April 2019
Volume 14, Issue 4

Share Your Information With Care

From the desk of Thomas F. Duffy, MS-ISAC Chair

It is very easy to find any information you need in today's connected world. Have you ever Googled yourself to see what information about you is online? A search can often provide your address history, phone number, age, birthdate, employment information, public records, and social media accounts. Consider what can be done with Personally Identifiable Information (PII) from the perspective of a cyber-criminal looking to commit identity theft or other crimes.

Children, teens, and senior citizens are all groups who especially may not realize how vulnerable they are to being a victim of cyber-crime. Senior citizens may be more trusting of the material that is presented to them online. Children and teens are growing up with technology, and may be using it to communicate with each other with only a recreational level of understanding. They may not realize that once you post online, it rarely goes away.

In order to keep information safe or private, we need to take care in sharing it, and teach cyber hygiene to those who may not understand its importance. Here are examples of how we are asked to provide information, or how people share information that should be kept private:

Store loyalty and other accounts online – When you sign up for a store loyalty program or other online accounts, you are asked to provide information such as name, address, phone number, birthdate, email address, etc. By providing this, you can get discounts on the merchandise they are selling, or can receive promotions by email. However, is that information you provide kept private, or is it sold to other companies so they can market to you? Read the terms of use and privacy policy before signing up for such a program.

Phishing Emails – Cyber criminals will offer false and unbelievable deals to get you to click on a link and provide them with your information. You may hear about a loan offer, or a notification that your order shipped and that you need to log in by clicking their link to track it. Criminals seek your information in an effort to steal your identity and use it to open up fraudulent accounts in your name. Always shop with trusted vendors, and never follow an unsolicited link in an email asking you to log in to an account. Instead head to the website you normally use by typing it into your browser to check on your account.

Fraudulent phone calls (Vishing) – Criminals may call saying they are from Microsoft or another device/software company, telling you that your software has expired or your device is infected with malware. They may ask for money to renew a license, as a method to complete the fraudulent activity. Other criminals may pose as the IRS, pressuring you into paying taxes. Never offer payment information or personal information to someone calling you unsolicited. Always end the call and attempt to contact the organization through a publicly listed phone number that is legitimate, then see if you need to work with them on a problem.

Social Media Sites – These sites provide a relaxed atmosphere where you can chat with friends and family. The issue is that anything you post or share is likely a permanent submission that many others can access online. Oversharing on social media may lead to you voluntarily giving up answers to account security questions, like the color of your car or the town where you were born. Also, posting about being on vacation sends a signal to criminals that your home may be unoccupied and a great target for a robbery! With all this information about you on social media, be sure to set your account privacy settings so only friends can view your content. Lastly, consider deleting old, unused social media accounts to cut down on your digital footprint.

Whenever communicating with people or posting online, avoid sharing too much. When receiving emails, mail or calls asking for sensitive information (birthdate, social security number, credit card, etc.), always contact them at the legitimate address or phone number you normally use for that organization. Do not share information if you do not initiate the communication!

Below are resources on protecting privacy and identity along with practices for online security. These help you to protect yourself, your children, and your elders from being victims of a crime.

Resources:

Federal Trade Commission:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
https://www.consumer.ftc.gov/articles/0033a-share-care
https://www.consumer.ftc.gov/topics/protecting-kids-online
Stay Safe Online:
https://staysafeonline.org/
Family Online Safety Institute:
https://www.fosi.org/good-digital-parenting/ftc-share-care/
Protect Seniors Online:
https://www.protectseniorsonline.com/

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™