SECURITY AWARENESS
In a Nutshell

A quick guide to common awareness topics

Phishing

Email fraud – also known as "phishing" or "brand spoofing" are fraudulent attempts by cyber criminals to obtain your personal information or to install malware on your computer. The email messages look like they are from a legitimate company, such as a bank, credit card company, online retailer, or government agency. The email may look real, with company logos, links and branding, but beware – you may have received it from an illegitimate source.

There is more than one way to Phish:

- Vishing – scams that make use of VoIP (Voice over Internet Protocol)
- Spear Phishing – attacks that are customized to the recipient of the email, such as corporate executives
- SMS Phishing or Smishing –cell phone or smartphone text messages that influence people to divulge personal information

Protecting Against Phishing

Here are a few things you should know:

- Your bank will never send you an email or call you on the phone asking you to disclose personal information such as, your credit card number, banking password, or your mother's maiden name
- Be suspicious of unsolicited emails that appear to have a sense of urgency and warnings that your accounts will be closed or your access restricted if you don't reply.
- Review the email carefully. While some fraudulent emails may look professional at first glance, look for spelling errors, incorrect grammar, or unusual language
- Hover over the link (don't click) to see if it is identical to what is written. If they are different that is an indicator that the source is probably illegitimate. You can check the validity by using a reputable search engine to look up the address and/or company name

Ransomware

Ransomware is a form of malicious code or malware that infects a computer or network and spreads rapidly to encrypt the data. The malware makes the data inaccessible to the user and the criminals responsible will demand payment in order to unencrypt and return the files or unlock the infected computer.

The 3 common ways computers are infected:

- via Phishing Emails – the individual receives an email with a malicious link or attachment
- via Malvertising – the individual visits a legitimate website that displays infected third party advertisements
- via Zero Day exploit – the individual visits a legitimate website that contains a malicious program

Protecting Against Ransomware

What you can do to protect against an infection:

- Do not open and delete emails from spammers or unknown sources
- Do not click on email attachments from an unknown source
- Avoid suspicious websites altogether, such as the ads/links that often appear at the right or bottom of a website
- Do not accept software updates that are triggered from a website or email, such as Java and Adobe Flash

If you receive a pop-up or encounter a message that prompts you to pay a ransom:

- Immediately disconnect the device from the network/Internet and stop using it
- Report it immediately to IT support or get assistance in removing the infection
- Do not pay the ransom
- Change your important passwords (i.e. online banking, email) from a different (uninfected) device

Password Best Practices

Government employees should never use their IDIR password for logging onto anything other than their Government account

- Create a strong (complex) password or passphrase that's easy to remember
- Passwords should contain a minimum of 10 characters
- Use a combination of upper and lower case letters, numbers, and symbols

A phrase such as "Our one dog Pete is at the vet today" can become "R1dPi@tv2d". (Substitute a letter, number or symbol for the individual words)

Fraud

Fraud (or defrauding or scamming) is a crime in which someone tricks somebody else for unfair or unlawful gain. Frauds are almost always about money, either directly or indirectly. Fraud is both a criminal and civil wrongdoing.

Identity Theft

Identify Theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud, theft or forgery. Identity thieves and fraudsters seek your financial information (card numbers and PINs, banking information), your personal identifying information (Social Insurance Number, Driver License number), and other things that are unique to you.

Protect your Mobile Devices

Today's mobile devices are very portable and they can be easily lost or stolen. Be cautious when using mobile devices in uncontrolled locations such as hotels, airports, and other public places, and be aware of the risks to the devices and the information they contain. A loss can lead to significant security and privacy issues when sensitive and/or personal information is stored on the device. Following are some tips to keep devices safe:

- Learn about and use the security settings
- Never leave your device unattended
- Use a locking cable to secure your mobile computer
- Do not allow the device to automatically connect to unknown wireless networks; connect to Wi-Fi with care
- Use a strong password/passcode and don't share it
- Use encryption and/or password protection security features
- Backup your data regularly and especially before you travel. You can't always avoid the loss of your device but you can mitigate the loss of your information

How is Information Stolen?

Everyone is a target! Below are some examples of how personal information can be stolen:

- Stealing a wallet or purse
- Mail theft of bank and credit card statements, and unsolicited credit offers
- "Dumpster diving" by rummaging through trash or recycle bins for personal information
- Shoulder surfing at debit machines or using hidden devices to steal your card number and PIN
- Skimming your credit or debit card during a payment transaction
- Using a scam by posing as a legitimate businessperson or government official to obtain your personal information

Protecting Against Fraud and Identity Theft

Use the following best practices to guard against fraud and identity theft:

- When providing personal information ask why, how, and where the information will be used and how it will be safeguarded
- Shred receipts, credit card offers, bank statements, preapproved credit card or loan applications, and any other documents that contain your personal information
- Disclose your Social Insurance Number only when absolutely necessary and don't carry your card with you
- Sign new credit or debit cards as soon as you receive them and destroy the old ones
- Never provide your Personal Identification Number (PIN) to anyone
- Beware of shoulder surfing at bank machines or paying for transactions
- Regularly monitor your accounts and report any discrepancies or suspicious activity
- Report lost or stolen cards to your bank immediately
- Request a copy of your credit report annually from Equifax or TransUnion
- If you suspect your identify has been stolen report the crime to the Canadian Anti-Fraud Centre at 1-888-495-8501 or www.antifraudcentre.ca