FYI

Best Practices to Stay Cyber Safe

Overview

Cyber-criminals exploit human nature to trick you into giving them confidential information.

Cyber-criminals pursue organizations that hold sensitive data, such as governments, and by using social engineering (i.e., manipulation) tactics can illegally acquire personal, financial, medical, renewal resources, etc. information from their unknowing targets.

This FYI identifies common tactics used by cyber-criminals and best practices to stay cyber safe.

Common Tactics

Phishing - E-mail attack that imitates a trusted source and asks you to provide confidential information by clicking a link, opening a document or simply replying to the e-mail.

Vishing - Telephone equivalent to Phishing.

Smishing - A form of Phishing that occurs via text message.

Whaling - Targets specific, high-ranking individuals within an organization.

Clone Phishing - Replicates the look, feel, content and attachments of a legitimate email, but replaces attachments with those containing malware.

Quishing - Redirects you to a malicious website when a quick response (QR) code is scanned.

Baiting - Entices you (e.g., e-mail stating you have a won a prize, but you have to provide information to claim it) or piques your curiosity (e.g., found USB Drive labelled 'Confidential').

Response to a question you never had - E-mail or call-in response to your "request for help" even though you did not initiate the request.

Best Practices

Don't trust display names. Check the sender's complete email address before opening a message.

Read the salutation! If the email is not addressed directly to you (e.g., "Valued Customer"), it's likely fraudulent.

Check for typos! Spelling mistakes and poor grammar are typical.

Don't be quick to click! If something seems off with an email, review it carefully.

Don't follow unknown links. Hover over hyperlinks to inspect the link address. Rather than clicking on provided links, find the site yourself using a search engine.

Beware of downloads! If you are not expecting it; don't download it.

Don't share your passwords! No one else should ever need it.

Be Unique! Do not use the same security questions and passwords for your government employee activities and personal activities.

If you suspect deceit, hit delete! Delete any e-mail requests for passwords or financial information.

Control + Alt + Delete! When you leave your seat.

Reject requests for unsolicited help. If you did not specifically ask for it.

Restart is Smart! When leaving your computer for the day, logging off or periodically restarting your computer will prepare it to receive critical updates.

Always On, Always Connected. Always leave your work computer powered on and connected to the government network to help ensure critical security updates are applied.

Cyber Security is **EVERYONE's** responsibility. For more information, contact the Cyber Security Office at: cso@gov.nl.ca.

Supporting Materials

FYI – Information Protection – Phishing – Don't Get Hooked
https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/Phishing.pdf

FYI – Information Protection – USB Drives – What You Should Know
https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/FYI_Information_Protection-USB_Drives.PDF

FYI – Safe Web Browsing
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-fyi-information-protection-safe-web-browsing.pdf

FYI – Information Protection – Ransomware – What You Should Know
https://www.gov.nl.ca/exec/ocio/files/FYI-IP-Ransomware-What-You-Should-Know.pdf

FYI – Staying Safe on Social Media
https://www.gov.nl.ca/exec/ocio/files/FYI-Staying-Safe-on-Social-Media.pdf

Version History

Date (yyyy mm dd)	Reference
2019-08-15	Version 1.0
2020-10-01	Version 2.0
2021-10-01	Version 3.0
2022-10-01	Version 4.0
2023-10-01	Version 5.0