Protecting Your Identity in a High-Tech World

What to Know

What is Identity Theft?

Identity theft occurs when someone uses the personal identifying information of someone else to pose as that consumer in order to fraudulently obtain goods or services in the victim's name.

We are all potential victims of identity theft. Knowing what scammers are looking for, how they get our personal information, and what we can do to protect ourselves will help reduce our vulnerability to scammers.

What Information are Scammers Looking For?

Any of the following personal identifying information can be used by scammers:

- Social Security number (SSN)
- Birth date
- Address
- Driver's license number
- Bank account number
- Credit card number

Note: With one or two pieces of information, scammers can often get other information about you.

How do Scammers Get My Information?

It is important for you to keep all your identifying information confidential; however, things happen that allow scammers to get your identifying information:

- Lost or stolen wallet
- Theft by family or friends
- Dumpster diving - obtaining personal information from the trash
- Stolen mail
- Buying it from a corrupt insider at a bank, hotel, car rental agency, etc.
- Data breach - an incident in which an individual's name plus a social security number, driver's license number, medical record or financial record (credit and debit cards included) is potentially put at risk because of exposure
- Skimming - occurs when scammers place a device on an ATM, gas pump or other point-of-service device and electronically copy transmitted data on the magnetic strip of a credit card to enable valid electronic payment authorization to occur between a merchant and the issuing financial institution.

Social Networking

Social networking sites (e.g., Facebook, Instagram, Twitter), chat rooms, virtual worlds, and blogs have become the "new normal" when socializing with our friends. However, it is important to learn how to navigate these spaces safely.

What to Do

Protect your personal identifying information.

- Do not carry your Social Security card.
- Keep documents locked (paper) and secure (online).
- Protect smartphones/devices.
  - Increase the security configuration of the smartphone before using it. Security settings are often set at the lowest level by default.
  - Run firewall and anti-malware software.
  - Use caution when surfing the internet and opening email. If you do not know the sender, do not open the email, click on any links or open any attachments. Because text is small and often wraps, it is easier to overlook something, so be even more careful.
  - Make sure to set up a password on your smartphone to prevent others from accessing its data or making unauthorized telephone calls.
  - Only download files from trusted websites. Malware on a phone can steal information, account credentials, or infect your computer when you synchronize.
- Be careful of what you share.
  - Before sharing your SSN, ask questions.
  - Make sure you verify the source requesting your SSN.
- Practice cyber safety.
  - Use strong passwords.
  - Beware of email phishing scams. Phishing is the online scamming of your financial information by posing as a legitimate company.
- Safely dispose of personal identifying information.
  - Shred confidential documents before discarding in trash.

Where to Turn

If you think you are a victim of identity theft:

1. Contact the credit reporting agencies to place a fraud alert.
2. Close accounts that have been accessed.
3. As a precaution, change your passwords on other accounts.
4. Call the Michigan Attorney General to file a complaint.
5. File your complaint by phone or online at www.ftc.gov. You will receive an ID Theft Affidavit.
6. File a police report. When you attach the ID Theft Affidavit to the police report, this becomes an Identity Theft Report. This is necessary for providing persuasive evidence of theft when disputing debts.

For additional information visit:

www.michigan.gov/difs
www.michigan.gov/AG
www.ftc.gov

EXTRA

In a report by the Federal Trade Commission, American consumers reported losing over $1.6 billion to fraud. The FTC reported approximately 82 million U.S. consumer records were exposed through data breaches. Be on the lookout for skimming devices cleverly disguised to look like normal ATM equipment. A "skimmer" is mounted to the front of the normal ATM card slot that reads the ATM card number and transmits it to the criminals sitting in a nearby car. Another piece of equipment used to capture your ATM card number and PIN is a wireless camera disguised to look like a leaflet holder that may be mounted in a position to view ATM PIN entries. The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM.