CATS/TIF Joint Annual Meeting: December 7, 2016

Doing Good Digitally: The Realities of Cyber Security

Presenter: Tristan Lawson, Senior Security Engineer

The digital threat landscape is full of social engineering exercises (i.e. fishing attacks). Threats are usually close. Small credit card interactions such as going to dinner maybe a vector for cybercrime. 5 billion people is realistic number for personal information that has been compromised. Largely via email.

Web based waterhole attack. Hiding in the waterhole, waiting for someone to approach..... Sending out fishing emails. DROPBOX is one place that this can happen.

Social media don't post personal information to your site.
Video and pictures: open source coding software can capture and pull information out of the background of a picture. Lock down your social networking sites. Facebook "aware" pages can see all your Facebook information.

Mobile devices are not any safer than desktop computers for transactions. The belief that a device will only be accessed by the graphic user interface (GUI), doesn't mean that the device can't be compromised. This can happen behind the scenes. Web transactions are probably less secure on mobile phones. Cell phones are tracking devices. Can be turned on by just visiting a web page. Can tap into your location with malicious code.

Ecommerce - getting gas at a gas pump is ecommerce. Information is still being transmitted over the internet. The information may be held on the gas station servers for a long period of time and could be a site of compromise. You can be compromised whenever you use your credit card. Do not use debit cards online. Change credit card number every six to twelve months.

Cloud Storage - Where is the data stored and how do you secure it?

Passwords stored in browsers can be easily retrieved off a computer. *Last Pass* is not a good choice because it is cloud based, but it is better than nothing, and probably better if used with a combination of services. Password management software is advised. Also, reset password questions, and not with publicly available information. Answer them with answers that don't make sense. Example: mother's maiden name is "King Kong". Set passwords to expire.

Health records are used to commit insurance fraud. Personal information is not as protected as you think it is, especially health records.

Email account: one of the most important accounts you have. Implement dual factor authentication on email. Set up a second email address to use for generic purposes. Verify emails. If you question an email received, you should call the sender. Set your email to not preload images. Images are a common vector for attack. JavaScript can run through image tags. Attachments: don't open them. Don't trust them. You can upload to virustotal.com to scan your file.

Internet: Quizzes can push you to a page that redirects you and compromises your site. Files downloading from the internet should be scanned. Most of the applications on source forge may have backdoors.
Incognito mode: not as incognito as you think, log files shipped to google.

Deleting Information: Information is not really deleted. Any cloud based emails that are older than six months can be searched without a warrant. They still exist, even after you delete them.

Software: Make sure your software is up to date. Turn on automatic updates for Windows.

Being safe in a digital world:

Web of trust plugin - community based trending rating
https://addons.mozilla.org/en-US/firefox/addon/wot-web-of-trust/
Free Antivirus on your system does not guard against the most recent threats. Usually, they are 2 to 4 weeks out of date.

Forticlient and web filtering tech
http://forticlient.com/
FortiClient extends the power of FortiGate's Unified threat management to endpoints on your network.

Qualys Browser Check
https://browsercheck.qualys.com/
Performs a security analysis of your browsers and plugins, will run several system checks including the Top4 Security Controls.

Sandboxie
https://www.sandboxie.com/
Trust no program. Uses isolation technology to separate programs from your underlying operating system preventing unwanted changes from happening to your personal data, programs and applications that rest safely on your hard drive.

Open DNS
https://www.opendns.com/
Remove your DNS blind spot.

MVPS host file
http://winhelp2002.mvps.org/hosts.htm
You can use a HOSTS file to block ads, banners, 3rd party Cookies, 3rd party page counters, web bugs, and even most hijackers.

Virus Total
https://virustotal.com/
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Cuckoo
https://www.cuckoosandbox.org/
Leading open source automated malware analysis system.

No real way to tell between a safe and a malicious bot agent when dealing with a tech service call.

Talk to kids about online threats.

Your savior can be your backup system.

Trust no one!

Game over when you let anyone on your system.