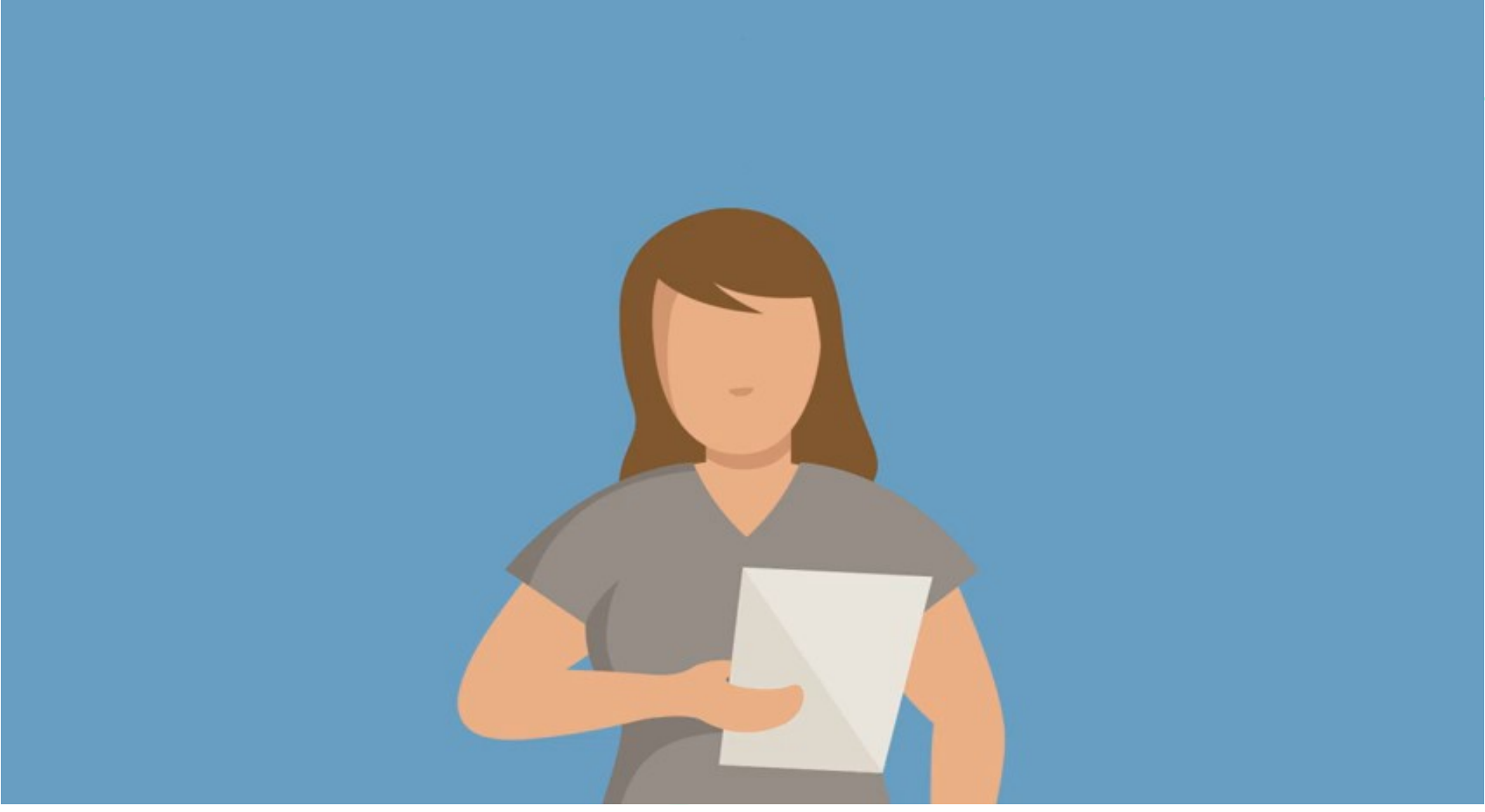
Employee: Did you email them that information?

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 time

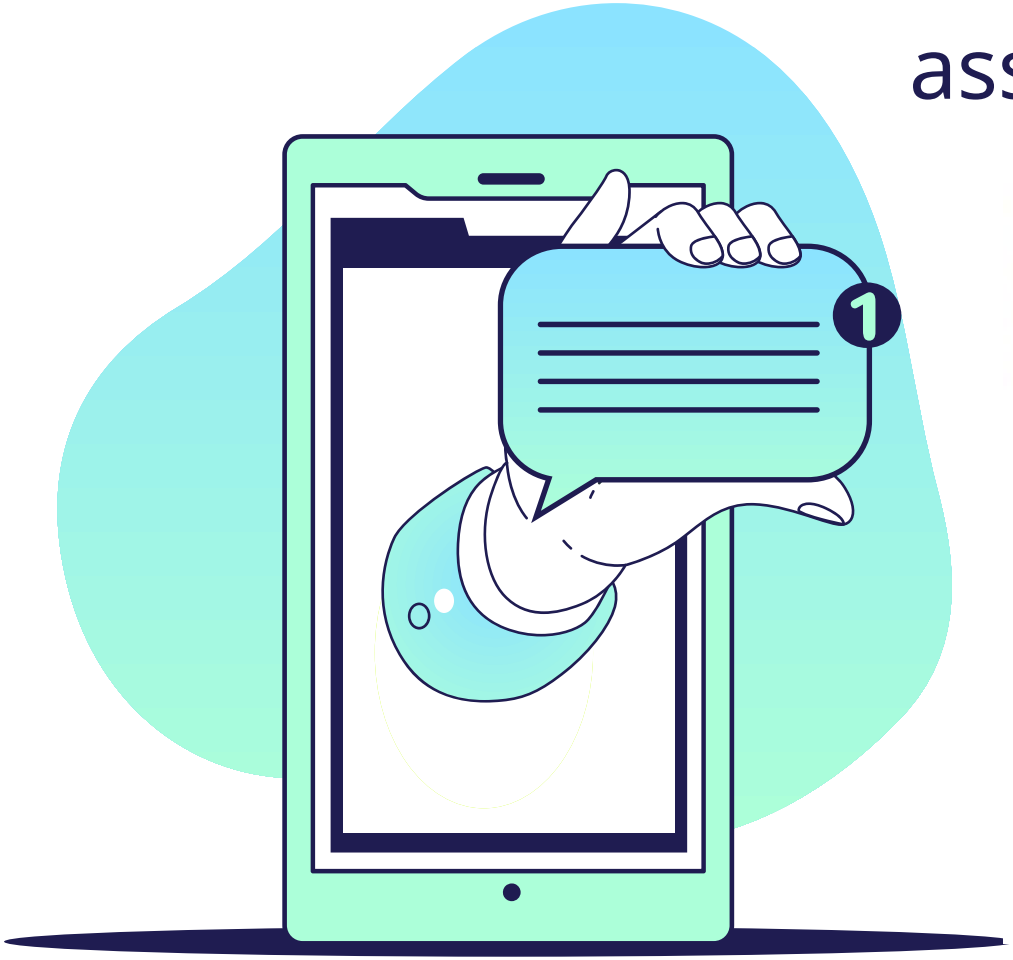
Work in pairs

Make up a dialogue

Act your dialogue out



Your home assignment



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*

ALTERNATIVE RESOURCES

