Three Practical Tips to Safeguard Your Identity

Protecting your identity is extremely important in today's digital world. When fraudsters steal your personal information, you can suffer serious consequences, including financial loss, credit card debt, compromised health insurance and even legal trouble. In this article, we'll delve into what identity theft is, the potential risks involved and practical steps you can take to safeguard your personal information.

Understanding Identity Theft
Identity theft happens when someone unlawfully uses your personal information, like your name, Social Security number or financial details. When thieves are armed with this information, they can access your bank accounts, open new charge accounts or loans in your name, make unauthorized purchases with your credit card or even attempt to assume your identity to evade the law.

Potential Consequences
Identity thieves can wreak havoc on your life by wiping out your accounts, plunging you into credit card debt, depleting your health insurance benefits or entangling you in legal issues. Resolving that havoc can take months or even years.

Protecting Your Identity
Safeguarding your personal information is the best defense against identity theft. Here are some ways to protect your identity:

1. **Secure Your Mail**

It's well known that you're at risk for identity theft when you go online, but your mailbox can also be vulnerable.

- Shred any documents with personal information that identity thieves might use against you, such as receipts, financial and medical statements, cleared checks, credit offers and expired charge cards.
- Minimize mail theft risks by using U.S. Postal Service collection boxes or visiting the post office to send your letters.
- Retrieve your mail promptly after it's delivered and consider having it held at the post office if you'll be away for an extended period. You might also look in to getting a secure, lockable mailbox.

2. **Share Information Safely**

In a world where sharing information is common, prioritize safety.

- When providing information online or over the phone, make sure you know who you're giving it to.
- Share personal data only if you initiated the contact and are certain about the recipient's identity.
- If you receive an unsolicited contact, whether by phone, email or a website, don't disclose any sensitive information. Instead, offer to call back using a known, legitimate number.
- Exercise caution online and don't click on unfamiliar links, particularly those related to financial, medical or government matters, including the IRS.
- Be extra careful with your Social Security number (SSN). Some entities, like employers, financial institutions, medical insurers and the IRS, may legitimately request your SSN. However, for any others, ask whether providing your SSN is necessary or if an alternative identifier can be used.

3. **Consider a Credit Freeze**

A credit freeze can restrict access to your credit report, making it more challenging for identity thieves to open accounts in your name. Here are the key points to know:

- Credit freezes are free of charge.
- You must contact each of the three national credit bureaus to freeze each report.
- Your credit score won't be affected.
- You can still obtain your free annual credit report.
- You have the ability to temporarily or permanently lift the freeze for specific inquiries or a set duration.
- Existing creditors and government agencies responding to court orders can still access your credit report.

Recognizing Signs of Identity Theft

Learn to spot the potential signs of identity theft so you can take prompt action. Watch out for these indicators:

- Unfamiliar withdrawals on your bank statements
- Suspicious charges on your credit or debit card
- Missing bills and other mail that you are expecting
- Rejected checks
- Statements from unfamiliar credit cards
- Unwarranted calls from debt collectors
- Notifications of data breaches
- Unexpected credit or loan application denials
- Unsolicited requests for personal information
- Fraudulent tax returns filed in your name
- Bills for medical services or medications you never received
- Accounts appearing on your credit report that you didn't open or charges you didn't make

Suspect Identity Theft? Take Action

If you suspect that your wallet, Social Security number or other personal information has been lost or stolen, act swiftly to protect yourself from further harm. Visit IdentityTheft.gov, a comprehensive resource provided by the federal government, to report the incident and initiate the recovery process.

Reducing Your Risk

Protecting your identity should be a top priority in today's digital world. By following the recommended steps to safeguard your personal information, you can significantly reduce the risk of falling victim to this crime.

To learn more or to report fraud, visit stbank.com/security-center/ .