cyber SNAPSHOT

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

March 20, 2017
CS-01-2017

CYBER SNAPSHOT: Protecting Your Personal Information

In 2016, researchers found that 15.4 million U.S. consumers fell victim to identity theft which resulted in 16 billion dollars stolen. This is a 16% rise from 2015. While numerous steps are being taken to address this issue, cyber criminals have learned and developed ways to get around some security solutions put in place.

Theft of personal identifiable information (PII) can happen to anyone. PII includes information such as date of birth, social security number, address, phone number, and etc. While it may seem to be an invisible crime, its impact is real and can be long lasting. Many victims lose time and money. They may also suffer an emotional toll.

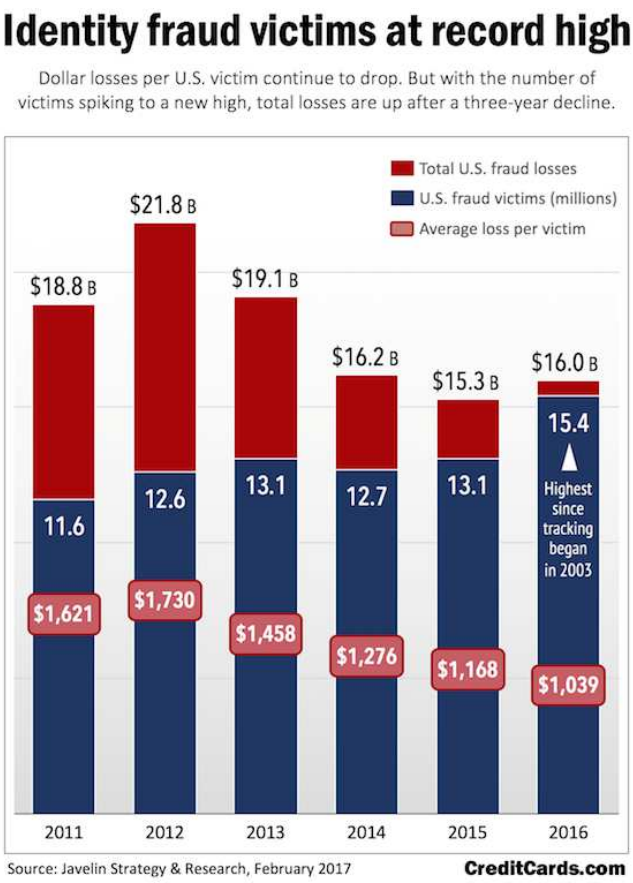
As technology advances and its uses increase, so does the need to protect ourselves electronically. While completely protecting against identity theft may not be possible, there are some important steps you can take to protect your personal information and make it harder for cybercriminals to steal.

Some signs of misuse of your personal information include but are not limited to:

- An unfamiliar charge on a credit card
- An unknown account on your credit report
- A debt collector calling about a bill that isn't yours
- A business not accepting your check due to unknown insufficient funds

To help protect your information online, consider taking the following steps:

- Keep your passwords private and use a separate password for each account.
- Be cautious when clicking on links or attachments contained in unsolicited emails.
- Use anti-virus, anti-malware, and other security software to help protect your devices.
- Keep all of your software patched and updated.
- Don't overshare on social networking sites. Cybercriminals can use information shared online to trick victims into giving up more information, use it to guess passwords, and gain access to personal information which can be utilized to access other accounts



- Limit your use of public Wi-Fi networks. These networks may be less secure than a private network and should not be used for making online purchases or entering personal information.
- When making purchases online, look to see if the web site uses Hypertext Transfer Protocol Secure (HTTPS). HTTPS encrypts your data making it harder for cybercriminals to gain access to your information.

Additional important steps to take:

- Safely dispose of personal information. This includes permanently deleting personal information from electronic devices such as phones and computers before getting rid of them.
- Don't give out personal information over the phone, internet, or mail unless you have initiated the contact.
- Monitor your credit score. Checking one of the three credit bureaus every four months will allow for continual monitoring without charge.
- Consider utilizing credit freezes which allows you to use existing credit but prevents new credit from being issued without your prior approval.
- Monitor your financial accounts frequently. The sooner you can identify a fraudulent charge on your credit card or bank account, the sooner it can get addressed.

Information on identity theft and steps to address it can be found out https://www.identitytheft.gov/Steps.