Yukon
Information
and Privacy
Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

RANSOMWARE ADVISORY

What is Ransomware?

Ransomware is a malicious software (malware) that installs itself on an electronic device or system, including smartphones and tablets, and encrypts the entire hard drive or specific files and then demands a ransom be paid before the information is decrypted. Ransomware also encrypts files that are located on network drives mapped to an infected device or system. More importantly, hackers may access information stored on a device or system during the course of an attack.

Ransomware typically spreads via phishing where an attachment or link in an email or text message contains malware that is installed when opened. Ransomware on one device or system may spread to others through network vulnerabilities.

Variations of ransomware exist to attack most operating systems, including Windows, Linux, Android and iOS (Apple). Publicized instances of ransomware have occurred elsewhere in Canada including at hospitals, universities, businesses and on thousands of personal devices. Local businesses here in Yukon just this week reported being affected by ransomware. There are several types of ransomware that you can learn more about online.

Preventative Measures

Yukon's privacy laws require reasonable steps be taken by public bodies and health care custodians to protect against risks to personal or health information, such as accidental loss or alteration, and unauthorized access, collection, use, disclosure and disposal. Given that a ransomware attack can result in a breach of privacy if the intruder accesses the information stored on a device or system, it is recommended that public bodies and health care custodians take preventative measures to protect against these attacks including the following.

- Educate users about phishing attacks. In particular, only download email attachments or click on links from trusted sources.
- Back up information and system files regularly, and test backups to ensure they are working as expected.
- Install internet security software and apply updates as they become available.

- Configure internet security software to receive automatic malware notices and perform real-time malware scans, in addition to regularly scheduled malware scans.
- Install security patches for operating systems as soon as they become available.
- Bookmark trusted websites and access those websites using bookmarks.
- Avoid using administrator accounts for general use on a device. Administrator accounts that are exploited by malware may cause more damage.
- Ensure a breach response plan is in place and educate users about what to do if attacked.

Ransomware Response

The severity of the attack and the safeguards in place will impact the response. Generally, the foregoing actions are recommended.

- Disconnect the affected device or system from the rest of the network and from the Internet.
- Run anti-malware scans in an attempt to identify and remove the ransomware, if possible.
- If you are able to restore files or the system from backup, you may not need to comply with a ransom demand.
- Review the response plan and update, as appropriate.
- Further education on preventative measures.

If a breach of privacy has occurred as a result of the attack:

- Health care custodians must consider if the intrusion presents a risk of significant harm. If it does, under the *Health Information Privacy and Management Act* the custodian must notify the individuals affected about the breach as well as the OIPC.
- Public bodies are not required to report such incidents to the OIPC under the *Access to Information and Protection of Privacy Act* but are encouraged to contact the OIPC for advice including about notifying affected individuals.

Businesses that are not subject to Yukon's privacy laws may wish to contact the Privacy Commissioner of Canada's Office if an attack involves personal information.