Tips to Prevent I.D. Theft and Fraud

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

The FTC estimates that as many as 9 million Americans have their identities stolen each year. reminds you that you must be careful to protect your private financial information both at home and on the internet.

First, ***NEVER GIVE YOUR ACCOUNT INFORMATION*** unless you initiated the phone call or transaction. Superior Savings Credit Union will ***NEVER*** email you or text you to request personal information such as account numbers, Social Security Numbers or similar private information. If any company or institution requests this information, verify their authenticity first and then call a phone number or visit a website that you know is authentic.

When you access your credit union online banking and loan applications, always use our website directly at www.superiorsavingscu.com.

How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.
Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing**. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

How can you find out if your identity was stolen?

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. For more information, visit the FTC's Detect Identity Theft section.

You should also monitor and review your credit report every year. You may request your free credit report online, request your report by phone or request your report through the mail at www.annualcreditreport.com, a centralized service for consumers to request free annual credit reports.

What should you do if your identity is stolen?

Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name. To learn more about these steps and more, visit the the FTC's DEFEND: Recover from Identity Theft section. To file a complaint with the FTC, click here.