PROTECT YOURSELF FROM IDENTITY THEFT

Identity theft is a huge concern these days, but there are a few simple steps you can take today to ensure your identity stays safe.

BE CAREFUL WITH SENSITIVE DOCUMENTS

Thieves are not above going through your trash to gain access to your personal information. Protect yourself by switching all of your accounts to e-statements, so you're not tempted to leave paper lying around. If you must receive paper statements, be sure to dispose of them using a shredder or shredding service.

FREEZE YOUR CREDIT

All three of the major credit reporting bureaus offer an option to freeze your credit report. This prevents any lenders from attempting to pull your credit report in the process of approving you for a loan. Most people don't apply for credit frequently, so they can simply unfreeze their credit just before they are ready to apply for a loan, and then freeze it again once the process is complete.

MAKE YOUR PASSWORDS STRONG

Most Americans use common combinations of letters and numbers for their passwords. These can be easy for a hacker to figure out. Whenever possible, use random combinations of letters, numbers and special characters to create passwords that are hard to crack. Be sure to use different passwords for each account so if one is discovered it doesn't provide access to everything, and if you really want to be safe, change your passwords often.

USE SOCIAL MEDIA WISELY

Social media is great, but if you're not careful it can also provide identity thieves with a great way to get supporting personal information that they need to steal your identity. Consider leaving personal details, such as your birthday or address, off your profiles, and keep your profiles private so only those that you accept as friends can see your information.

SECURE YOUR PHONE

The easiest way to protect your phone is with a password. You should also turn off Bluetooth when you're not using it and never enter your passwords or information into an app or a website while on a public WiFi network. Be very cautious when downloading new apps, especially free versions, which may contain malicious software designed to steal information from your phone. Only download apps from the Apple App Store or the Google Play Store so you know they are coming from a reputable source.

WATCH OUT FOR PHISHING SCAMS

The most common method for stealing your information is by gaining access to one of your accounts. Phishing scams involve a thief contacting you by e-mail, text or through a phone call, and posing as your bank, credit union or lender. These scams will often try to scare you by saying your accounts have been compromised and then ask you to verify your information by providing your password, account number or your social security number. Please remember, any reputable financial institution or lender will NEVER ask you to provide this information online or through your phone. If you are contacted by what appears to be your bank or credit union and they are asking for any personal information, immediately hang up and call your financial institution at the main phone number on their website and report in the incident.

KNOW YOUR SCORE.

RECOGNIZE IDENTITY THEFT AND REACT FAST

When it comes to identity theft, how fast you react and the actions you take are critical to minimizing the damage caused to your credit.

RECOGNIZE IDENTITY THEFT

Here are some warning signs that your personal information may have been stolen.

- You see withdrawals from your bank account that you can't explain
- You stop receiving your bills or other mail
- A check or payment is returned unexpectedly
- Debt collectors call you about debts that aren't yours
- You receive bills for products or services you didn't use
- Your health plan informs you that you've reached your benefits limit
- A health plan won't cover you because your medical records show a condition you don't have
- The IRS notifies you that more than one tax return was filed in your name
- The IRS notifies you that you have income from an employer you don't work for
- You get a notice that your information was compromised by a data breach at a company where you do business or have an account.

If any of these things have happened to you, follow the steps below to investigate and report the issue.

WHAT TO DO IF MY IDENTITY IS STOLEN

Above all else, acting quickly when your identity is stolen will limit the damage to your credit and limit your liabilities.

Place a Fraud Alert on your Credit Reports

Placing a fraud alert on your credit reports prevents a thief form opening any new accounts in your name. Fortunately, you only need to contact one of the three credit reporting bureaus. They are required to contact the other two on your behalf.

TransUnion: www.transunion.com
Equifax: www.equifax.com
Experian: www.experian.com

While you are on the websites of the credit bureaus, be sure to request a copy of your credit report from all three so you can identify any fraudulent accounts that were created.

Close Any Fraudulent Accounts Immediately

Review all three of your credit reports and identify any accounts that you did not open. Call each account holder and report the account as fraudulent and cancel it. For each account, be sure to capture the name of the representative you spoke with and the date you reported the account. Then follow up each call with a letter sent via certified mail-return receipt requested, to prove that you took action.

Notify the Police

Identity theft is a serious crime, so report it to the local police and be sure to request a copy of the police report for your records as you may need it in the future if disputes arise.

KNOW YOUR SCORE.