Cyber Crime Session at the 2014 OTA Winter Conference.

Michael Bazzell, FBI Cyber Crime Task Force

Ref: computercrimeinfo.com & osforensics.com

Several of us recently attended a Cyber Crime training class at the Ohio Township Association Winter Conference. Below are some of the highlights. Even people who do not use computers, cell phones, or other electronic devices can be victims.

No anti-virus software can detect a new virus until it has been identified and added to the anti-virus database. (No anti-virus software could have found the virus that struck Target, Michael's, etc.)

Do not save your password on any site or application and do not use auto-fill. This makes it easier for hackers to access your information. The dots that they fill in for your password mean nothing; can easily be converted back to text if you leave it on the screen of a public computer.

Many viruses record your keystrokes and then relay them to the hacker. Change your passwords often.

One nasty virus encrypts all of the files on your computer, making them unusable until a password is entered. The scammers send you information on where to send your ransom money in return for the password. No one can help you with this, except the hacker.

Your primary e-mail account is your most important account to protect. Change your password at least once per year and use a strong password. It is recommended that you use one that includes capitol letters, numbers, and special characters.

Go to "haveibeenpwned.com" to find out if your email is on the list of compromised email addresses.

At the very least, use a different password for different types of sites.

- One for "Fun" sites like EBay, Amazon (on-line shopping), etc.

- One for your personal e-mail account.

- One for your banking and financial accounts.

- One for Face Book and other social media.

- Work (There are probably more than one, but keep separate from personal)

Security questions are often used as alternate verification in case you forget your password. Take these questions seriously. They are as important as your password and are often easier to hack. Use the "make your own question" option and make it something that only you or a small number of people would know. Do not use anything as an answer that they could find anywhere on the internet. (No pets, schools, maiden names, uncle’s names etc. Face book is a great place to learn these things). If “make your own question” is not an option, pick a standard question, but lie so they can’t find your answer anywhere. Be careful not to forget your lie.

Challenge all e-mails that you receive. Do not click on link icons within the e-mail, unless you are confident in the source. When you hover the cursor over the icon, it will tell you the path it is going to connect to. If it does not match what it says it is, DO NOT OPEN IT.

Always password protect wireless devices. (Routers, phones, etc.) If you have a router, do not name it with your family’s name. Use something more vague so they may not know where it is coming from.

Always connect to encrypted networks if possible. When you are somewhere that offers paid or free internet access, make sure that you are connecting to their real access point. Scammers set up wi-fi zones, using a simple router, and give you access to the internet. Every aspect of your internet session (Passwords, logon ID’s, etc.) passes through their router and can be recorded.

Look for anything suspicious at gas pumps and ATMs. Anywhere you swipe your credit or debit cards. Thieves put “Skimmers”, or devices that record your information in these locations.