Protecting your Identity

Identity theft isn't just when someone steals your credit card information. When your identity is stolen, a criminal can use your social security number to get a job, rent an apartment or take out a loan—and do it all in your name. In some cases, criminals are even filing tax returns in victims' names and taking their tax refunds.

How to Avoid Frauds & Scams

The following tips may help prevent you from becoming a fraud victim.

- Be aware of incoming e-mail or text messages that ask you to click on a link because the link may install malware that allows thieves to spy on your computer and gain access to your information;
- Be suspicious of any e-mail or phone requests to update or verify your personal information because a legitimate organization would not solicit updates in an unsecured manner for information it already has;
- Confirm a message is legitimate by contacting the sender (it is best to look up the sender's contact information yourself instead of using contact information in the message);
- Assume any offer that seems too good to be true, is probably a fraud;
- Be on guard against fraudulent checks, cashier's checks, money orders, or electronic fund transfers sent to you with requests for you to wire back part of the money;
- Be wary of unsolicited offers that require you to act fast;
- Check your security settings on social network sites. Make sure they block out people who you don't want to see your page;
- Research any "apps" before downloading and don't assume an "app" is legitimate just because it resembles the name of your bank or other company you are familiar with;
- Be leery of any offers that pressure you to send funds quickly by wire transfer or involve another party who insists on secrecy; and
- Beware of Disaster-Related Financial Scams. Con artists take advantage of people after catastrophic events by claiming to be from legitimate charitable organizations when, in fact, they are attempting to steal money or valuable personal information.

The Best Ways to Avoid Getting Scammed

- **Don't respond:** If you're not 100% certain of the source of the call, email or text, then hang up the phone, don't click on the link in the email and don't reply to the text message.

- **Don't trust caller ID or answer phone calls from unknown numbers:** If you recognize the caller ID but the call seems suspicious, hang up the phone. Phone numbers can be easily spoofed to appear to be from a legitimate caller.

- **Don't give out your information:** Do not give out any personal identifiable information unless you're absolutely certain the person and reason are legitimate.

- **Research and validate:** If the individual or organization seems suspicious, make sure the request being made is legitimate by calling the organization through an official number from their website or consulting with a trusted family member or friend.

Revised August 2019.

Examples of Common Types of Scams

	Identify the Red Flags	This is what you might here
Threat of Lawsuit	You receive a request from a government agency asking you for a payment and/or to verify your personal information.	"I'm with the IRS and a lawsuit is being filed against you for back taxes."
Technology Support	You receive a request from tech support claiming your computer has malware and requesting payment to fix the defects or access your computer.	"We've detected malware on your computer, let's go ahead and get this fixed for you."
Plea for financial help from a loved one	You receive a call from someone claiming to be a grandchild or loved one asking for money to help with an emergency and instructions on where to send the funds.	"Grandma I'm in trouble, I need your help, I need some money really fast."
Romance	You receive a request for financial support from a partner in an exclusively online relationship.	"I'd love to come to see you, but I don't have the money to travel right now. Can you help me out?"
Lottery and Sweepstakes	You receive a request to prepay fees or taxes in order to receive a large prize you supposedly won.	"Your email address was randomly picked to participate in a drawing. Send us your details."
Investment	You receive a request to invest in a business opportunity with promises of high returns to getting rich quick.	"Glad I got you! Sometime back you responded to one of our programs for information. Are you ready to invest?"
Charity	You receive a request to donate to a charity that you've never heard of and for which you can't find an official website.	"Hi, the reason for my call is to see if you would donate to help preserve our local park."
Debt Relief	You receive a request for payment in order to establish a service relationship to pay, settle, or get rid of debt.	"I can help you reduce or eliminate your debt."

Internet Safety Tips

As more people bank and shop online, proper internet security is more important than ever. Safeguarding your information can be as simple as consistently reviewing your bank accounts and reporting any suspicious activity. But there are a number of other things you can do to stay safer online. Here are some tips to help protect you:

1. Use strong passwords

A strong password (one that is not easily guessed by a human or computer) will have eight or more characters, including letters, numbers and symbols. Make sure to use different user IDs and passwords for your financial accounts and for any other sites you use online. Follow the tips below to create a strong password.

- ### Create long and complex passwords

  When creating a strong password, the longer the better. Try to make sure it's at least eight characters, but preferably longer. Complexity also helps. For instance, a six-letter, lowercase password could take five minutes to break; one with nine letters could take two months. A six-character password that alternates numbers and symbols could take less than nine days to break, but one with nine characters could take a cybercriminal nearly 20,000 years to figure out.

- ### Create unique passwords

  Security service providers tell us that the most common (and therefore the worst) passwords in use "123456" and "password" are at the top of the list. Don't use those passwords-and don't use common dictionary words or consecutive numbers when creating your password. Passwords with simple patterns, such as "1234" or "qwerty," or with obvious substitutions, such as "H0u$e," are easy to guess.
    - A strong password has to be unique, not just a variation of passwords you use on other sites. Consider using a password manager to help keep track of your various log-in credentials.
    - Don’t use any part of your Social Security number (or any other sensitive information, such as credit card numbers or birthdays) as a password, user ID or personal identification number (PIN). If someone gains access to this information, it may be among the first things used to try to get into your account.
    - Avoid storing your passwords in unencrypted files, like the notes app on your phone. Instead, write them down and store them in a safe place such as a password manager.
    - No matter how strong a password may be, it is still at risk of being hacked. With two-factor authentication, a second level of security is added to strengthen your defenses against a breach. Also, enable biometrics like fingerprint sign-on, or retina or facial recognition where available.

2. Beware of email attachments

It’s never a good idea to click on email attachments or free software from unknown sources. You could end up exposing your computer (and the information on it) to online fraud and theft. Keep in mind that links you receive in emails or in messages on social networking sites can be harmful or fraudulent, even if they appear to come from friends.

3. Watch how much you share online

The more you post about yourself on social networking sites, the easier it might be for someone to use that information to access your accounts, steal your identity and more. Maximizing your privacy settings on social networking sites can also help protect your personal information.

4. Be careful about what (and where) you click

Look for security-enabled website addresses that start with “https” (the extra “s” indicates security). These sites take extra measures to help secure your information. This is particularly important if you’re making purchases using your credit card. If you suspect a link might give you a virus or steal personal data, don’t click on it. If the link was sent to you, talk to the sender directly to verify where it came from.

Smart Phone Safety

By following these online and mobile security tips, you can help protect your personal information from falling into the wrong hands. If you suspect information related to your bank account has been compromised, contact your bank immediately for assistance addressing the issue.

1. Secure Your Smartphone

Many mobile devices give you the option of locking your screen, which helps keep data stored on them secure. Depending on your phone, this can come in the form of a passcode, a pattern you draw on your phone's touch screen or even your fingerprint.

2. Don't keep sensitive information on your phone

Sensitive information includes your bank account numbers, identification information, passwords and other personal details such as answers to your security questions. If you bank via mobile app, don't worry, as the information in our mobile app is secured.

3. Be cautious about downloading apps

It's a good idea to review the privacy policy and understand what personal data an app can access before you download. It's best to purchase or download apps from authorized stores.

4. Keep your technology up to date

Make sure to update your computer's operating system, your internet browser and the software on your mobile devices. Updates generally include the latest security patches. Be sure to also use antivirus and antispyware software: These programs help find and remove malicious programs from your computer.