Learn to protect yourself from Identity Theft.

Two Rivers Bank & Trust can help.

Your identity is one of the most valuable things you own. It's important to keep your identity from being stolen by someone who can potentially harm your good name and financial well-being. Identity theft occurs when someone uses your name, address, Social Security Number, credit card or financial account numbers, passwords, and other personal information without your knowledge to commit fraud or other crimes. While the words may sound like a foreign language -- Phishing, Pharming, Vishing, Spyware, Dumpster Diving — they are actually techniques used by thieves to put your identity and finances at risk. And their attacks grow more frequent and sophisticated every year. Identity theft is the fastest growing crime in the United States. According to US Department of Justice statistics, it's now passing drug trafficking as the number one crime in America.

How to protect your identity

The simple fact is you can protect yourself against most forms of identity theft. The first step is education. To make it easier to understand, we've divided identity theft into the "Danger Zones." Take a few moments to learn about each of the Danger Zones and the steps you can take to avoid being a victim.

Danger Zone: Email

Phishing is an email scam used to steal your personal information. Email similar to the one pictured below may appear in your inbox, claiming to be from your financial institution, credit card company, or another source. It may appear authentic, but be careful - any email requesting personal information or to "verify" account information is usually a scam. Do not respond to this and do not click on any link from this email.

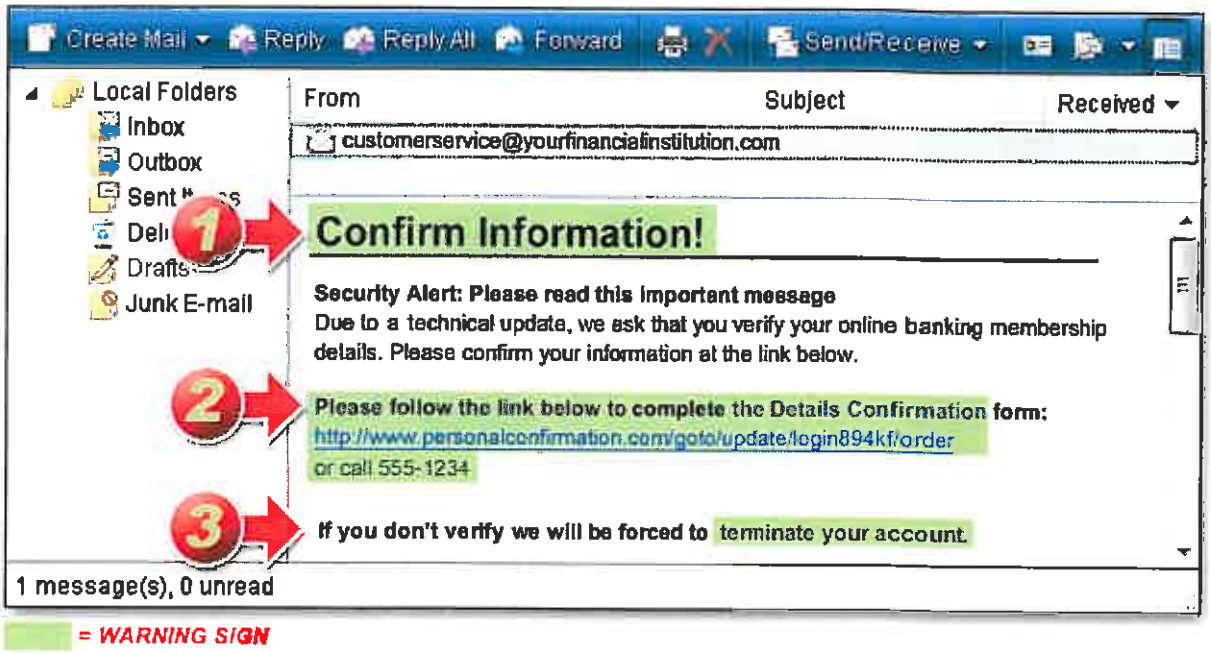
How to spot Phishing and other email scams

1. Any email requesting personal information, or asking you to verify an account, is usually a scam... even if it looks authentic.

2. The email may instruct you to click on a link, or call a phone number to update your account or even claim a prize.

3. The message will often threaten a dire consequence if you don't respond immediately, such as closing your account.

These are clear signs that someone is "Phishing" for your information. **Do not follow the instructions in the email.**



Follow these steps instead to avoid email scams

1. **Never respond to any email asking for confidential information, even if it appears urgent.** Chances are it is a fraudulent email.

2. **Never click on a link from an email.** Instead, type the known Website address into your Internet browser.

3. **Do not call any phone number provided in a suspicious email.** It could be a fake phone number.

4. **Always use anti-virus and anti-spyware software on your computer, and keep them up-to-date.**

Remember, email is not a secure form of communication. So feel free to use your email, but don't use it to send or receive confidential information. And if you follow the four basic steps listed, you can protect yourself from most phishing and other email scams.

Danger Zone: The Internet

The Internet is a great place to browse and do business. But it can also be a Danger Zone for identity theft if you don't know what to watch for or how to protect yourself.

There are several types of malware – which means malicious software – that can infect your computer as you surf the web including:

- Viruses
- Spyware
- Trojan Horses
- Keystroke Loggers

These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal information.

Learn how to practice safe surfing

Follow these steps to protect your computer from the majority of Internet crime:

1. Make sure you have anti-virus and anti-spyware software installed on your computer, keep them updated, and run a full system scan at least weekly.

2. Keep your computer operating system up-to-date, and your firewall turned on.

3. Use strong passwords for secure sites. Use eight or more characters with a combination of at least one upper case letter, one lower case letter, numbers and special characters. Change your passwords every six months.

4. If you download anything from the Internet such as music, movies, or pictures, make sure you do so only from trusted websites. Downloads can be infected with spyware attached to the file.

5. Watch for signs of spyware—frequent pop up ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection. Run a full system anti-virus and anti-spyware scan to safely remove.

6. Be careful when using public computers to perform any type of personal transactions. Just logging into a Website may give away passwords and other private information if spyware has been installed on that computer.

Following these steps will help protect you from the most common forms of identity theft while surfing the Internet.

Danger Zone: Telephone

The telephone is one of the most often used sources for criminal activity. Here's how it works. Your phone rings. The caller claims to be from your financial institution, or any other source. They begin asking questions about you and your account. This could be a telephone scam called Vishing. Someone is attempting to steal your identity. And it happens to millions of Americans every year.

Protect yourself from telephone scams

Follow these steps to protect yourself from most types of identity theft telephone scams:

1. Never offer personal or account information over the phone without verifying the caller's identity.
2. If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.
3. Do not call any phone number received in a voice message or email asking for personal information. It could lead you to a phony answering system.

As a general guideline, be highly suspicious anytime you are requested to provide personal information over the phone.

Danger Zone: Payments

Payment fraud happens when someone uses information from your checks, credit and debit cards, or any other form of payment without your knowledge to commit fraud or other crimes. But this, and other forms of identity theft, can be avoided, if you know how to protect yourself.

Avoid being a victim of payment fraud

Don't make it easy for criminals to steal your personal information. Here are some common sense tips to protect your identity:

1. Balance your checkbook, and verify all account and credit card statements as soon as they arrive.
2. Keep all checks, credit and debit cards in a safe place.
3. Don't leave outgoing checks or paid bills in your mailbox, and report lost or stolen items immediately.
4. Don't write PIN numbers on your credit or debit cards, or leave them in your wallet for a thief to find.
5. Use a paper shredder to securely dispose of any documents containing personal information.

6. Make online purchases only from trusted Web sites. If you have questions about a company, you can check them out with the Better Business Bureau.
7. NOTE! Consider paying all your bills electronically with online bill pay. This method is considered more secure than mailing paper checks.

Reducing your risk of identity theft starts with protecting your personal information. Keep it from getting into the wrong hands. Always be diligent about protecting your identity.

Danger Zone: Home

The simple act of sending and receiving mail, and putting your trash out at night, can put your personal information at risk. Financial information, checks, account and credit card statements, and monthly bills can be stolen from your home, mailbox or even from your trash, and used to access your accounts and steal your identity.

Follow these steps to protect against identity theft in your home

1. Invest in a personal shredder. This is your first line of defense. Shred checking and credit card statements, cancelled checks, pre-approved credit card offers, or anything with your personal information on it before disposal.
2. Place your garbage out on the morning of pickup rather than the night before. This gives dumpster divers less opportunity to go through your trash.
3. Install a mailbox with a locking mechanism, or pick up your mail immediately after it is delivered each day.
4. Change that old habit of placing mail in your mailbox for the carrier to pick up. Always place out-going mail in an official, secure mailbox.
5. It's good practice to store your mail, account statements, and other papers where they are out of sight and out of reach of anyone who might be in your home.

By following these steps you are on the right track to protecting your identity. Learning about all the identity theft danger zones and the simple steps you can take to avoid being a victim, is the best way to protect your good name.

Protect yourself from fraudulent transactions.

Consumers are protected in a number of ways against unauthorized electronic transactions, but it's very important to do your part.

1. **Report lost or stolen debit/ATM cards within two business days.**
   If you lose your debit/ATM card (or other access device) report it immediately. By contacting your financial institution within two business days of discovering the loss, you limit your liability to $50. Waiting more than two business days to report the loss increases your liability up to $500.

2. **Important! Review your statement every month**. If you find an unauthorized electronic transaction, you have 60 days to report it to your financial institution in order to limit the amount for which you are liable. If you wait more than 60 days you become liable for the unauthorized transactions. So review your statements every month and report any suspicious activity immediately.

The security of your money and identity is as important to us as it is to you. Let's work together to protect it.

To report suspicious activity, contact us at: 888-226-6063.

Mobile Security

The most important step in Mobile Banking security is treating your mobile device like a portable computer. A few common-sense precautions will help protect you from fraud and I.D. Theft:

1. **Set the phone to require a password to power on the handset or awake it from sleep mode.** If it's lost or stolen any personal information stored on the device will be more difficult to access.
2. Whether you're using the mobile Web or a mobile client, don't let it automatically log you in to your bank account. Otherwise, if your phone is lost or stolen, someone will have free access to your money.
3. **Don't save your password, account number, PIN, answers to secret questions or other such information on the mobile device.**
4. **Immediately tell your bank or mobile operator if you lose your phone.** The sooner you report the loss, the better protected you are from fraudulent transactions.
5. **Download and install antivirus software for your mobile device, according to the manufacturer's recommendations.**
6. **Be careful when downloading Apps.** Downloads should always be from a trusted and approved source, and endorsed by your mobile device provider.
7. **Avoid "free offers" and "free ringtones."** An email or instant message that offers free software downloads, such as ringtones, may contain viruses or malware.
8. **Be cautious of e-mails or text messages from unknown sources asking you to update, validate or confirm your personal details including password and account information.** Don't reply to text messages from people or places that you do not know.
9. **Treat your mobile device as carefully as you would your wallet, cash or credit cards.**
10. **Keep track of account transactions.** Review your bank statements as regularly as possible to rule out the chances of fraudulent transactions. If you notice discrepancies, contact your bank immediately.

11. **Only use Wi-Fi on your device when connected to password protected hotspots.** Turn-off any auto-connect features. They might cause your phone to log into unsecure wireless networks without your knowledge.
12. **Make sure you log out of social networking sites and online banking when you've finished using them.**
13. **Install operating system updates for your device as they become available - they often include security updates.**
14. **Before you upgrade or recycle your device, delete all personal/business details.**

Mobile Banking is a useful tool that can simplify your life and make managing your money incredibly convenient. By using common sense, it can also be a safe and secure part of your daily life.

Social Engineering

"Social Engineering" is any method of theft that manipulates your human nature in order to gain access to your online financial accounts. Here are a few ways you can protect yourself from thieves using Social Engineering techniques:

- **Don't respond to ANY email or social network post or message that asks for money or confidential information.** Thieves can hack email and social network accounts, and then pose as a friend or family member in order to gain your trust.
- **Don't assume that an unsolicited phone call or email is actually from a trusted source.** Thieves can research your purchases or donations, then pose as a business or charity you trust. Or, they may pose as law enforcement, a bank officer or another trusted authority figure. Just because they have bits of information about you or your past activities doesn't mean they are legitimate.
- **Verify, verify, verify.** If someone on the phone, or a message in your inbox, is telling you there is a problem with your online banking account, online auction account or credit card account, don't give them additional information to "fix" the problem. Instead, hang up the phone or delete the email and check those accounts directly by logging in normally or calling a published customer service number.
- **Be conscious what can be learned about you.** Many kinds of online accounts, including online banking, use challenge questions as part of their security. Make sure you don't choose responses that can be found online. For example, don't use your mother's maiden name if it is mentioned on a social network profile; or the model of your first car, if you discussed it on a forum. Thieves are very good at digging out those details from online searches.
- **Remember, even the most innocent email attachments can be infected with computer malware**. Common and popular files like PDFs, JPGs and spreadsheets can provide a platform for installing viruses or keystroke-logging malware on your computer. If you aren't certain the file came from a legitimate

business, charity or person, don't open it without verifying. Call them and ask if they sent an email with an attachment.

Thieves are smart and very good at exploiting your honesty and natural cooperation. They can send email that looks like it came from a family member, or hijack your best friend's social network account. Don't let your good nature become your downfall.

The best way to avoid Social Engineering schemes is to be cautious and suspicious of ANY request for money, passwords, account numbers or other confidential information no matter where it appears to be coming from.

Additional Resources

The following links are provided solely as a convenience to our visitors. Two Rivers Bank & Trust neither endorses nor guarantees in any way the organizations, services or advice associated with these links. Two Rivers Bank & Trust is not responsible for the accuracy of the content found on these sites.

- Identity Theft, Privacy, and Security Publications for Businesses
- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
- NIST's Risk Management Guide for Information Technology Systems (pdf)
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
- U.S. Computer Emergency Readiness Team (US-CERT)
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center
- Center for Internet Security (CIS)
- The Open Web Application Security Project
- Institute for Security Technology Studies