FYI

Ransomware – What You Should Know

Overview

Ransomware is a type of malicious software used by cyber-criminals to hold a device (e.g., network, computer, laptop, tablet, smartphone, etc.) and its information hostage until a ransom is paid using cryptocurrency (e.g., Bitcoin). Ransomware is commonly distributed by phishing emails, whereby the malicious software is contained in an embedded link in the email or disguised as a legitimate file that a user is tricked into downloading or opening.

Common Types of Ransomware

There are several types of Ransomware but they all have one thing in common - the user must pay to 'possibly' recover their information or to prevent it from being disclosed.

Locker Ransomware will lock a user out of their device making it impossible to access information on the device.

Crypto Ransomware or Encryptors will encrypt information stored on and accessible by the device (i.e., data becomes unreadable). A decryption key is required to revert the data to a readable format.

Doxware / Leakware Ransomware threatens to publish sensitive information.

Mobile Ransomware affects mobile devices (e.g., Apple iPhone, Samsung Android, etc.) by encrypting files and locking the mobile device.

Scareware is fake software claiming to have detected a virus or other issue on your device and directs you to pay to resolve the problem. Scareware may lock your device or flood your screen with pop-up windows.

Best Practices to Prevent a Ransomware Cyberattack

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

Don't follow unknown links. 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.

Limit Information Access. Limit access to the information required to perform a job duty, as ransomware will encrypt and affect all the information a user can access (e.g., shared drives).

Where NOT to save! Do not save government information on a local drive (e.g., C drive, My Documents folder, Desktop).

Connect with Care. Even with security enabled, public wireless networks should not be considered entirely safe. When accessing government information, over a wireless network, only do so through a secured VPN connection using a government-issued laptop or tablet.

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

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.

Patch Your Smartphone! Ensure your government smartphone has the latest available security updates applied.

Download Mobile Apps with Caution. Download apps for mobile devices from a trusted source (e.g., App Store, Google Play, etc.).

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

Signs Your Device is Infected with Ransomware

It can be difficult to detect if a device has been infected with ransomware, but common symptoms include:

- Your device is locked with a message that payment is required to access the device or its files.
- New file extensions appended to filenames (e.g., .encrypted, .locked, etc.).
- Pop-up windows appear on your device.
- Spam emails sent from your account.
- Slow computer performance.
- Unknown programs running on your device.
- Unauthorized password changes.

Suspected Ransomware Infection – What to Do

- Immediately disconnect your government-issued laptop or tablet from the network by unplugging the network Ethernet cable and disabling Wi-Fi.
- Disconnect external devices such as USB Drive, mobile devices, etc.
- Turn off Wi-Fi and Bluetooth on a mobile device. Enable Airplane Mode.
- Power off your device.
- Contact the OCIO (1-709-729-HELP).
- Once your device has been reset, wiped and returned, reset your passwords on all systems, devices and accounts.

Supporting Materials

Canadian Centre for Cyber Security – Protect Your Organization from Malware
https://www.cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057

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

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

FYI – Best Practices to Stay Cyber Safe
https://www.gov.nl.ca/exec/ocio/files/FYI-Best-Practices-to-Stay-Cyber-Safe.pdf

FYI – USB Drives – What You Should Know
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-fyi-information-protection-usb-drives.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
2020-10-01	Version 1.0
2021-10-01	Version 2.0
2022-10-01	Version 3.0
2023-10-01	Version 4.0