FSA - Keeping You Safe

Public Safety Tip: How to Prevent Identity Theft

When a criminal steals your personal information, they can use it to drain your bank account, damage your credit and wreak havoc on your life. And the worst part is, you might not even know it happened until it's too late.

Thankfully, there are ways to protect yourself and your personal information from the crime of identity theft. Here's the rundown on what you can do and what you need to know as a responsible consumer.

What is Identity Theft?

According to the Federal Trade Commission, identity theft is when **someone uses your personal or financial information to make purchases, get benefits, file taxes or commit fraud.**

Many attacks come in the form of a phone call or email that asks you to provide or confirm personal information. Some even include a fictional threat of danger or arrest if the target does not provide financial information or make a payment. Other attacks are more discreet and occur from online hacking, phishing attacks or stolen mail.

A criminal might use your stolen information to:

- Open a bank account or new credit card in your name.
- Make purchases with your existing credit cards.
- Use your health insurance to receive medical care.

Tragically, criminals often target vulnerable groups, such as older adults. And these attacks can have devastating consequences when a retired target suddenly finds themselves without their life savings. That's why it's important to learn about this very real threat and how to avoid being a victim. The more you know, the more you can share with others who might not have access to the same information.

Protecting Yourself from Identity Theft

Like most crimes, there's nothing you can do to completely prevent identity theft from happening, but you can make yourself a more difficult target. Here are the basics.

For more tips please visit the Florida Sheriffs Association's Crime Prevention Tips: flsheriffs.org/crime-prevention.

Protect Your Documents. It's important to take care with any documents containing personal information, such as financial records, Social Security cards and Medicare cards. When disposing of any of these items, use a shredder. Also, don't leave mail sitting in the mailbox for longer than necessary.

Don't Give Out Your SSN. Always take care when giving out your Social Security number, as it can be used to steal your identity. When in doubt, be skeptical of anyone asking for your SSN, and remember that you will never be required to give this information over the phone to a financial institution or credit card company.

Be Smart Online. Always use strong passwords when creating online accounts and use two-factor authentication whenever it is available. Be aware of phishing attacks that can come via email or text message and seek to steal your personal information. Scam emails can look 100% real, so it's always worth your time to independently check before completing any actions. Do not click on unknown links or attachments, especially if you do not recognize the sender.

The more you know about identity theft, the better you can protect yourself against common attacks. For instance, the police are not going to show up at your door over an IRS dispute – a threat often used to frighten targets in phone-based scams.

How do I Know My Identity Has Been Stolen?

To minimize damage, it's important to know how to recognize when you have been the target of an attack. To spot any unusual activity, make the following part of your routine:

- Routinely review your bank account statements and bills. Are there transactions or withdrawals that you don't recognize?
- Keep a sharp eye on your incoming mail. Did you receive any unexpected notices from the IRS for a tax return you didn't file, or a medical bill for services you did not receive?
- Take advantage of free credit card reports. Check for accounts you don't recognize.

Keeping an eye on your finances is the best way to recognize and respond to an attack as soon as it happens.

Recovering from Identity Theft

If you believe your identity has been stolen, don't panic. According to the FTC, here's what you need to do:

- Contact the fraud department of the companies where the fraud occurred and ask them to freeze your accounts.
- Change your passwords and PINs for all important accounts.
- Place a fraud alert on your accounts at IdentityTheft.gov.
- Get a free credit report and look for any unauthorized transactions.
- Report the incident to the FTC. This site also provides resources to create a recovery plan.
- If you are in Florida, you can also go to FraudFreeFlorida.com.

Depending on what information has been compromised (for instance, your driver's license), you may need to take additional steps. Click here for a full list.

For more tips please visit the Florida Sheriffs Association's Crime Prevention Tips: flsheriffs.org/crime-prevention.

Stay Safe with FSA

While the threat of stolen identity is very real, you can stay ahead of the game by monitoring your accounts, using caution when giving out personal information and knowing what to do when an attack does occur. As a reminder, the Florida Sheriffs Association will never ask you to provide personal or financial information over the phone.

The Florida Sheriffs Association is committed to helping you stay informed and stay safe. You can read more crime and public safety tips here.

For more tips please visit the Florida Sheriffs Association's Crime Prevention Tips: flsheriffs.org/crime-prevention.