FEDERAL DEPOSIT INSURANCE CORPORATION

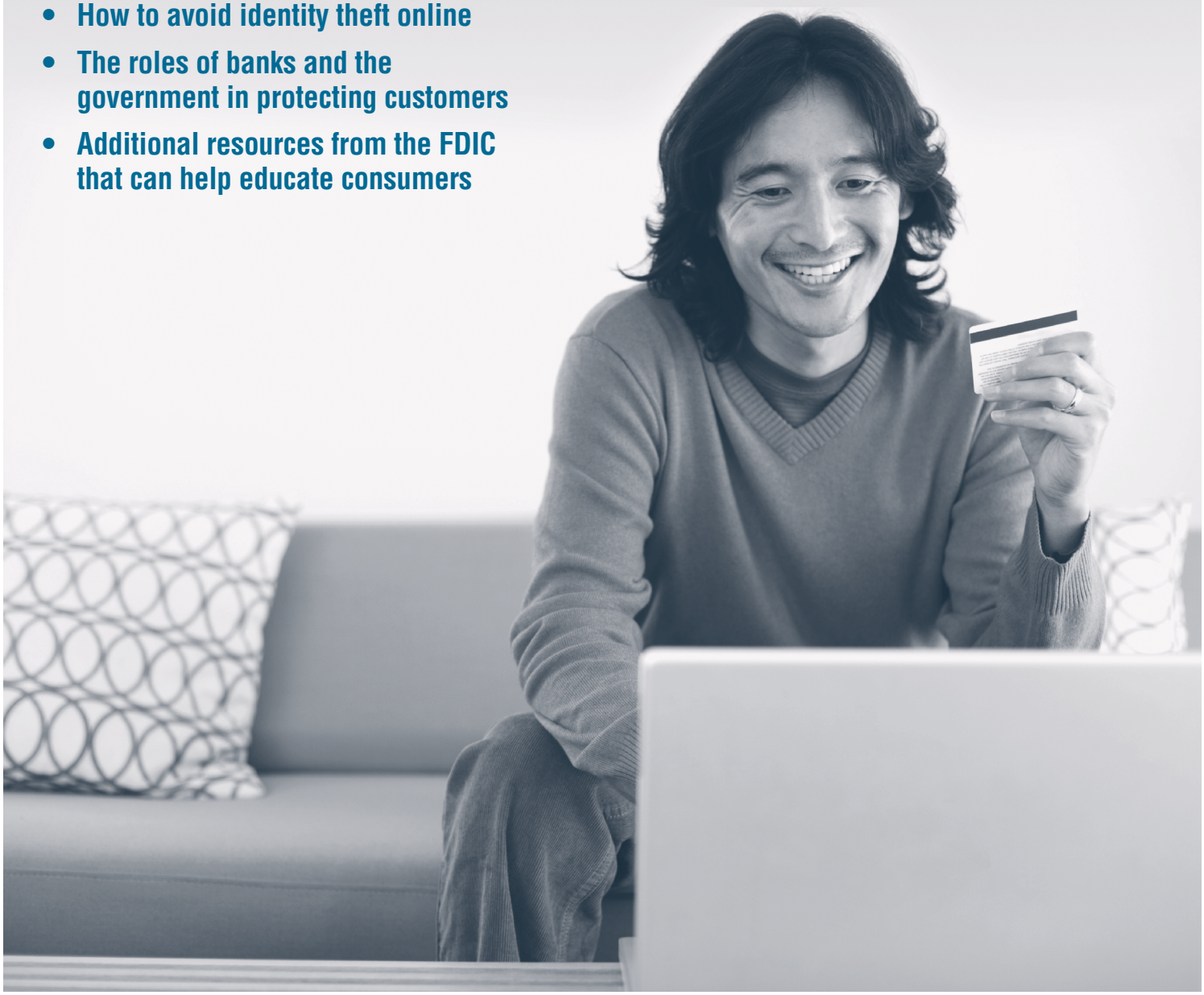
FDIC Consumer News

SPECIAL EDITION — Winter 2016

A Bank Customer's Guide to Cybersecurity

What Consumers Can Do ... and What Banks and Regulators *Are* Doing ... to Help Prevent Online Fraud and Theft

- **Safety precautions for Internet banking or shopping**
- **How to avoid identity theft online**
- **The roles of banks and the government in protecting customers**
- **Additional resources from the FDIC that can help educate consumers**



Protect Your "Cyber Home" With a Solid Foundation

Simple steps to secure your computers and mobile devices for Internet banking and shopping

Your home has locks on the doors and windows to protect your family and prevent thieves from stealing cash, electronics, jewelry and other physical possessions. But do you have deterrents to prevent the loss or theft of your electronic assets, including bank account and other information in your personal computers, at home and when banking or shopping remotely online?

"Think about all of the access points to and from your computer — such as Internet connections, email accounts and wireless networks," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "These always need to be protected. Otherwise, it's like leaving your front door wide open while you are away so that anyone could come in and take what they please."

Consider these strategies.

For Banking by Computer or Mobile Device

Take extra precautions for logging into bank and other financial accounts. These measures include using "strong" user IDs and passwords by choosing combinations of upper- and lower-case letters, numbers, and symbols that are hard for a hacker to guess. Don't use your birthdate, address or other words or numbers that can be easy for con artists to find out or guess. Don't use the same password for different accounts because a criminal who obtains one password can then log in to your other accounts. Keep your user IDs and passwords secret, and change them regularly. Make sure to log out of financial accounts when you complete your transactions or walk away from the computer.

Consider using a separate computer solely for online banking or shopping. A growing number of people are purchasing basic PCs and using them only for banking online and not Web browsing, emailing, social networking, playing games or other activities that are more susceptible to malicious software — known generally as "malware" — that can access computers and steal information. As an alternative, you can use an old PC for this limited purpose, but uninstall any software no longer needed and scan the entire PC to check for malicious software before proceeding.

Take precautions if you provide financial account information to third parties online. For example, some people use online "account aggregation" services that, from one website, can provide a convenient way to pay bills, monitor balances in deposits and investment accounts, and even keep track of your frequent flyer miles. While these websites may be beneficial, they can also present potential issues related to the security of the account information you have shared with them. If you want to use their services, thoroughly research the company behind the website, including making sure that you're dealing with a legitimate entity and not a fraudulent site. Also ask what protections the website offers if it experiences a data breach or loss of data.

Periodically check your bank accounts for signs of fraud. If you bank online, check your deposit accounts and lines of credit at regular intervals to spot and report errors or fraudulent transactions, just as you would review a paper statement. Online banking makes it easier and faster to monitor your accounts. This is important, because the sooner you can detect a problem with a transaction, the easier it should be to fix.

Federal laws generally limit your liability for unauthorized use of your debit, credit and prepaid cards, especially if you report the problem to your financial institution within specified time periods, which vary depending on the circumstances (see Page 8 for more details). A good rule of thumb is to check your accounts online once or twice a week. Also, many banks make it easier for customers to keep track of their accounts by offering email or text message alerts when balances fall below a certain level or when there is a transaction over a certain amount.

A Message to Readers

The Federal Deposit Insurance Corporation has been publishing ***FDIC Consumer News*** quarterly since 1993 to help people protect their money, including tips in practically every issue about how to avoid financial fraud and theft. A lot has changed over the years, especially consumers' increased reliance on computers and the Internet — the "cyber" world — for everything from shopping and communicating to banking and bill paying. While the benefits of faster and more convenient cyber services for bank customers are clear, the risks posed by these services, as well as the strategies for preventing or recovering from cyber-related crimes, may not be as well-known by the average consumer and small business owner.

That is why the FDIC has produced this special edition of our newsletter — a guide to safe online banking that features precautions to take at home and when banking remotely (using laptop computers, smartphones and other mobile devices). We include tips and information for parents and guardians wanting to protect their children from online fraud and identity theft, and for small businesses needing to secure their computer systems and data. You'll also learn about what banks and bank regulators are doing to protect your money.

Note: This and other issues of ***FDIC Consumer News*** can be read or printed at www.fdic.gov/consumernews. Check back there for versions of this issue for e-readers and portable audio (MP3) players. Single copies of this special edition and articles referenced here are available upon request to the FDIC's Public Information Center (toll-free 1-877-275-3342 or publicinfo@fdic.gov). Our publication also may be reprinted in whole or in part without permission.

Basic Security Tips

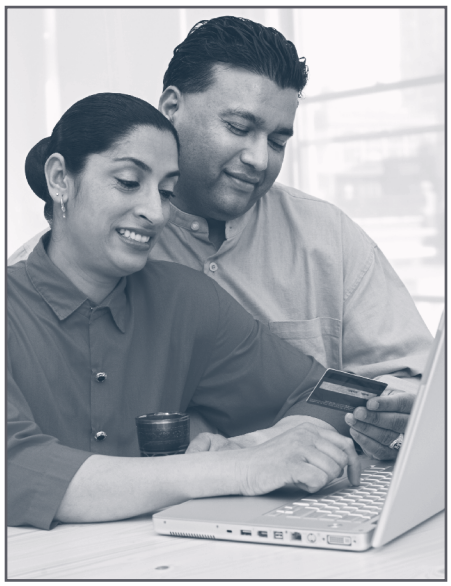
Keep your software up to date. Software manufacturers continually update their products to fix vulnerabilities or security weaknesses when they find them. "All of your software should be checked and updated as generally recommended by the manufacturer or when flaws are found," explained Kathryn Weatherby, a fraud examination specialist for the FDIC. "This advice goes for everything from your operating system to your word processing software, Internet browsers, spreadsheet software, and even your digital photography applications. A vulnerability in one piece of software, no matter how insignificant it may seem, can be exploited by a hacker and used as a pathway into your whole computer."

Some software manufacturers may issue "patches" that you need to install to update a program. Others may simply provide you with a completely new version of the software. "Before installing any update you receive, make sure it is legitimate, especially if it is emailed to you," said Benardo. "Check the software manufacturer's website or contact the company directly to verify the update's validity. Criminals have been known to imitate software vendors providing a security update when, in fact, they are distributing malware. Once you confirm that an update is legitimate, install it as soon as possible to correct whatever security flaw might exist."

Install anti-virus software that prevents, detects and removes malicious programs. Crooks and computer hackers are always developing new malware that can access computers and steal information, such as account passwords or credit or debit card numbers. These programs also may be able to destroy data from the infected computer's hard drive.

Malware can enter your computer in a variety of ways, perhaps as an attachment to an email, a downloaded file from an infected website, or from a contaminated thumb drive or disk. Fight back by installing anti-virus software that periodically runs in the background of your computer to search for and remove malware. Also be sure to set the software to update automatically so that it can protect you from the latest malware. For more information about malware, see Page 5.

Use a firewall program to prevent unauthorized access to your PC. A firewall is a combination of hardware and software that establishes a barrier between your personal computer and an external network, such as the Internet, and then monitors and controls incoming and outgoing network traffic. In simple terms, a firewall acts as a gatekeeper that helps screen out hackers, malware and other intruders who try to access your computer from the Internet.



Only use security products from reputable companies. Some anti-virus software and firewalls can be purchased, while others are available free. Either way, it's a good idea to check out these products by reading reviews from computer and consumer publications. Look for products that have high ratings for detecting problems and for providing tech support if your computer becomes infected. Other ways to select the right protection products for your computer are to consult with the manufacturer of your computer or operating system, or to ask someone you know who is a computer expert.

Take advantage of Internet safety features. When you are banking online, shopping on the Internet or filling out an application that requests sensitive personal information such as credit card, debit card and bank account numbers, make sure you are doing business with reputable companies. You also can have greater confidence in a website that encrypts (scrambles) the information as it travels to and from your computer. Look for a padlock symbol on the page and a Web address that starts with "https://." The "s" stands for "secure."

Also, current versions of most popular Internet browsers and search engines often will indicate if you are visiting a suspicious website or a page that cannot be verified as trusted. It's best not to continue on to pages with these kinds of warnings. Review your Internet browser's user instructions and explore the "tools" and "help" tabs to learn more about the security settings and alerts offered.

Be careful where and how you connect to the Internet. A public computer, such as at an Internet café or a hotel business center, may not have up-to-date security software and could be infected with malware. Similarly, if you are using a portable computer (such as a laptop or mobile device) for online banking or shopping, avoid connecting it to a wireless (Wi-Fi) network at a public "hotspot" such as a coffee shop, hotel or airport. Wi-Fi in public areas can be used by criminals to intercept your device's signals and as a collection point for personal information.

The bottom line, especially for sensitive matters such as online banking and activities that involve personal information, is to consider only accessing the Internet using your own computer with a secure, trusted connection, and to only connect laptops and mobile devices to trusted networks.

For more tips on computer and Internet security for bank customers, watch the FDIC's multimedia presentation "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams" at www.fdic.gov/consumers/consumer/guard. Also, visit www.OnGuardOnline.gov for information from the federal government on how to be safe online. The site includes videos from the Federal Trade Commission on what to do if your email is hacked or if malware attacks your computer.

Going Mobile: How to be Safer When Using a Smartphone or Tablet

Everywhere you look, people are using smartphones and tablets as portable, hand-held computers. "Unfortunately, cybercriminals are also interested in using or accessing these devices to steal information or commit other crimes," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "That makes it essential for users of mobile devices to take measures to secure them, just as they would a desktop computer."

Here are some basic steps you can take to secure your mobile devices.

Avoid apps that may contain malware. Buy or download from well-known app stores, such as those established by your phone manufacturer or cellular service provider. Consult your financial institution's website to confirm where to download its official app for mobile banking.

Keep your device's operating system and apps updated. Consider opting for automatic updates because doing so will ensure that you have the latest fixes for any security weaknesses the manufacturer discovers. "Cybercriminals try to take advantage of known flaws, so keeping your software up to date will help reduce your vulnerability to foul play," said Robert Brown, a senior ombudsman specialist at the FDIC.

Consider using mobile security software and apps to protect your device. For example, anti-malware software for smartphones and tablets can be purchased from a reputable vendor.

Use a password or other security feature to restrict access in case your device is lost or stolen. Activate the "time out" or "auto lock" feature that secures your mobile device when it is left unused for a certain number of minutes. Set that security feature to start after a relatively brief period of inactivity. Doing so reduces the likelihood that a thief will be able to use your phone or tablet.

Back up data on your smartphone or tablet. This is good to do in case your device is lost, stolen or just stops working one day. Data can easily be backed up to a computer or to a back-up service, which may be offered by your mobile carrier.

Have the ability to remotely remove data from your device if it is lost or stolen. A "remote wipe" protects data from prying eyes. If the device has been backed up, the information can be restored on a replacement device

continued on Page 9

What Banks and Bank Regulators are Doing to Protect Customers From Cyberthreats

In today's world, financial institutions must be aware of current cyberthreats and take appropriate precautions in order to protect their customers' money and personal information. "Banks are tempting targets for cyberthieves who want to commit financial fraud," said Jeff Kopchik, a senior policy analyst with the FDIC. "But what customers need to remember is that banks and regulators are working together to prevent these crimes."

Banks have employees or use outside firms that work to prevent cyberfraud. Also, financial institutions must continually improve their information security programs so they can effectively respond to the latest cyberthreats.

In addition, the FDIC and other regulators work with financial institutions to help protect customer information and money. Since 2001, federal law and regulations have required that financial institutions have programs to ensure the security and confidentiality of customer information. Federal and state bank examiners also regularly conduct on-site examinations of FDIC-insured institutions and their outside firms to ensure that they comply with these and other regulations.

Banking regulators also work with institutions to share overviews of the cyberthreat landscape and discuss steps they can take to be prepared. For example, in 2015, the FDIC produced an educational video on cybersecurity to help boards of directors and senior management at banks protect against potential threats. That same year, the regulators unveiled a voluntary "cybersecurity assessment tool" to help institutions identify risks and assess their preparedness.

"Banks may use any risk assessment tool they choose. FDIC examiners are available to discuss the results with bank management and help them focus on areas that need improvement," said Mark Moylan, FDIC deputy director for operational risk. "We view this communication as an important part of our strategy to help ensure the safety of customer financial information."

The FDIC also recommends that institutions join industry organizations that provide reliable and timely information designed to help institutions protect critical systems from cyber threats.

"Cybercriminals are constantly looking for new ways to commit financial fraud against a bank and its customers," Kopchik said. "That is why the FDIC devotes significant resources to financial institution compliance with federal information security laws and alerts bank management about the newest cyber threats and effective countermeasures. It's part of the FDIC's mission to maintain stability and public confidence in the nation's financial system."

Beware of Malware: Think Before You Click!

Malicious software — or "malware" for short — is a broad class of software built with malicious intent. "You may have heard of malware being referred to as a 'computer bug' or 'virus' because most malware is designed to spread like a contagious illness, infecting other computers it comes into contact with," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "And if you don't protect your computer, it could become infected by malware that steals your personal financial information, spies on you by capturing your keystrokes, or even destroys data."

Law enforcement agencies and security experts have seen an increase in a certain kind of malware known as "ransomware," which restricts someone's access to a computer or a smartphone — literally holding the device hostage — until a ransom is paid. While businesses have been targeted more than consumers to date, many home computer users have been victims of ransomware. For more information, see an alert issued by the U.S. Department of Homeland Security at www.us-cert.gov/ncas/alerts/TA13-309A.

The most common way malware spreads is when someone clicks on an email attachment — anything from a document to a photo, video or audio file. Criminals also might try to get you to download malware by including a link in the wording of an email or in a social media post that directs you somewhere else, often to an infected file or Web page on the Internet. The link might be part of a story that sounds very provocative, such as one with a headline that says, "How to Get Rich" or "You Have to See This!"

Malware also can spread across a network of linked computers, be downloaded from an infected website, or be passed around on a contaminated portable storage device, such as a thumb drive or flash drive.

Here are reminders plus additional tips on how to generally keep malware off your computer.

Don't immediately open email attachments or click on links in unsolicited or suspicious-looking emails. Think before you click! Cybercriminals are good at creating fake emails that look legitimate but can install malware. Either ignore unsolicited requests to open attachments or files or independently verify that the supposed source did send the email to you (by using a published email address or telephone number). "Even if the attachment is from someone you know, consider if you really need to open the attachment, especially if the email looks suspicious," added Benardo.

Install good anti-virus software that periodically runs to search for and remove malware. Make sure to set the software to update automatically and scan for the latest malware.

Be diligent about using spam (junk mail) filters provided by your email provider. These services help block mass emails that might contain malware from reaching your email inbox.

Don't visit untrusted websites and don't believe everything you read. Criminals might create fake websites and pop-ups with enticing messages intended to draw you in and download malware. "Anyone can publish information online, so before accepting a statement as fact or taking action, verify that the source is reliable," warned Amber Holmes, a financial crimes information specialist with the FDIC. "And please, don't click on a link to learn more. If something sounds too good to be true, then most likely it's fraudulent or harmful."

Be careful if anyone — even a well-intentioned friend or family member — gives you a disk or thumb drive to insert in your computer. It could have hidden malware on it. "Don't access a disk or thumb drive without first scanning it with your security software," said Holmes. "If you are still unsure, don't take a chance."

To learn more about how to protect against malware, visit www.onguardonline.gov/articles/0011-malware.

Beware of Phishing Scams: Don't Take the Bait

Identity thieves like to go "phishing" — pronounced "fishing" — on the Internet for consumers' personal financial information using fake emails and websites to trick people into providing Social Security numbers, bank account numbers and other valuable details.

Typically, the most common phishing emails pretend to be from a bank, a retail store or government agency to lure you into divulging personal financial information, and often use a variety of tricks to make the email look legitimate. They might include a graphic copied from a bank's website or a link that looks like it goes to a bank's site, but actually leads to a fake site.

Also beware of "pharming." In this version of online identity theft, a hacker hijacks Internet traffic so when you type in the address of a legitimate website you're taken to a fake site. If you enter personal information at the phony site, it is harvested and used to commit fraud or sold to other identity thieves.

Here are some tips to avoid becoming a victim of a phishing or pharming scam.

Be suspicious if someone contacts you unexpectedly online and asks for your personal information. It doesn't matter how legitimate the email or website may look. Only open emails that look like they are from people or organizations you know, and even then, be cautious if they look questionable.

For example, scam artists may hack into someone's email account and send out fake emails to friends and relatives, perhaps claiming that the real account owner is stranded abroad and might need your credit card information to return home.

Be especially wary of emails or websites that have typos or other obvious mistakes. "Because some requests come from people who primarily speak another language,

continued on the next page

Using Social Networking Sites: Be Careful What You Share

A lot of people use social media sites — such as Facebook, LinkedIn, Twitter, Google+ and Instagram — to stay in touch with family and friends, meet new people and interact with businesses like their bank. However, identity thieves can use social media sites in hopes of learning enough information about individuals to be able to figure out passwords, access financial accounts or commit identity theft.

Identity thieves create fake profiles on social networks pretending to be financial institutions and other businesses, and then lure unsuspecting visitors into providing Social Security numbers, bank account numbers and other valuable personal information. Identity thieves also have created fraudulent profiles and then sent elaborate communications to persuade "friends" to send money or divulge personal information. "They might claim to work at the same organization, to have attended the same school, or share similar interests and hobbies," said Susan Boenau, manager of the FDIC's Consumer Affairs Section. "They know that communicating a false sense of trust can be easy on social media."

"Valuable pieces of information to someone seeking to steal your identity include, for example, a mother's maiden name, date or place of birth, high school mascot or pet's name," explained Amber Holmes, a financial crimes information specialist with the FDIC. "Fraud artists use social networking sites to gather this kind of information because it can help them guess passwords to online accounts or answers to 'challenge questions' that banks and other businesses frequently use for a second level of authentication beyond a password. Someone who has your password and can successfully answer challenge questions may be able to access your accounts, transfer money or even reset passwords to something they know and you don't."

What safety measures can you take with your social media account?

Check your security settings on social network sites. Make sure they block out people who you don't want seeing your page. If you have doubts about your security settings, avoid including information such as your birthday or the year you graduated college. Otherwise, though, experts say it is OK to provide that kind of information on your social media pages.

Take precautions when communicating with your bank. If you want to communicate with your bank on social media, keep in mind that your posts could become public, even though you can protect your posts to some extent through your account settings. You should not include any personal, confidential or account information in your posts. "Also, reputable social media sites will not ask you for your Social Security, credit card or debit card numbers, or your bank account passwords," said FDIC Counsel Richard Schwartz.

Before posting information such as photos and comments, you should look for a link that says "privacy" or "policies" to find out what can be shared by the bank or the bank's social media site with other parties, including companies that want to send you marketing emails. Read what the policies say about whether and how the bank will keep personal information secure. Find out what options you may have to limit the sharing of your information.

It is a good rule of thumb to avoid posting personal information on any part of a bank's social media site. "That type of information is often requested by banks for their security 'challenge questions' that are used to control access to accounts," advised Schwartz. "A criminal could use that information to log in to your account."

Be cautious about giving third-party programs or apps, such as sites for games or quizzes, the ability to use information from your social networking pages. "Some of these third parties may use information from your page to help you connect with others or build your network — for example, to pair you with strangers wanting to play the same game," Boenau said. "But they could also be selling your information to marketing sites and others, possibly even to people who might use your information to commit a fraud."

Periodically search to see if someone has created a fake account using your name or personal information on social networking sites. Checking common search engines for your name and key words or phrases (such as your address and job title) may turn up evidence that someone is using your information in a dishonest way.

For more tips on avoiding fraud at social media sites, visit the Internet Crime Complaint Center website at www.ic3.gov/media/2009/091001.aspx.

Phishing Scams

continued from the previous page

they often contain poor grammar or spelling," said Amber Holmes, a financial crimes information specialist with the FDIC.

Remember that no financial institution will email you and ask you to put sensitive information such as account numbers and PINs in your response. In fact, most institutions publicize that they will never ask for customer personal information over the phone or in an email because they already have it.

Assume that a request for information from a bank where you've never opened an account is probably a scam. Don't follow the link and enter your personal information.

Verify the validity of a suspicious-looking email or a pop-up box before providing personal information. Criminals can create emails stating that "you're a fraud victim" or a pop-up box with another urgent-sounding message to trick people into providing information or installing malware (malicious software). If you want to check something out, independently contact the supposed source (perhaps a bank or organization) by using an email address or telephone number that you know is valid.

For more tips, see the federal government's OnGuardOnline page at www.onguardonline.gov/phishing.

For Parents and Caregivers: Tips for Protecting Your Child's Personal Information

Part of building a strong foundation for a child's financial future is taking steps to minimize the risk that his or her Social Security number, bank account details or other valuable personal information will be stolen. Here are tips to help parents and caregivers protect young people from cyber-related identity theft and financial fraud.

Talk with your child about safe online practices. Consider discussing the risks of sharing personal information online, including the possibility that someone can gather small amounts of personal information to guess the correct answers to security questions, reset passwords and take control of financial accounts.

"Encourage your young person to be selective with his or her 'friends' online, just as he or she would in real life," said Bobbie Gray, an FDIC supervisory community affairs specialist. "Discuss how not everything they see on the Internet is true, and that some criminals may pretend to be friends or relatives in order to obtain personal information or worse."

Consider agreeing on a short list of what your child can and cannot do online. For more information, read our tips for young adults in the Fall 2012 ***FDIC Consumer News*** (www.fdic.gov/consumers/consumer/news/cnfall12/avoidfraud.html).

Help your child learn to analyze advertisements, some of which may be fraudulent. "Explain that advertising, even in an online video clip, is intended to get people to make purchases or otherwise act on things they might not usually do," said Luke W. Reynolds, chief of the FDIC's Outreach and Program Development Section. The Federal Trade Commission (FTC) has an online game called "Admongo" (www.admongo.gov) to help youngsters age 8-12 think critically about advertising and make smarter decisions as consumers.

Explain why keeping money in a financial institution is safe. Checking, savings or other deposit accounts at a federally insured financial institution carry protections related to theft and fraud (see Page 8), making them a safe place for your money. If your child doesn't already have a deposit account, consider opening one. Learn about federal deposit insurance if a bank fails, including how to verify that a bank is FDIC-insured, by going to www.fdic.gov/deposit/deposits. And, to find age-appropriate information and activities for kids plus FDIC "Money Smart" guides that help parents and caregivers talk with their children about key financial topics, visit a website developed by the FDIC and the Consumer Financial Protection Bureau at www.consumerfinance.gov/parents.

Secure electronic equipment. Make sure your child's devices are configured to download the latest updates from the manufacturer because they usually include security-related enhancements. Almost all video game equipment connects to the Internet and may link to information such as credit or debit card numbers.

If a company wants to collect data on your child, find out why. Controlling access to a child's information is one of the best ways to protect him or her from identity theft. Under a federal law called the Children's Online Privacy Protection Act (COPPA), websites and online services (including apps) that are directed to children under 13 must notify parents directly and get their approval before they collect, use or disclose a child's personal information. When notifying you, the company must disclose how it plans to use your child's information. The company also may ask for your approval of different options for using information it wants to collect, such as whether it can share the information with others or use it for marketing purposes. To learn more, start at the FTC's Web page "Protecting Your Child's Privacy Online" (www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online).

Be aware of possible signs that a child is the victim of identity theft.

Criminals may steal the identity of children to file claims for government benefits or apply for a loan online. "While not necessarily a sign of identity theft, your child receiving unsolicited mail or phone calls from marketers can indicate that personal information has been shared somehow. It's best to take the time to understand why," Reynolds noted.

Consider asking the three major nationwide credit reporting agencies — Equifax, Experian, and TransUnion — to check if your minor child has a credit report. If the answer is "yes," review the report to find out if a thief has misused your child's name. For additional guidance, go to the FTC's "Child Identity Theft" page (www.consumer.ftc.gov/articles/0040-child-identity-theft#credit), which has contact information for the credit reporting agencies and tips if a child's identity has been stolen, including how to place a fraud alert in a credit report that can minimize future damage.

The FTC adds that it is generally a good idea for parents to conduct this review of credit reports close to a child's 16th birthday. Doing so allows time to fix errors or other problems before he or she might want to apply for a loan or a job.

For more information and tips on how to protect kids online, visit the federal government's OnGuardOnline website at www.onguardonline.gov/topics/protect-kids-online. The FDIC also has Money Smart guides that offer exercises, activities and conversation starters for parents and caregivers to help young people of all ages to learn about money (https://catalog.fdic.gov/store/youth).

How Federal Laws and Industry Practices Limit Losses From Cyberattacks

When criminals make unauthorized purchases using stolen payment card numbers or other information, federal consumer laws and financial industry practices protect victims from losses under certain circumstances. Here are key details to remember.

If your credit card number is accessed by cyberthieves: "Under federal law, a consumer's liability is normally capped at $50 for all unauthorized transactions on each card. However, if your credit card number is stolen, but not the card, you are not liable for any unauthorized use," said Richard Schwartz, a counsel in the FDIC's Consumer Compliance Section. "In addition, credit card losses are typically absorbed by the card issuer because of zero-liability policies, which preclude consumers from having to pay any amount of an unauthorized charge. These policies are set by the card industry."

If your debit card or the card number is used to withdraw money from a checking or savings account: To minimize your losses, you should contact your bank as soon as possible if you discover that your debit *card* has been lost or stolen. Your maximum liability under federal law is $50 if you notify your bank within two business days after learning of the loss or theft of your card. But if you notify your bank after those first two days, under the law you could lose more.

What if your debit card *number* (not the card itself) is stolen in an online hacking incident? Remember to check your account activity regularly. Timing is critical because under federal law you will not be liable for the transaction if you report it within 60 days after your account statement showing the transaction is sent to you. But if the charge goes unreported for more than 60 days, all your money in the account could be lost. However, remember to check with your bank about the payment card networks' zero-liability policy, which may protect you.

If you have a debit card for a business account that is used fraudulently: Debit cards issued for business use have different loss protections than debit cards for consumers. The Uniform Commercial Code (UCC), which sets many rules for businesses, requires a standard of "ordinary care" by the card holder in order to avoid liability for losses from online fraud. "This can be a technical area, so check with an attorney to make sure you are managing your business account consistent with the UCC rules," Schwartz advised.

If a prepaid card account is used fraudulently: Prepaid cards have money deposited onto them, and they usually aren't linked to a checking or savings account. In terms of legal protections against losses as a result of fraud, the rules vary depending on the type of prepaid card:

- Prepaid cards used by employers to pay their employees are covered under the same laws described earlier for consumer debit cards.

- General-purpose "reloadable" prepaid cards, which display a network brand such as American Express, Discover, MasterCard or Visa, currently have no protections limiting liability under federal law but do, in most cases, include in their contracts with customers the same protections as those for consumer debit cards. However, regarding liability for losses, the Consumer Financial Protection Bureau (CFPB) in November 2014 proposed a rule that would include reloadable prepaid cards under the federal law for consumer debit cards. Visit the CFPB website at www.consumerfinance.gov for updates.

- Prepaid gift cards for purchases at stores are typically not registered and, therefore, are not subject to federal consumer liability rights and protections. And, issuers of prepaid gift cards generally do not provide their own fraud liability coverage to card holders. "If you lose your gift card, you will probably lose the entire value of that card," Schwartz said.

To learn more about loss limitations under the law, search by topic at the websites of the CFPB and the Federal Trade Commission (www.ftc.gov). Also be aware that FDIC deposit insurance only covers deposits if a bank fails, not for theft from bank accounts (see below). For information about how to protect yourself from data breaches, which may involve the theft of credit or debit card information, see our Spring 2014 issue (www.fdic.gov/consumers/consumer/news/cnspr14/databreach.html).

Dear FDIC: Questions About Deposit Insurance and Online Banking

It appears that some FDIC-insured financial institutions pay higher interest rates on deposit accounts that are opened online. I would like to take advantage of these interest rates, but I have never banked online. Can an online account be FDIC-insured? If so, would FDIC insurance help me if there is a theft or other problem with an online transaction?

Most banks offer deposit accounts at their branches as well as online, and others only operate online — they have no physical offices where the public can open accounts or transact other business. In response to your first question, deposit accounts opened online at any FDIC-insured bank will be covered up to federal limits by FDIC insurance. "Deposit insurance coverage is the same for online-only banks as for brick-and-mortar banks," said Calvin Troup, an FDIC senior consumer affairs specialist.

The most important thing to confirm before working with an online bank is to make sure that it is a legitimate bank, and that you are not looking at a fictitious website. A bank can have one name that it uses for its traditional operations and a different name ("trade name") that it uses for marketing online. You can call the FDIC toll-free and ask to speak to a deposit insurance specialist who will help confirm if the online bank in question is FDIC-insured. The FDIC's online tool BankFind at https://research.fdic.gov/bankfind also provides useful information, such as headquarters locations and financial information, for all FDIC-insured depository institutions.

continued on the back page

Cybersecurity for Small Businesses: Ways to Stay Protected

In today's world, it's important for small business owners to be vigilant in protecting their computer systems and data. Among the reasons: Federal consumer protections generally do not cover businesses for losses they incur from unauthorized electronic fund transfers. That means, for example, your bank may not be responsible for reimbursing losses associated with an electronic theft from your bank account — for instance, if there was negligence on the part of your business, such as unsecured computers or falling for common scams. (To learn more about the rules pertaining to electronic theft, including losses involving a business debit card, see the previous page.)

Here are tips to help small business owners and their employees protect themselves and their companies from losses and other harm. Several of these tips mirror basic precautions we have suggested elsewhere in this issue for consumers.

Protect computers and Wi-Fi networks. Equip your computers with up-to-date anti-virus software and firewalls to block unwanted access. Arrange for key security software to automatically update, if possible. And if you have a Wi-Fi network for your workplace, make sure it is secure, including having the router protected by a password that is set by you (not the default password). The user manual for your device can give you instructions, which are also generally available online.

Patch software in a timely manner. Software vendors regularly provide "patches" or updates to their products to correct security flaws and improve functionality. A good practice is to download and install these software updates as soon as they are available. It may be most efficient to configure software to install such updates automatically.

Set cybersecurity procedures and training for employees. Consider reducing risks through steps such as pre-employment background checks and clearly outlined policies for personal use of computers. Limit employee access to the data systems that they need for their jobs, and require permission to install any software.

And, train employees about cybersecurity issues, such as suspicious or unsolicited emails asking them to click on a link, open an attachment or provide account information. By complying with what appears to be a simple request, your employees may be installing malware on your network. You can use training resources such as a 30-minute online course from the Small Business Administration (SBA) at www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses.

Require strong authentication. Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices and online accounts by using combinations of upper- and lower-case letters, numbers and symbols that are hard to guess and changed regularly. Consider requiring more information beyond a password to gain access to your business's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

Secure the business's tablets and smartphones. Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your company's network. In the case of the latter, require employees to password-protect their devices,

encrypt their data and install security apps to prevent criminals from accessing the device while it is connected to public networks. Also develop and enforce reporting procedures for lost or stolen equipment.

Back up important business systems and data. Do so at least once a week. For your backup data, remember to use the same security measures (such as encryption) that you would apply to the original data. In addition, in case your main computer becomes infected, regularly back up sensitive business data to additional, disconnected storage devices.

Use best practices for handling card payments online. Seek advice from your bank or a payment processor to select the most trusted and validated tools and anti-fraud services. This may include using just one computer or tablet for payment processing.

Be vigilant for early signs something is wrong. "Monitor bank account balances regularly to look for suspicious or unauthorized activity," suggested Luke W. Reynolds, chief of the FDIC's Outreach and Program Development Section.

Cybersecurity tips for small businesses also can be found in a new FDIC brochure at fdic.gov/consumers/assistance/protection/brochures/CyberBusiness.pdf. Also go to OnGuardOnline (www.onguardonline.gov/features/feature-0007-featured-info-small-business) and the SBA website (www.sba.gov/content/top-ten-cybersecurity-tips).

Going Mobile

continued from Page 4

or the original (if you get it back). A number of reputable apps can enable remote wiping.

To learn more about safely using smartphones and tablets, see the "Devices" section of the Federal Trade Commission's Computer Security Web page at www.consumer.ftc.gov/topics/computer-security.

Test Your Cybersecurity IQ

Take our quiz, which is based on information in this special guide

1 **A good password to use for logging into your online banking website is:**

a) 123456789
b) Password
c) 1Banana+1Pineapple
d) None of the above

2 **It's always safe to use your laptop computer or other mobile device to access your online banking site from a coffee shop, airport or other public place that promotes the use of its Wi-Fi network. True or False?**

a) True
b) False

3 **In case your tablet computer or smartphone is lost or stolen, which of the following precautions would *NOT* be a good way to restrict access to your device and the data on it?**

a) Use a password to restrict access.
b) Add an "auto lock" feature that secures the device when it is left unused for a certain number of minutes.
c) Add a GPS tracking system for your mobile device.
d) Download an app that enables you to remotely wipe data from the device.

4 **Parents and guardians should ensure that the devices their children use have the latest security updates from the software manufacturer. Which of the following equipment should have the latest security updates? (Select all that apply.)**

a. Computers
b. Tablets
c. Smartphones
d. Video game devices
e. All of the above

5 **You receive an email offering you a free entry in a million-dollar sweepstake if you click on a link that leads to an entry form. It's safe for you to:**

a) Click on the link but not download the attachment (the supposed entry form).
b) Delete the email without clicking on the link.
c) Do either of the above.

6 **Never include your birthday on your social media pages. True or False?**

a) True
b) False

7 **FDIC deposit insurance will not protect my deposits in the event that a thief online (or otherwise) takes money from my account. True or False?**

a) True
b) False

8 **If a thief uses one of your small business' debit cards to make fraudulent purchases online, your protections against loss from cyberattacks are the same as those for your personal debit card. True or False?**

a) True
b) False

The answers are shown upside-down on the right.

1. (c) Experts recommend creating "strong" user IDs and passwords for your computers, mobile devices and online accounts by using combinations of upper- and lower-case letters, numbers and symbols that are hard to guess. In our example, "1Banana+1Pineapple" would be a good password because it could be easy for you to remember and difficult for others to guess. You should also change your passwords on a regular basis. (See Page 2.)

2. (b) False. Not all public Wi-Fi networks are up to date with anti-virus and other security precautions that could prevent cyberthieves from stealing information that can be used to commit crimes. For sensitive matters such as online banking, consider only accessing the Internet using your own computer with a secure, trusted connection, and only connecting laptops and mobile devices to trusted networks. (See Page 3.)

3. (c) Passwords and auto-lock and remote-wipe features are good ways to prevent a criminal from accessing your device and data. It's also a good idea to back up your data in case you don't get your device back. Although you can add a GPS tracker to a tablet or smartphone for help locating and recovering the device, it won't prevent a thief from accessing account numbers and other important data. (See Pages 2 and 4.)

4. (e) Any device that can connect to the Internet, including video games, needs security updates. (See Page 7.)

5. (b) Delete the email without clicking on the link or opening the attachment, which could contain "malware" (malicious software) that a criminal can use to monitor your keystrokes, learn your online banking information and move money out of your account. And, just clicking on the link may be enough to download malware onto your computer. (See Page 5.)

6. (b) False. While cybercriminals can use facts such as your birthday or your place of birth to help them figure out passwords to online accounts, experts say it is OK to provide that kind of information on your social media pages but only if you have adjusted your security settings to prevent strangers (especially criminals) from seeing these details. (See Page 6.)

7. (a) True. FDIC deposit insurance only protects deposits if an FDIC-insured institution fails; it does not cover thefts from accounts. However, other federal consumer laws and financial industry practices may protect theft victims from losses, especially if they have been paying attention to their account activity. (See Page 8.)

8. (b) False. Debit cards issued for business use are covered by different loss protections than those for debit cards for consumers. Business debit cards are covered by the Uniform Commercial Code (UCC), which sets many rules for businesses. (See Page 8.)

A Cybersecurity Checklist

Reminders about 10 simple things bank customers can do to help protect their computers and their money from online criminals

1. Have computer security programs running and regularly updated to look for the latest threats. Install anti-virus software to protect against malware (malicious software) that can steal information such as account numbers and passwords, and use a firewall to prevent unauthorized access to your computer.

2. Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information. Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they don't have up-to-date security software.

3. Get to know standard Internet safety features. For example, when banking or shopping online, look for a padlock symbol on a page (that means it is secure) and "https://" at the beginning of the Web address (signifying that the website is authentic and encrypts data during transmission).

4. Ignore unsolicited emails asking you to open an attachment or click on a link if you're not sure it's who truly sent it and why. Cybercriminals are good at creating fake emails that look legitimate, but can install malware. Your best bet is to either ignore unsolicited requests to open attachments or files or to independently verify that the supposed source actually sent the email to you by making contact using a published email address or telephone number.

5. Be suspicious if someone contacts you unexpectedly online and asks for your personal information. A safe strategy is to ignore unsolicited requests for information, no matter how legitimate they appear, especially if they ask for information such as a Social Security number, bank account numbers and passwords.

6. Use the most secure process you can when logging into financial accounts. Create "strong" passwords that are hard to guess, change them regularly, and try not to use the same passwords or PINs (personal identification numbers) for several accounts.

7. Be discreet when using social networking sites. Criminals comb those sites looking for information such as someone's place of birth, mother's maiden name or a pet's name, in case those details can help them guess or reset passwords for online accounts.

8. Be careful when using smartphones and tablets. Don't leave your mobile device unattended and use a device password or other method to control access if it's stolen or lost.

9. Parents and caregivers should include children in their cybersecurity planning. Talk with your child about being safe online, including the risks of sharing personal information with people they don't know, and make sure the devices they use to connect to the Internet have up-to-date security.

10. Small business owners should have policies and training for their employees on topics similar to those provided in this checklist for customers, plus other issues that are specific to the business. For example, consider requiring more information beyond a password to gain access to your business's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

FDIC
Consumer News

Published by the Federal Deposit Insurance Corporation

Martin J. Gruenberg, *Chairman*

Barbara Hagenbaugh, *Deputy to the Chairman for Communications*

David Barr, *Assistant Director, Office of Communications (OCOM)*

Jay Rosenstein, *Senior Writer-Editor, OCOM*

Aileen Wu, *Graphic Designer*

FDIC Consumer News is produced quarterly by the FDIC Office of Communications in cooperation with other Divisions and Offices. It is intended to present information in a nontechnical way and is not intended to be a legal interpretation of FDIC or other government regulations and policies. Due to periodic changes in statutes and agency rules, always check the FDIC Web site — www.fdic.gov — for up-to-date information. Mention of a product, service or company does not constitute an endorsement. This publication may be reprinted in whole or in part. Please credit ***FDIC Consumer News***.

Send your story ideas, comments, and other suggestions or questions to: Jay Rosenstein, Editor, ***FDIC Consumer News,*** 550 17th Street, NW, Washington, DC 20429, e-mail jrosenstein@fdic.gov.

Find current and past issues at www.fdic.gov/consumernews or request paper copies by contacting the FDIC Public Information Center. Call toll-free 1-877-ASK-FDIC (1-877-275-3342) or e-mail publicinfo@fdic.gov.

Subscriptions: To receive an e-mail notice about each new issue with links to stories, go to www.fdic.gov/about/subscriptions/index.html. To receive ***FDIC Consumer News*** in the mail, free of charge, call or write the FDIC Public Information Center as listed above.

For More Help or Information

Go to www.fdic.gov or call the FDIC toll-free at 1-877-ASK-FDIC (1-877-275-3342)

Dear FDIC
continued from Page 8

As for your second question, by law, deposit insurance only protects accounts *if your insured banking institution fails.* FDIC deposit insurance does not protect accounts from a fraud or theft online (or otherwise). However, other laws and industry practices may provide coverage from cyber theft. For information, see our article on Page 8.

"If you have any questions about setting up an account online, be sure to get answers prior to making any deposits," added Troup.

You can learn more about FDIC deposit insurance coverage by calling us toll-free at 1-877-ASK FDIC (1-877-275-3342) or visiting www.fdic.gov/deposit/deposits. For those who are deaf or hard-of-hearing, please call 1-800-925-4618.

For More Help or Information on Cybersecurity

The Federal Deposit Insurance Corporation has tips on computer and Internet security for bank customers, including small businesses. See a new FDIC website about the basics of cybersecurity awareness at fdic.gov/consumersecurity, which includes two new brochures — one for consumers about how to protect and maintain their computer systems, and the other for business customers on how to safeguard their systems and data. Also search by topic in current and past issues of our quarterly ***FDIC Consumer News*** at www.fdic.gov/consumernews and watch the FDIC's multimedia presentation "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams" at www.fdic.gov/consumers/consumer/guard.

Other federal government agencies also publish information on how to protect against cybercrimes.

- Visit www.OnGuardOnline.gov, the federal government's website for information on how to be safe online, for general tips for consumers as well as more targeted information for parents, kids and small businesses.
- Go to the Federal Trade Commission's computer security page for consumers at www.consumer.ftc.gov/topics/computer-security, which has links to videos on topics like what to do if your email is hacked or malware attacks your computer.
- See the Federal Bureau of Investigation's "How to Protect Your Computer" Web page at www.fbi.gov/scams-safety/computer_protect, which includes links to more information on Internet schemes and how to protect yourself online.
- Consult the federal government's one-stop resource for identity theft victims at www.IdentityTheft.gov, which includes online tools for developing a recovery plan and generating pre-filled letters and forms to send to credit bureaus, the police and others who can help after an ID theft incident.