

Cyber Fraud

Identity theft occurs when a criminal uses a victim's personal information to establish new accounts in the victim's name.

According to a recent survey by Gartner, Inc., 3.6 million individuals in the United States were victims of phishing schemes, a type of cyber crime, in 2007. This is over a million more people than in 2006, for a total loss of \$3.2 billion dollars. As indicated by these statistics, the number of **cyber crimes**—crimes that rely on the Internet—is on the rise, and credit union members are often the targets. This chapter explains some of the methods cyber criminals use and details methods you can use to protect the credit union's members against cyber crimes.

Identity Theft

Identity theft occurs when a criminal uses a victim's name, Social Security number, credit card number, or other personal information to establish new accounts in the victim's name. Identity theft is different than transactional fraud, which involves the unauthorized use of a victim's preexisting credit card or other transactional documents to make purchases or to take cash advances.

The financial loss due to identity theft runs into the billions. According to an Experian-Gallup Personal Credit Index study conducted in October 2006, up to one in five consumers may be a victim of identity theft. In addition, identity theft costs American households \$5 billion annually and businesses \$48 billion annually; victims spend 30 to 60 hours and \$500 to \$1,200 resolving problems caused by

Objectives

Upon completion of this chapter, you will be able to:

1. Identify the behaviors that put members at risk of identity theft;
2. Recognize the steps involved in phishing attacks;
3. Explain how a computer contracts a virus;
4. Differentiate between pharming and phishing; and
5. Explain how malware invades a computer.

identity theft.

Many victims don't realize their identity has been stolen until they get turned down for credit or a job, or they start getting phone calls from debt collectors. Unfortunately, the same technology that has made financial transactions faster and easier, such as online-payment options, has also opened the door to acts of fraud like identity theft. Later in this chapter, we examine some of the ways criminals take advantage of technology to accomplish this fraud.

Identity Theft Can Happen to Anyone

Identity theft can happen to anyone and may take many different forms. The following two testimonies illustrate that everyone is at risk for identity theft. Michael's experience involves

Many people put themselves at risk for identity theft without realizing it.

low-tech identity theft, and Jessica's experience involves high-tech identity theft.

Michael: My wife passed away in 2003. About six months after her funeral, I started receiving a cell phone bill in her name. I immediately went to the cell phone vendor and to the police. It turned out a neighbor had taken my wife's maiden name and address from the funeral announcement in the newspaper. That information was enough to open a new cell phone account in my wife's name. While I spent several hours of frustrating phone calls with the cell phone vendor and the police to get the problem resolved, the police said I was actually relatively lucky.

Jessica: I used to work at a financial institution. I never worried about checking my e-mail at work or downloading attachments from friends and acquaintances, until one day when we got a call from the FBI.



They had discovered that our members' personal information was being traded in online chat rooms. It turned out that an attachment downloaded by an employee had a virus in it. The virus collected our members' financial information and transmitted it to hackers, who sold the information online. The buyers used our members' personal information to open new accounts in their names. Many of our members closed their accounts after that.

Risky Behavior

Many people put themselves at risk for identity theft without realizing it. Improper disposal of credit card statements, for example, can increase one's vulnerability to fraud. Risky behaviors involve the use of computers and technology and include the following:

- Failing to protect an ATM card PIN at a store or an ATM machine;
- Making purchases on an unsecured Internet site;
- Making online transactions that require a Social Security number;
- Using Web browser auto-complete functionality, which retains usernames, passwords, addresses, and credit card numbers in the computer;
- Failing to secure a computer against malware, or using an outdated or insecure Web browser;
- Using a public computer to make online transactions;
- Opening e-mails or e-mail attachments from unknown sources;
- Improper disposal of credit card statements, credit card offers, and

Safeguarding one's Social Security number is crucial to avoiding identity theft.

- other financial papers; and
- Failing to check one's personal credit report at least once per year.

Minimizing Risk of Identity Theft

The risk of identity theft cannot be eliminated entirely, but it can be minimized. For example, everyone should carefully review their personal account statements, shred financial statements before discarding them, and review their credit reports annually. Personal computers should be protected to reduce the risk of identify theft. The following can minimize fraud:

- Install, run, and update anti-virus software;
- Use secure Web sites for transactions and shopping;
- Avoid downloading programs from unknown sources;
- Disconnect computers from the Internet when working offline;
- Turn computers off when not using them; and
- Install a firewall on computers.

Social Security Number Precautions

Safeguarding one's Social Security number is crucial to avoiding identity theft. The following precautions should be taken with Social Security numbers:

- Don't carry your Social Security card in your wallet.
- Don't use any part of your Social Security number as a PIN or password.
- Don't include your Social Security number on your driver's license.
- Don't allow clerks to write your Social Security number on checks.
- Never give out your Social Security number unless it is necessary.

Try activity 2.1 to see how well you understand identify theft risks and prevention.

Spoofing and Phishing

Cyber crimes often involve spoofing and phishing schemes. **Spoofing** occurs when a spoofer uses identification and authentication data to mimic

Activity 2.1

Identify Theft Acumen



See if you understand what increases and decreases your risk for identify theft. Fill in the blanks for each statement.

1. _____ occurs when a criminal uses a victim's name, Social Security number, credit card number, or other personal information to establish new accounts in the victim's name.
2. Identity theft is different than _____, which involves the unauthorized use of a victim's pre-existing credit card or other transactional documents to make purchases or to take cash advances.
3. Making purchases on an _____ Internet site puts a consumer at risk for identity theft.
4. Installing a _____ on computers is one way to lower the risk of identity theft.
5. Safeguarding one's _____ is crucial to avoiding identity theft.

Answers appear in appendix A.

a legitimate organizational Web site. Phishing is one type of spoofing. Phishers use spoofed Web sites to fraudulently acquire personal information, such as usernames, passwords, and credit card details. Phishers might secure the e-mail accounts of the members of a financial institution or another organization. Members are then sent e-mails directing them to enter or update their personal information on a site that mimics that of the organization. The phishers harvest this information for sale or personal use.

Phishing from Afar

Once phishers acquire members' sensitive personal information, they often sell it over the Internet to crimi-

nals. These criminals use it either to access a victim's existing accounts or to open new accounts in the victim's name. Phishing poses a special problem for law enforcement officials because phishers often operate in organized crime units based overseas. See an example of phishing in Figure 2.1

For information on what personal information fetches on the black market, see the table in figure 2.2.

What You Can Do

Financial institutions, including credit unions, are increasingly becoming targets of phishing. Unfortunately, the phisher solicits the credit union member directly, and the credit union can't prevent phishers from targeting its members. What the credit union

Figure 2.1

How to Spot a Phishing Attempt

Here is an example of a phishing e-mail. Notice that the e-mail link displayed in the e-mail is not where you are directed. By clicking on the link, the user is actually directed to a false Web site.

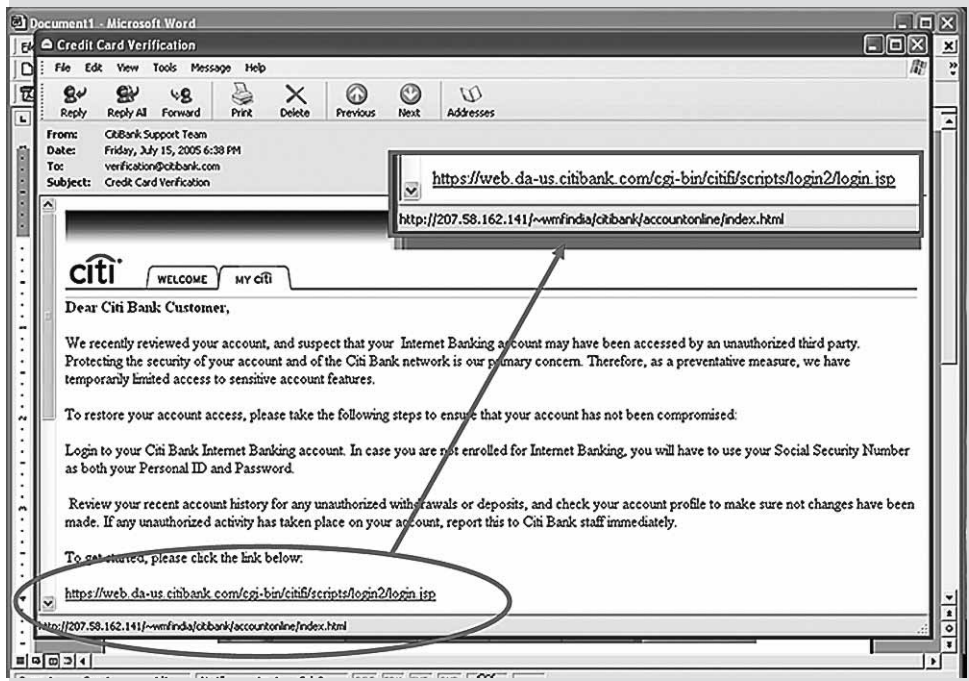


Figure 2.2

Your Information
for Sale

Advertised Prices of Items Traded on Underground Economy Servers

Item	Advertised Price (in U.S. Dollars)
United States–based credit card with card verification value	\$1–6
United Kingdom–based credit card with card verification value	\$2–12
An identity (including U.S. bank account, credit card, date of birth, and government-issued identification number)	\$14–18
List of 29,000 e-mails	\$5
Online banking account with a \$9,900 balance	\$300
Yahoo! Mail cookie exploit—advertised to facilitate full access when successful	\$3
Valid Yahoo! and Hotmail e-mail cookies	\$3
Compromised computer	\$6–20
Phishing Web site hosting—per site	\$3–5
Verified PayPal account with balance (balance varies)	\$50–500
Unverified PayPal account with balance (balance varies)	\$10–50
Skype account	\$12
World of Warcraft account—one month duration	\$10

Source: Symantec Corporation

can do is help protect members from becoming victims of identify theft by increasing their awareness of phishing. The credit union can also assist members who find they are victims of a phishing attack.

As a credit union employee, you should take every opportunity to educate members about phishing attacks. Teach members how to identify secure sites, and remind them never to give out personal information solicited by e-mail or the Internet. If members know that the credit union won't ask them for personal information through these channels, they're less likely to fall for phishing attempts in

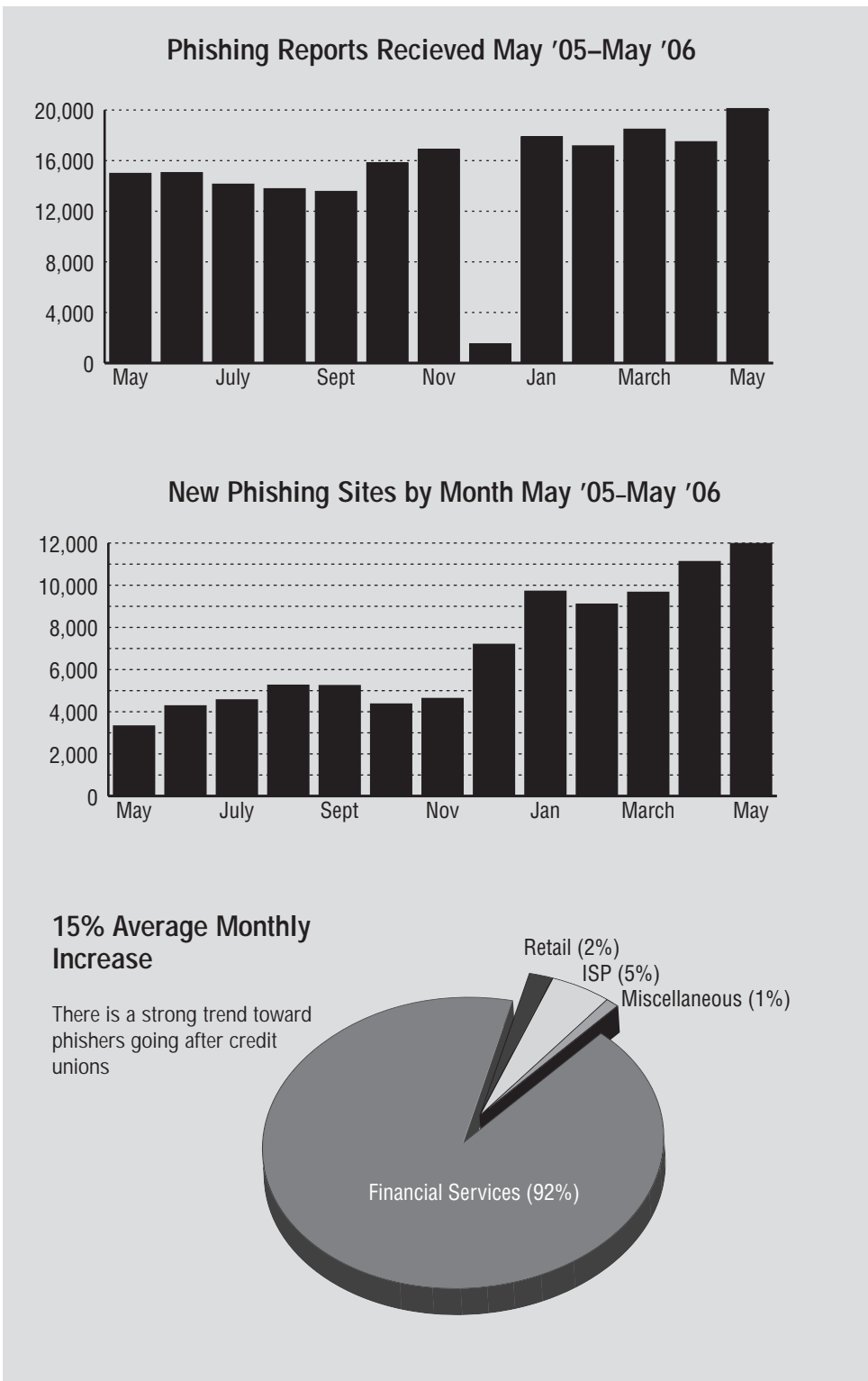
the first place. Try recalling the steps involved in a phishing attempt and refer to figure 2.3 to see how these crimes have increased over time.

Viruses

Some cyber criminals use computer viruses to obtain sensitive information and steal identities. A **virus** is a program that can infect a computer without permission or knowledge of the user. Once it infects a computer, the virus duplicates itself and uses the computer to attempt to infect other computers. Computer viruses are transmitted in a variety of ways. Viruses can be transmitted using **Web**

Figure 2.3

Phishing Trends



Activity 2.2**When One Goes Phishing**

Following are the steps involved in a phishing attack. Put the steps in order by placing the numbers 1–5 in the blank space.

- _____ Unsuspecting credit union members enter their sensitive information on the phony Web site.
- _____ Organized crime unit of phishers creates Web site that looks exactly like your credit union's Web site.
- _____ Criminals who purchase the members' information use it to open new accounts in member's name.
- _____ Phishers sell members' sensitive information on the black market for a profit.
- _____ Phishers send out e-mail requesting information updates to credit union members with a link to the phony site.

Answers appear in appendix A.

browsers, e-mail messages, storage media such as CDs and USB drives, and network connections. In all cases, the virus file must be moved onto a computer for that computer to become infected. Since viruses can spread by infecting files on a network file system, or a file system that is accessed by several computers, computers are at risk if any computer on the network becomes infected.

Financial Risks of Viruses

Each virus orchestrates a particular kind of attack. Some viruses destroy files. Other viruses destroy a computer's hard drive. Viruses are dangerous to credit unions because they have the ability to damage files, computers, and networks.

Viruses threaten the way a credit union does business on a daily basis. If a virus destroys a file that contains valuable information, the credit union must spend time retrieving that information. If a virus destroys a computer's hard drive, the credit union must

replace it. In addition, if a virus infects one computer on its network, the credit union might be forced to shut down the entire network to stop the infection from spreading. In each case, the result is lower efficiency and lost productivity while the credit union recovers from the virus attack.

Avoiding Computer Virus Infections

The following scenario, in which two credit union employees react to a potential computer virus, illustrates the importance of using safe practices to avoid computer virus infections:

Chad: Hey, Mary, did you get that e-mail about a free laptop?

Mary: I saw that, yes. I figured it was probably **spam** and deleted it without opening it.

Chad: I just opened that e-mail and downloaded the attached offer, and let me tell you, it sure looked like a scam to me!

Mary: You opened that here at work and downloaded the attachment?

Activity 2.3**Viruses
Don't Leave
Breadcrumbs**

It's important to know how computer viruses are contracted in order to protect yourself and members. Identify each statement about virus travel as True or False.

- _____ 1. Once it infects a computer, a virus duplicates itself and uses the computer to attempt to infect other computers.
- _____ 2. Computer viruses are transmitted in one way: via e-mail messages.
- _____ 3. A virus file must be moved onto a computer for that computer to become infected.
- _____ 4. Viruses are capable of destroying files and hard drives, but in general, they pose little threat to networks.
- _____ 5. If a computer has been infected by a virus, the user will immediately know.

Answers appear in appendix A.

Malware is especially dangerous because of the ease with which it infects computers.

Chad: Sure. Somebody says they want to offer me a free laptop, I have to at least read the offer, right?

Mary: Chad, you should never open any e-mails that appear to be scams. And you should never download attachments, even from your friends, without running a virus scan first. They might contain computer viruses, which can infect your computer.

Chad: I could infect my computer by opening an e-mail or downloading an attachment? But I would know if my computer got infected.

Mary: Actually, your computer might not seem any different. And these viruses can damage our computers and our files, and make it impossible for us to do business. If your computer has a virus and you connect to the network and share files with other users on the network, that virus can replicate and spread through the whole network. The network could be shut down, and we wouldn't be able to communicate or share information using

the network.

Chad: Well, I think I better go disconnect my computer from the network and run a virus scan.

Mary: Good idea.

You can avoid contracting a computer virus by taking the following precautions:

- Never open an e-mail from an unknown source.
- Never download an attachment from an unknown source.
- Scan all files and attachments from known sources with **anti-virus software** before downloading them.
- Disconnect your computer from the Internet when not in use.
- Run an anti-virus software program on your computer.
- Update your anti-virus software program frequently.

See if you know what viruses are and are not capable of by completing activity 2.3.

Pharming

Another method that cyber crimi-

It's important to avoid malware infections on personal computers and to protect credit union computers from malware threats.

nals use for identity theft is pharming. **Pharming** is similar to phishing, but it occurs on a larger scale. Like phishing, pharming puts victims at risk for identity theft. Pharming occurs when a person accurately types in a Web address but is redirected to a site that mimics the legitimate site. For example, users might enter the URL for their credit union only to be directed to a phony Web site controlled by the attacker. Unlike phishing, where users are directed to a phony site one at a time by e-mail, pharming allows an attacker to collect personal information from a large number of users.

How to Protect Yourself

Protecting yourself from pharming is not always easy. The site you're visiting must have a security certificate for you to be sure it is legitimate. If you

visit a site with a security certificate, a dialog box will pop up, asking you whether to trust the certificate. The name on the certificate should match the site you're trying to visit. If it does, you're safe from pharming.

Try your hand at comparing phishing and pharming scemes in activity 2.4.

Malware

A number of cyber crimes involve the use of malware. **Malware** is a generic name for any malicious software that gets downloaded onto a computer. Malware usually has a more sophisticated and broader purpose than a computer virus. Malware does not intentionally destroy a computer or its operating system. Rather, malware attempts to operate without detection on the computer. Malware programs are used for the following

Activity 2.4

Phishing vs. Pharming



Reflect on what you've learned about phishing and pharming. Write your short-answer response to each question below.

1. How is pharming similar to phishing?

2. How does pharming differ from phishing?

3. How can users protect themselves against pharming?

Suggested answers appear in appendix A.

purposes:

- Gather sensitive information and relay it back to the attacker;
- Use the infected computer to forward spam;
- Capture the personal information of those who use the infected computer; and
- Allow the attacker to remotely control the infected computer.

How Malware Infects

Malware is especially dangerous

because of the ease with which it infects computers. There are many ways in which malware can infect a computer. E-mailing and Web surfing are the most common ways for a computer to contract a malware infection. You don't even have to open an e-mail or download an attachment for your computer to become infected. Simply visiting a malicious Web site can infect your computer with malware. One estimate suggests that, in companies with 500 or more employees, 30 per-

Activity 2.5

Your Malware Savvy



Now that you've learned several characteristics of malware, select the best response for each of the questions below.

1. Malware can be defined as:
 - a. any malicious software that gets downloaded onto a computer.
 - b. a program that can infect a computer, then duplicate itself, and use the computer to infect other computers.
 - c. a specific program used for spoofing.
 - d. a malicious Web site used to fraudulently acquire personal information.
2. Which of the following is not a purpose of various malware programs?
 - a. using the infected computer to forward spam
 - b. capturing the personal information of those who use the infected computer
 - c. allowing the attacker to remotely control the infected computer
 - d. destroying the operating system of the infected computer
3. According to one estimate, what is the most common cause of malware infections?
 - a. general e-mailing
 - b. Web surfing
 - c. opening e-mails from unknown sources
 - d. downloading e-mail attachments
4. How can malware be eliminated?
 - a. running virus scans
 - b. only visiting necessary Web sites
 - c. using malware detection software
 - d. not opening e-mail attachments

Answers appear in appendix A.

When encounters with malware are so frequent, it's hard to avoid the occasional infection.

cent incurred malware infections through simple Web surfing, while 20 to 25 percent incurred malware infections through e-mail.

Protecting Credit Union Members

It's important to avoid malware infections on personal computers and to protect credit union computers from malware threats. Malware puts the sensitive financial information of all credit union members at risk. In the following scenario, two credit union employees discuss avoiding malware and protecting their members:

Chad: Hey, Mary, did you remember it's Rafael's birthday tomorrow?

Mary: No, but thanks for reminding me. I'll send him an e-card tomorrow morning.

Chad: I wouldn't do that if I were you.

Mary: Why not?

Chad: After our conversation the other day, I decided to learn more about computer security. I don't want to be the one to shut our system down or compromise our members' sensitive financial information.

Mary: Of course not. But what's that got to do with sending Rafael an e-card?

Chad: Malware can infect your computer just through Web surfing. If you visit a malicious site, your computer can get infected. And you wouldn't even know it. Malware that captures the keystrokes we enter while working or captures screenshots of member information could seriously compromise our members

and put them at risk of identity theft.

Mary: I had no idea that just using a Web browser was so dangerous!

Chad: To be safe, I'm not going to visit any Web sites that I don't need to visit for work. Like I said, I don't want to be the person to compromise our members' financial security.

Mary: I'll follow your lead on this one, Chad. Thanks for the information. I guess I'll stop by the card shop on my way home tonight instead.

Eliminating Malware

When encounters with malware are so frequent, it's hard to avoid the occasional infection. The good news is that there are programs available that detect malware and remove it from computers. An organization's information technology expert carefully selects malware detection software to protect system computers. Ask your information technology expert what programs your organization uses to detect malware and use activity 2.5 to test your own knowledge of malware.

Conclusion

Cyber criminals use a variety of methods to access credit union networks to steal members' information. This chapter introduced a number of these methods, as well as precautions that can be taken to secure sensitive information and protect organizations' computers and networks.

Identity theft can happen to anyone, but certain activities, especially those

PLAY PAGE



Matching Exercise

Test your understanding of cyber fraud by completing this matching activity.

Reminder:

To access the Play Page, go to <http://training.cuna.org/playpage/index.html> or go to www.cuna.org and type "Play Page" into the Search Box. Select the title of this module, and then the chapter you want to review.

involving computer use, can put a person at greater risk for this kind of fraud. Consumers should take certain steps to protect personal computers and minimize the risk of identify theft. And, it is especially important to take precautions to protect one's Social Security number.

Spoofing, which involves mimicking legitimate organizational Web sites, is one particular method cyber criminals use to acquire personal information. Phishing is a type of spoofing. Phishers secure the e-mail accounts of members of an organization and send them e-mails containing links to phony sites, where members are directed to enter or update their personal information. Often, this information is sold to criminals. The credit union can protect its members by educating them about phishing attacks.

Pharming, like phishing, involves Web sites that mimic legitimate organizational sites. Pharming redirects users to the phony site when users type in the URL. Thus, pharming enables the attacker to collect personal information on a larger scale than phishing. To guard against pharming, users

should check the security certificate of the site they are visiting.

Computer viruses are also a cyber threat to credit unions. When a virus infects a computer, it duplicates and can then be transmitted to other computers. Viruses can destroy files and hard drives or damage networks. To avoid computer viruses, credit union employees should never open e-mails from unknown sources or download attachments without first running a virus scan.

Malware, unlike viruses, does not intentionally destroy computers or networks. Instead, it attempts to operate undetected on computers in order to gather sensitive information. Web surfing can put a computer at risk for malware when the user visits a malicious site. Programs are available that detect and remove malware.

By using the information presented in this chapter to avoid computer viruses and malware and to take precautions against cyber crimes, such as phishing and pharming, you will be better equipped to protect the credit union and its members against cyber fraud and identity theft.