Identity theft information and tips

Identity Theft

Identity (ID) theft happens when someone steals your personal information to commit fraud.

The identity thief may use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status and cost you time and money to restore your good name.

You may not know that you're the victim of ID theft immediately. You could be a victim if you receive:

- Bills for items you didn't buy
- Debt collection calls for accounts you didn't open
- Denials for loan applications

Children and seniors are both vulnerable to ID theft. Child ID theft may go undetected for many years. Victims may not know until they're adults, applying for their own loans. Seniors are vulnerable because they share their personal information often with doctors and caregivers. The number of people and offices that access their information put them at risk.

Types of ID Theft

There are several common types of identity theft that can affect you:

- Tax ID theft – Someone used your Social Security number to falsely file tax returns with the IRS or your state
- Medical ID theft – Someone steals your Medicare ID or health insurance member number. Thieves use this information to get medical services or send fake bills to your health insurer.
- Social ID theft -Someone used your name and photos to create a fake account on social media.

Prevent Identity Theft

Keep these tips in mind to protect yourself from identity theft:

- Half of all Phishing sites now have the Padlock. Just because there is a padlock or the https, doesn't mean its safe.
- Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet. Only give out your SSN when absolutely necessary.
- Limit what other cards you carry, only take the credit or debit cards you need.
- Don't share personal information (birthdate, Social Security number, or bank account number) just because someone asks for it. Only do so if you initiated the contact or know who you are dealing with.
- Collect mail every day. Take outgoing mail to the post office collection box or post office. Place a vacation hold on your mail when you are away from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Use the security features on your mobile phone.
- For security purposes do not use unsecure public Wi-Fi for personal transactions.
- Review your credit card and bank account statements regularly and report suspicious activity. Compare receipts with account statements. Watch for unauthorized transactions.
- Shred documents with personal and financial information.
- Store personal information in a safe place.
- Maintain your computer with virus and malware protection and regular security updates.
- Do not click on links or attachments in unsolicited e-mail or texts. It's easy for fraudsters to copy corporate or government logos into fake e-mails that can install malware on your computer.
- Take precautions on social networking sites. Criminals go there to gather details about you to figure out and reset your passwords.
- Always log off when you are done.
- Close the Internet Browser when finished and/or reopen a new one between sites to help break cookie connections from each site.
- Create complex passwords . Choose combinations of upper and lower-case letters, numbers and symbols that are hard for a hacker to guess.
- Change your passwords if a company that you do business with has a breach of its databases.
- Review each of your three credit reports annually. Be certain that they don't include accounts that you have not opened. You can order them for free from Annualcreditreport.com or call 877-322-8228.
- You can even Freeze your credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for credit account or utility services in your name.
- Inform us of your travel dates and current contact information.
- Due to the recent increase in online card fraud, **we recommend that you enroll your Visa® Debit Card in Verified by Visa®**. Enrolling for this protection requires you to set up a private code for your account which will give you an additional layer of online shopping security. When shopping online at a participating merchant, you will be prompted to enroll, if you haven't already, or to enter your private code during the online checkout process.