IDENTITY THEFT

In an era characterized by digital interconnectedness, the risk of identity theft has been heightened. Online activities like socializing and shopping come with both convenience and potential danger. As technology evolves, so do the tactics of cybercriminals who aim to misuse others' personal data for their gain. Understanding the threats and learning proactive strategies to safeguard your identity is vital.

QUICK TIPS

- Store sensitive documents in a locked cabinet, or use a secure digital storage system. Avoid carrying unnecessary identification and shred old financial statements before disposing of them.
- Create unique, strong passwords for all online accounts, and avoid using easily guessable information like birthdays or names. Enable multi-factor authentication whenever possible.
- Only provide personal information on secure websites with "https://" in the URL. Be wary of unsolicited emails or calls asking for sensitive data, and never share personal details over the phone unless you initiated the call.
- Regularly review bank and credit card statements for unauthorized transactions. Sign up for account alerts to receive notifications of suspicious activities.
- Consider freezing your credit to prevent unauthorized access to your financial information. This adds an extra layer of protection and prevents fraudsters from opening new accounts in your name.

IDENTITY THEFT SAFETY TIPS

PREVENTION

- If you receive mail with your personal information on it, be sure to remove the mail from your mailbox as soon as you can each day.
- Be cautious of suspicious emails, texts or links. Hackers often try to trick you into sharing personal information. Always verify the source before clicking.
- Protect your Social Security number. Do not carry your Social Security card, and refrain from sharing the number unless necessary. Ask the organization requesting it why, how it will protect the number and if you can provide only the last four digits or different identifying information altogether.

- Use complex passwords with a mix of letters, numbers and symbols. Avoid using easily guessable information like birthdays or names.
- Use reliable antivirus software and keep your devices up to date with the latest security patches.
- Avoid using public Wi-Fi for sensitive transactions, and opt for a Virtual Private Network (VPN) when accessing the internet on the go.
- Use a strong password to protect your home Wi-Fi network.
- Adjust your privacy settings on social media platforms to limit who can see your personal information and posts.
- Identity thieves may pose as government agencies, financial institutions or even acquaintances. Always verify the authenticity of requests for personal information before sharing anything.
- Whenever possible, enable multi-factor authentication for your online accounts. This adds an extra layer of security by requiring a second verification step.

DETECTION

Here are some ways you can find out if identity theft occurs:

- You may be notified by organizations if your data was involved in a data breach.
- If bills you owe stop coming, that may signal someone altered your billing address. Similarly, beginning to receive bills for services you do not use could also be a sign someone is using your identity for new accounts.
- Check your banking and financial account statements, including Social Security statements, to look for errors or charges that you did not authorize.
- Obtain free credit reports from all three major bureaus annually, and review them for inaccuracies or suspicious activities. Report any discrepancies immediately.
- You may be unexpectedly denied credit, including credit cards or loans, or your credit score may change unexpectedly.
- You may be notified that a tax return has been filed on your behalf without your knowledge.

REPORTING

If you suspect you may be a victim of identity theft, you can get help from trusted organizations.

- Start a log of all the conversations you have and steps you take as you start to deal with the situation.
- Report your suspicions to your bank and financial institutions.
- Contact the three major credit bureaus. Ask them to place fraud alerts and credit freezes on your accounts.
- Contact the Federal Trade Commission and follow its recommended steps at www.identitytheft.gov.