Cyber Security Awareness Month

With October being Cyber Security Awareness Month, we would like to address a few current trends we are seeing in the Niagara Region.

Sextortion

Sextortion occurs when someone online threatens to send sexual images or video of you to other people if you don't pay the suspect. Normally a person is contacted online by an unknown person and after chatting the conversation turns sexual and the suspects encourage the user to share intimate images.

Cyber Tips when using social media apps

- Be careful on how much information you share on social media, people with some technical knowledge can exploit the information you post online.
- Get familiar with the security settings on your devices / applications like Facebook and Twitter to limit what people see.
- Be cautious of friend requests from unknown people or multiple profiles using the same name as a known friend.
- Stop communications with suspects but don't delete the chat logs.

Avoid connecting with suspicious profiles. This can include:

- Unknown profiles that attempt to video chat for sexual purposes
- Profiles that ask for financial assistance in any way, often because of a sudden personal crisis
- Claims to be from the Canada but is currently living, working, or traveling abroad
- Disappears suddenly from the site then reappears under a different name
- Gives vague answers to specific questions
- Overly complimentary and romantic too early in your communication
- Pressures you to provide your phone number or talk outside the dating app or site.
- Requests your home or work address under the guise of sending flowers or gifts
- Tells inconsistent or grandiose stories
- Uses disjointed language and grammar, but has a high level of education

Crypto Currency Investment Scam

With the rise in popularity of Crypto Currencies many people are curious about investing in the market. We have seen several reports of people investing with fraudulent online crypto currency companies. Victims have let company representatives of the company to access their computers remotely to install software for them to access their accounts or install a fake mobile app. The suspects then direct the victims to transfer funds to their "Crypto Wallets". Over time the software shows gains in their investments, and they encourage more funds be deposited. When the victim asks to withdraw some funds, the suspects stop communication, and the victim finds the funds are no longer available. The phrase buyer beware applies, be diligently and research about any company before investing.

- Scammers guarantee that you'll make money. If they promise you'll make a profit, that's a scam. (Those are easily faked.)
- Scammers make big claims without details or explanations. Smart businesspeople want to understand how their investment works, and where their money is going. And good investment advisors want to share that information.

Marketplace Scams

Many online marketplaces allow users to buy and sell items locally. Fraudsters take can advantage of prospective buyers as well as sellers.

- Be cautious of a suspicious low price for a high demand item.
- Sellers that ask for payment using gift cards.
- Buyers should be cautious of any sellers that requests advanced payment via e-transfer or online methods.
- Buyers that overpay for their item and request a reimbursement of funds. It possible the original payment was fraudulent.
- Be careful of buyers that request the seller to mailing items. They can craft a real looking email from a payment service advising funds were paid to your account.
- If you do meet with a seller meet in a public well-lit place.

Ransomware

Ransomware is malicious software that encrypts or steals a user or company's data and login credentials and forces them to pay a fee to the hacker to regain access to their data or prevent the data and credentials.

Not only can ransomware encrypt or steal data and credentials on a single computer, but the software is also smart enough to travel across your environment and encrypt or steal data and credentials from any other computer located on the same network.

How attacks occur

Email (Phishing / Spear-phishing) – Hackers can craft a general email or specific email to a target to have the user open a malicious file or link.
Drive by downloads – Visiting a web site infected with Malware may spread to your computer.
Free Software – Downloading free software from non-reputable sources may be bundled with Malware.
DRP (Remote Desktop Protocol) – With more users working from home hackers attempt to find / exploit login credentials to access networks.
Exploits – Hackers may scan your publicly available networks to locate exploits.

Before an attack

Educate employees regarding phishing emails and other social engineering attacks.
Avoid opening suspicious links, double check the sender information and look for typos.
Keep your Operating System up to date and patch network devices.
Use an Anti-virus and keep It updated
Maintain a log of devices on the network and perform regular audits
Use MFA for RDP access to the network
Segregate the business network to minimize the risk of ransomware spreading.
Provide the least amount of privilege as possible to users.
Keep regular back ups that are separated from the main network.
Disable Marco in Microsoft Office
Employ an email filtering to block spam and suspicious emails

After the attack

Isolate the infection - Remove computers from network
Find the scope of the infection, did it spread across the network.
Determine the Malware variant.
Attempt to locate a decryptor / unlocker keys
Preserve back ups protect and isolate any back up files to protect them.
Determine your options, pay the ransom, remove the malware, wipe the system and start from scratch.