Information and Privacy
Commissioner of Ontario
Commissaire à l’information et à la
protection de la vie privée de l’Ontario

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or “malware,” that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: “phishing” attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an “official” correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an “urgent matter,” such as an unpaid invoice or notice of audit. More advanced versions (also known as “spear phishing”) target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

Software Exploits

The programming code used to run the apps and programs on your computer may contain weaknesses which affect their security. Hackers can exploit these weaknesses to install malware on your computer.

In the case of ransomware, it is common for the hacker to infect a website with a number of exploits (also known as an "exploit kit") and try to lure individuals to visit it, either through phishing attacks, pop-ups or by masquerading as a legitimate website.

Ransomware may be installed if you visit a website compromised by hackers and the software on your computer has a weakness known to them.

PROTECTING YOUR ORGANIZATION

Under Ontario's freedom of information and privacy laws, public institutions must have "reasonable" measures in place to ensure the security of the records held by them and healthcare organizations must do the same with respect to personal health information. To protect against ransomware, you should assess the risk it poses to your data holdings and put in place preventative measures, which may include:

- **Employee training.** Employees should be aware of the threat posed by ransomware, how it gets installed and what they can do to prevent it. For example, employees should know to use caution when opening attachments or clicking on links in emails they were not expecting from outside the organization. When in doubt, verify the legitimacy of the communication before clicking.
- **Data backups.** Electronic records should be backed up regularly. When not in use, backups should be disconnected from the network and stored "off-line." Backups should also be tested periodically to ensure they can restore access to files. The retention period of backups should also be reviewed, taking into consideration the fact that ransomware may run in the background for days before being detected.
- **Antivirus software.** Software used to prevent, detect and remove malware should be installed and set to perform real-time scans, in addition to regularly scheduled scans.
- **Software updates.** All software and operating systems should be updated and patched regularly. Where possible, set updates to be automatic.
- **Email quarantines.** Emails from outside your organization with attachments containing executable files, archive files or files with potentially active content, such as Microsoft (MS) Office documents, should be blocked or quarantined. The recipient should be notified and asked to verify the legitimacy of the email before being granted access.

- **Minimal user privileges.** All user accounts should only be given privileges and granted access rights which are necessary for that user's work duties. For example, if a user does not need access to certain network drives and does not need to install software, that access and privilege should be disabled for them. The use of administrator accounts should also be strictly controlled.
- **Limited active content.** The ability of users to run computer code embedded in documents should be limited. For example, macros in MS Office documents from outside your organization should be blocked and JavaScript files should be opened with a text editor, such as Notepad, by default.
- **Simulated attacks.** To test the awareness of your employees and the effectiveness of your training, simulated phishing attacks may be sent to your employees. Your approach to securing your data holdings should be informed by the results.

RESPONDING TO INCIDENTS

If a computer on your network has been compromised, you should take immediate steps to mitigate the effects of the attack. These may include:

- Disconnect the infected computer from all networks, including any wireless connectivity (Wi-Fi, Bluetooth, near-field communication (NFC)).
- Determine the scope of the infection, including how much of the local and shared file system is compromised or encrypted.
- Try to determine the strain of ransomware and whether a decryption tool exists.
- Evaluate your options and determine the best path towards recovery. A recommended option is to reinstall the operating system of the infected computer from a clean installation source and restore files from backups. Once restored, you should scan the computer and any affected resources to ensure no infection remains.
- Update your preventative measures to address the weakness in security exposed by the incident.

If an infection of ransomware has occurred, public institutions and healthcare organizations should contact the Office of the Information and Privacy Commissioner of Ontario for advice and further guidance. You can reach us at 1-800-387-0073 or info@ipc.on.ca.