Harris County
FEDERAL CREDIT UNION

Minimize Your Risk of ID Theft

There are many ways you can minimize your risk of ID theft or fraud, below are a few ways to help keep your information safe. Review them below to ensure that you are using safe practices.

Steer Clear

Use strong passwords that include upper and lower case letters, numbers, and symbols. Considering passphrases, or memorize a sentence, and then use the first letter of each word – including numbers and symbols – as your password. Never use easily recognizable passwords or authorize payment over the phone unless you initiated the call. Fraudsters could contact you and state they're from a utility provider trying to get your information cause a payment declined. Never access sensitive personal information, or accounts, from a public computer or using a public Wi-Fi network. Never give personal information to callers (even the IRS), a call from the IRS is likely a scam. While on vacation do not use public computers to login to your accounts or type your credit card information.

Get in the Habit

Whether you're at home or traveling, expect occasional challenge questions when conducting online transactions to verify your identity and protect your accounts from crooks. Check your credit report annually as well as your child's. Review statements monthly more often online for any unfamiliar charges. Safeguard wallets, purses, checkbooks, and account statements – at home and at work. Safeguard wallets, purses, checkbooks, and account statements at home and at work. Mail bills from a locked mailbox or the Post Office. Shred (cross-cut) preapproved credit card offers, statements, bills, and personal documents or submit to a verified shredding company. Guard against shoulder suffers, cover the keyboard or pin pad as you punch in your PIN at ATMs or point of sale terminals. Don't carry your social security card in your wallet unless you need it that day.

Be Proactive

Go paperless! Use electronic deposit of paychecks, dividends, pension and social security payments, and tax refunds. Use online bill pay it's safer than mailing checks or entering your card information on a third-party site. It's important to ensure they all have secure and complex passwords. Lock down your smartphone, set up a PIN or complex passcode, install Lookout software that can allow you to lock the phone remotely and locate your phone. Keep a list, in a safe place, of account information in order to report theft. Never keep this list in your wallet or purse or anywhere that could be stolen. Dry up junk mail. Opt out of prescreen credit card offers, or for the unwanted catalogs or marketing mail.

Shop Safely

Shop only with companies you know. You can also look up the companies information with the Better Business Bureau. Pay with a credit card or third-party intermediary to keep your information secure. For online transactions use a Verified by Visa and or MasterCard's Secure Code. Use a separate credit card for online purchases to track them easily and limit the possibility to fraud to one card. Use a secure browser and sites that have "HTTPS://" along with forms that are secure. Keep a paper trail, by printing receipts or taking screen captures. Never send financial information via email and understand website cookies and their privacy policies.

Minimize Your Risk of ID Theft

Protect Your Computer

Install virus protection software, also ensure you update it regularly. Install firewall software to partially guard against spyware, which can capture account numbers and passwords, slow down your computer, cause pop-up ads to appear, and report surfing behavior to advertisers. Resource onguardonline.gov. Install spyware detection and removal software. Beware of look-alikes or online providers that are not verified. Check spyware removal program ratings when you install a spam blocker and beware of Google searches that can yield malicious websites. Beware peer-to-peer file sharing services many include spyware. Run the latest patches and fixes from Windows update to keep your computer any other regularly used software up-to-date. Use a secure browser to scramble communications. Set browser security level to at least medium. Secure your wireless network. Disable the broadcasting of the SSID after you configure your router. Make sure your wireless router has an encryption feature or turn it on if it was turned off before delivery. Consider using MAC Address only access to your wireless network to ensure only select devices has access.

General Usage Tips

Use strong passwords as stated above. Turn off your wireless network when you're not using it or away for long periods of time. Do not use public hot spots or open access Wi-Fi systems. Don't use public computers to access financial accounts. Avoid emailing personal and financial information. Password-protect tax returns and other documents which could contain sensitive information. Don't click on links or webpages you're not expecting or did not type on your own. Don't download files or open attachments from strangers and avoid automatic logins. Always log off your accounts when done, lock your computer when you leave the work station. Lock your laptop with a security cable and never leave it in a car. Wipe devices clear of information, personal documents, and consider shredding software to delete files.

ATM Card Skimming & PIN Capture

ATM Card skimming is a method used by criminals to capture data from the magnetic stripe on the back of an ATM card. Devices used are smaller than a deck of cards and are often fastened near, or over the top of the ATM's factory-installed card reader. ATM skimming is a world-wide problem. Check ATMs or card readers for tampering by looking at the card reader entry slot, ATM keyboard area, speaker area, and the camera area. PIN capturing occurs when individual has strategically attached or positioned cameras and other imaging devices to ATMs or card readers to capture your PIN. Once captured, the electronic data is put onto a fraudulent card and the captured PIN is used to withdraw money from accounts. PIN capturing is a world-wide problem. Skimming devices can be attached to card entry slot and is designed to look like a standard part of the terminal it's clearly different from the photo on the left. No flashing card entry indicator can be seen, and the shape of the snout is different. A skimming device works to piggy-backed onto the card reader or can look just like a normal card entry slot. PIN capturing devices can be installed in the overhead lighting system, or rain cover, including a brochure holder next to the ATM. A skimmer plate can be placed over the top of the existing keyboard as a method of PIN capturing.

Reduce your risk by familiarizing yourself with the look and feel of the ATM fascia on machines, inspect the ATM and all areas for unusual or non-standard appearance. If you notice anything unusual about the area, ATM, if so, walk away. Report any unusual appearance immediately to Police or the nearest branch. Always use your hand to shield your PIN when entering it at any terminal no matter how secure it looks.