Cyber Tips

Travelling

Portable computing devices have information on them that is particularly vulnerable when working away from the office or home. Many hotels, airports, conference centres and other public places offer free Wi-Fi, but it is rarely secure:

- Always use a VPN (virtual private network) when connecting to a public Internet connection.
- Be aware of your surroundings and watch for "shoulder-surfers."
- Never leave your device unattended.
- Be wary of USB devices (thumb drive, etc.) found in a public place or handed out at conferences.
- Always use your own charger plugged directly into a power outlet. Public charging stations can install software on your device without your knowledge.

Social Media

Social Media is a great way to connect with friends and family, and a valuable investigative tool. However bad actors can perform research on social media as well, and what you post on social media can reveal a great deal of information about you and put you at risk.

- Do not post information that would make you vulnerable, such as your address or information about your schedule or routine.
- Be aware of what your friends and family are posting about you as well as what you post yourself.
- Regularly review your privacy settings and ensure that you are not leaving too much information publicly available.
- If you post photos and videos, be careful not to include identifying information in the background, such as licence plates and addresses.
- Only connect and share with people you know in real life.
- Set strong passwords: A good password is at least eight characters long.
- How to make your password stronger: Use a passphrase (instead of a word) and include numbers and special characters.
- Don't forget to log out of apps and sites. If not, you could be vulnerable if a bad actor is able to get remote or physical access to your device.

Cyber Bullying

One of the downsides of social media making it easier for people to connect with each other is that it makes it easier to connect in a negative way, enabling bullying and harassment. Some tips for dealing with cyber bullying are:

- Don't respond or retaliate. Sometimes a reaction is exactly what aggressors are looking for because they think it gives them power over you, and you don't want to empower a bully.

- Save the evidence. If the harassment escalates and crosses the line of criminality you want a record of the harassment that can be used as evidence in a criminal case.
- Ask for help before things escalate. See if there's someone who can listen, help you process what's going on and work through it – a friend, relative or maybe an adult you trust.
- Make use of social media tools for blocking harassers or reporting them.

Email

One of the most common ways that criminals compromise online accounts, computers, or even entire computer networks is through email.

Often phishing emails will contain:

- Generic email addresses from unknown domains.
- Urgent subject lines.
- Spelling and/or grammar mistakes.
- Attachments or links to external websites.

However note that criminals may do extensive research to craft convincing-looking emails with company graphics and signatures and many have even compromised a legitimate accounts.

Mobile devices

As the capability of mobile devices increases, they are starting to surpass personal computers as the device of choice for everyday online browsing. This means that people are using it to engage on social media, do online banking, and shop online. This makes mobile devices an attractive target for criminals and hackers, but many people don't put as much effort into security as they do with their computers. Some tips for keeping your mobile device safe are:

- Update your operating system as promptly as possible.
- Only install apps from the official app store (and watch out for malicious clones of popular apps).
- Understand an apps' permissions before installing it. Many apps ask for more access then is necessary for its operations so that they can sell your information to third parties.
- Protect your device with a password.
- Turn off Bluetooth and WiFi when not in use and change your settings so your device will not try to automatically connect to unknown networks.
- Don't jailbreak your phone operating systems. This makes it more vulnerable to malware and other attacks.

Banking

Online banking is convenient and can save you a lot of time and effort. However online financial services are a favourite target of cybercriminals and fraudsters, and thus using these services carries some risks.

Some ways to protect yourself are:

- Always use a secure connection (http**s**:// in the address bar).
- Never use links provided in an email or text to go to your banking website, always navigate directly to the website yourself.
    - These types of phishing attacks are not just limited to customers of the bank. Tellers are also frequent targets of cybercriminals trying to gain access to the bank's systems so that they can siphon money from accounts or pass money through them to launder it.
- If you navigate to the website by typing in the address, be careful of spelling mistakes. Criminals will create websites with commonly misspelled addresses to try to trick you into going to a malicious site (called "typosquatting").
- Remember that a bank will never email you to ask for personal information or passwords.
- Always log off after finishing your banking and clear any saved passwords or cookies from your Internet browsing history.
- Only do online banking on a secure network.
- Verify your transaction history regularly for any suspicious activity.
- ATMs are also a popular target for cybercriminals. They can install devices called skimmers to steal credit card data and cameras to capture the associated PINs. In some cases they have even compromised the software of the ATM. Always look for signs of tampering. Skimmers can be placed over the card reader or inside it; and to collect the PIN they may have installed a camera or placed a false front over top of the keypad.

Online Shopping

Shopping online is convenient and can be a great way to find some good deals. Some tips for avoid getting scammed online are:

- Buy from reputable sites. There a many scam sites out there that offer deals that are too good to be true, but rarely deliver.
- Pay with credit card or escrow service. Vendors that ask for cash, cheque, money transfer, or gift cards as payment are to be treated with suspicion.
- As with any financial transaction, only shop on secure networks.
- Keep copies of receipts and confirmations of purchase.

Hospitals

Hospitals have become popular targets for cybercriminals, whether through theft of data, or through the use of ransomware and other malware to disrupt systems or lock critical systems for extortion. Medical records are also popular targets for cybercriminals as they contain much of the information needed to steal an identity.

- Medical devices like insulin pumps, heart monitors and pain-medication dispensers operate remotely through computer chips. Because those devices were built for function, not security, hackers can breach them to harvest their data or even cause them to malfunction.
- Kiosks on a hospital floor are convenient for doctors, nurses and visitors. But their accessibility makes it wasy for hackers to find a way in and tunnel into other hospital networks.

- Doctors and nurses handle highly sensitive information, making them a likely target for spear-phising attacks that seek to steal their passwords and access to the broader hospital network.

Industrial Infrastructure

Electronics developed for heavy industry are built to be simple and robust, not for security and therefore often do not have encryption or if they do they are often hardcoded into the device. On top of this, older infrastructure such as water and power plants will often have a mix of new and old infrastructure that are networked together opening the network to vulnerabilities present in the legacy hardware, or the devices used to connect old and new technology.

- Meters and sensors in the field may remain unpatched for years because they are either inaccessible or replacing them would mean interrupting service. This leaves an open surface of attack for hackers.
- Companies might have strong cybersecurity measures in place but many times, their vendors and suppliers do not. Compromises among these "trusted third parties" can expose them to malicious code that can seep into their networks through remote access or compromised software patches to spy on their operations and disrupt service.
- The industrial control systems that regulate industrial processes should ideally be completely self-contained and seperated from the administrative network elements. However, for reasons of convenience and cost savings, many elements of those systems increasingly connect to the internet, leaving them vulnerable to maniplation or infection which can cripple the system.

External Resources

For Individuals

Serene-RISC Cyber Security 101: https://www.cybersec101.ca/
Public Safety Canada Get Cyber Safe: https://www.getcybersafe.gc.ca
Canadian Centre for Child Protection: https://needhelpnow.ca/app/en/

For Businesses

Get Cyber safe for Businesses: https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx
FCC Cybersecurity: https://www.fcc.gov/general/cybersecurity-small-business
NIST Small business Centre: https://csrc.nist.gov/projects/small-business-community/detailed-overview
NCSC Small Business Guide: https://www.ncsc.gov.uk/smallbusiness

For Industry