Cyberattacks and Digital Privacy

David Weinkauf, Ph.D.
Senior Policy and Technology Advisor
Office of the Information and Privacy Commissioner

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

Toronto Reference Library

Hinton Learning Theatre

June 20, 2018

Who Is the Information and Privacy Commissioner?

- Established in 1987, the Office of the Information and Privacy Commissioner of Ontario (IPC) oversees the province's access and privacy laws
- **Brian Beamish** appointed by Ontario Legislature (March 2015)
- 5-year term
- Reports to **Legislature**, not government or minister
- Ensures independence as government "watchdog"

Ontario's Privacy Legislation

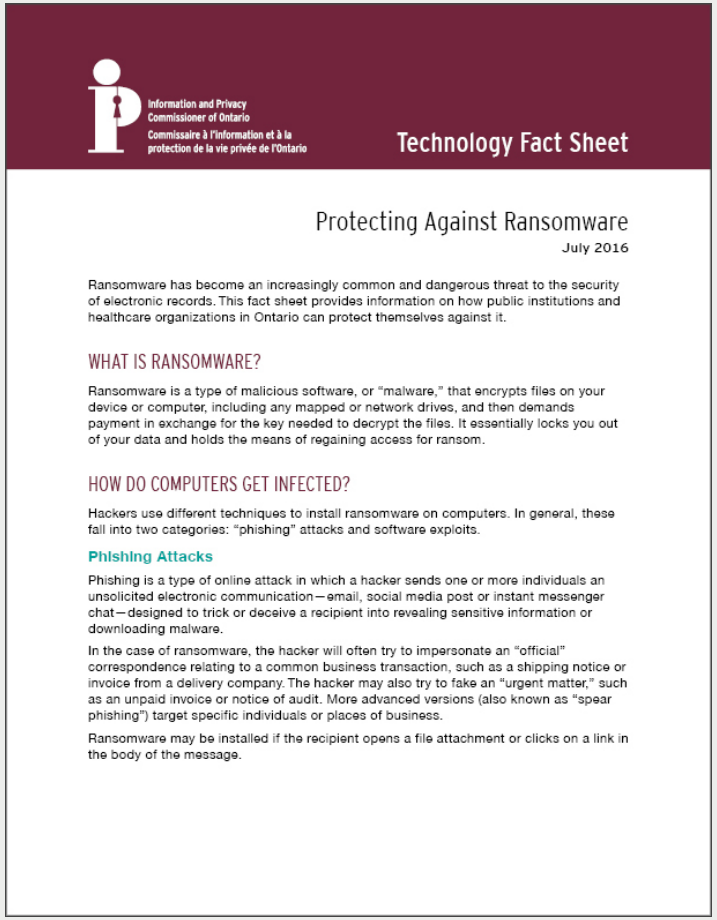
Public Sector	Health Sector	Private Sector
Government e.g. ministries, agencies, hospitals, universities, cities, police, schools, hydro *Freedom of Information and Protection of Privacy Act* (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	Health care individuals, organizations e.g. hospitals, pharmacies, labs, doctors, dentists, nurses *Personal Health Information Protection Act* (*PHIPA*)	Private sector businesses engaged in commercial activities *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
IPC/O oversight	IPC/O oversight	Privacy Commissioner of Canada oversight

Security Obligations

- *FIPPA* s. 4(1) of Regulation 460:
  - Requires government institutions to ensure that **reasonable measures** are defined, documented and put in place, taking into account the nature of the records to be protect, to prevent:
    - unauthorized access to records in their custody or control
- *PHIPA* s. 12(1):
  - Requires health information custodians (HICs) to take steps that are **reasonable in the circumstances** to ensure personal health information (PHI) in their custody or control is protected against:
    - theft, loss and unauthorized use or disclosure
    - unauthorized copying, modification or disposal

IPC's "Protecting Against Ransomware" Fact Sheet

- Released in July 2016
- High-level summary of issues
- What is ransomware?
- How do computers get infected?
  - Phishing attacks
  - Software exploits
- Protecting your organization
- Responding to incidents
- Available at www.ipc.on.ca



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.

What Is Ransomware?

- Various types of ransomware—crypto, locker, application, etc.
- **Crypto** is the most common type
- (Crypto)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
- In response to increased avoidance, a new development is **doxware** or **leakware** in which hackers threaten to publicly release sensitive information

How Do Computers Get Affected?

- In **phishing** a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive the recipient into downloading malware
- The hacker will often try to **impersonate** an "official" correspondence such as a shipping notice or CRA return, or fake an "urgent matter" such as an unpaid invoice or notice of audit
- **Publicly available information** on social media sites, e.g., LinkedIn, has facilitated **spear phishing** attacks, which target specific individuals or businesses

How Do Computers Get Affected? (2)

- Hackers may also exploit **software vulnerabilities** to install malware on your computer.
- The **programming code** used to run the apps and programs on your computer may contain weaknesses which affect their security.
- Hackers may infect a website with a number of exploits and try to **lure individuals** to visit it through:
  - phishing attacks
  - pop-ups
  - masquerading as a legitimate website
- "**Zero day**" exploits

Protective Security Measures

- Depending on level of risk, measures may include:
  - Employee training
  - Antivirus software
  - Email quarantines
  - Limited active content
  - Data backups
  - Software updates
  - Minimal user privileges
  - Simulated attacks

- The OWASP Anti-Ransomware Guide is a good resource: https://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project

Responding to Incidents

- If a computer on your network has been compromised:
  - Disconnect infected computer from all networks
  - Determine scope of infection
  - Try to determine the strain of ransomware
  - 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
  - Update preventative measures to address the weakness in security exposed by the incident

Tips to Help Identify a Phishing Email

- Do you know the sender?
- Were you expecting the email?
- Is the email urgent or threatening?
- Check the "From" address to verify domain name; ignore the display name
- Hover over links to see if they point to a different or strange address
- Check for spelling / grammar mistakes
- Does the signature have contact details?

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965