Advisory for

Ransomware

What is Ransomware?

Ransomware is malicious software (malware) installed on your device or system, including smartphones and tablets, that encrypts the hard drive or specific files then demands a ransom be paid before the device or information is decrypted. Importantly, hackers may access your data during the course of an attack.

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

Variations of ransomware exist to attack most operating systems, including Windows, Android and iOS (Apple). Publicized instances of ransomware have occurred at hospitals and media organizations, as well as thousands of personal devices. There are several types of ransomware that you can learn more about online.

Preventive Measures

Alberta's privacy laws require reasonable steps be taken to protect against risks to personal or health information. The OIPC recommends public bodies, health custodians and private sector organizations consider the following:

- Educate 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 maintain updates.
- 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 via bookmarks.
- Avoid using administrator accounts for general use on your 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 you have in place will impact your response. Generally, the following 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 your files or system from backup, you do not need to submit to a ransom demand.
- Review the response plan and update, as appropriate.
- Further education on preventive measures.

If a breach of personal information has occurred:

- Private sector organizations must consider if the intrusion presents a real risk of significant harm. If it does, under the *Personal Information Protection Act*, private sector organizations in Alberta must report the breach to the OIPC and may be required to notify affected individuals.
- Public bodies and health custodians are not required to report such incidents to the OIPC but are encouraged to contact the OIPC for advice and consider notifying affected individuals.

This document is an administrative tool intended to assist in understanding the *Freedom of Information and Protection of Privacy Act* (FOIP Act), *Health Information Act* (HIA) and *Personal Information Protection Act* (PIPA). This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of the FOIP Act, HIA or PIPA, please read the Acts and regulations in their entirety. This document is not binding on the Office of the Information and Privacy Commissioner of Alberta.

Office of the Information and
Privacy Commissioner of Alberta

www.oipc.ab.ca

MARCH 2016