

Cyber Security & Privacy Compliance in an Increasingly Digital Economy: A Playbook for Protecting the Organization and the Client

David Goodis
Assistant Commissioner
IPC Ontario



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Canadian Institute
Regulatory
Compliance for
Financial
Institutions
November 18, 2020

Who we are

- Information and Privacy Commissioner of Ontario provides **independent review** of access and privacy matters in the public sector
 - Commissioner not part of government of the day
- oversee Ontario's **access and privacy** laws
 - public's right to **access** information, have their personal **privacy** rights protected
 - laws apply to government, police, school boards, universities, hospitals...

Ontario's Legislative Framework

Public sector	Health sector	Private sector
<p>Government provincial ministries, agencies, hospitals, universities, cities, police, schools, hydro</p> <p><i>Freedom of Information and Protection of Privacy Act (FIPPA)</i> <i>Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)</i></p>	<p>Health hospitals, pharmacies, labs, doctors, dentists, nurses</p> <p><i>Personal Health Information Protection Act (PHIPA)</i></p>	<p>Private sector businesses engaged in commercial activities</p> <p><i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i></p>
<p>IPC/O oversight</p>	<p>IPC/O oversight</p>	<p>Privacy Commissioner of Canada oversight</p>

Privacy breach

- privacy breach: personal information collected, retained, used, disclosed in way not in accordance with privacy laws
- most common is **unauthorized disclosure** of personal information, such as:
 - **insecure disposal of records**
 - records in paper format intended for shredding are recycled
 - insecure disposal of hard drives
 - **mobile and portable devices**
 - lost or stolen, unencrypted devices such as laptops, USB keys
 - **unauthorized access**
 - snooping by otherwise authorized staff
 - malware (e.g. ransomware)

Ransomware and cyber attacks on the rise


- hacker gained access to City of Stratford servers that contained personal information
- servers disconnected to contain attack
- city paid \$75k ransom
- city returned to normal business operations about 2 weeks after the attack

THE BEACON HERALD NEWS SPORTS ENTERTAINMENT LIFE MONEY OPINION OBITUARIES

Cyber attack that cost Stratford city hall \$75K ransom should be wake-up call: Expert

An update published on the city's website stated Stratford paid out more than \$75,000 in Bitcoins as ransom following the ransomware cyber attack on April 14.

 Galen Simmons
[More from Galen Simmons](#)

 Jane Sims, The London Free Press
[More from Jane Sims, The London Free Press](#)

Published on: September 20, 2019 | Last Updated: September 20, 2019 3:30 PM EDT



Cyberattacks

Systems infected by:

- phishing schemes to gain access to passwords/information
- ransomware and other software exploits used to gain control of computer systems

Statement from the Town of Wasaga Beach regarding the ransomware attack on the municipality's servers

Wasaga Beach – The Town of Wasaga Beach computer system was subject to a ransomware attack on Sunday, April 29, 2018.

The attack encrypted the town's servers, locking out access to the data with... These servers contain all the town's data, including financial information... on the town's infrastructure

Ontario police warn of recent cyberattacks targeting local governments

THE CANADIAN PRESS Updated: September 14, 2018

Phishing

Guides public institutions on how to protect personal information from these attacks

- What is phishing
- Impacts of phishing attacks
- How to recognize phishing messages
- How to protect against phishing attacks
- How to respond to a phishing attack
 - training employees
 - limiting user privileges
 - using software protections and back-ups
 - having an incident response plan in place

Protect Against Phishing

Phishing is a common method hackers use to attack computer systems. Successful phishing attacks pose a serious threat to the security of electronic records and personal information.

Ontario's privacy laws require public and healthcare organizations to have reasonable measures in place to protect personal information in their custody or control.

Phishing attacks pose a serious threat to the security of electronic records and personal information

WHAT IS PHISHING?

Phishing is a type of online attack in which an attacker — using both technological and psychological tactics — sends one or more individuals an unsolicited email, social media post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.

Malware (malicious software) is any software intentionally designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing attacks can be generic or customized, and can target both individuals and entire organizations. Attacks that target a specific individual or organization are commonly referred to as spear phishing attacks.

The main goal of a phishing attack is to get the individual to do something that compromises the security of their organization. Attackers achieve this when recipients:

- reply to phishing emails with confidential information

Ransomware

What is ransomware

How computers get infected

- phishing attacks
- software exploits

How to protect your organization

- administrative, technological measures e.g. employee training, limiting user privileges, software protections

How to respond to incidents



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

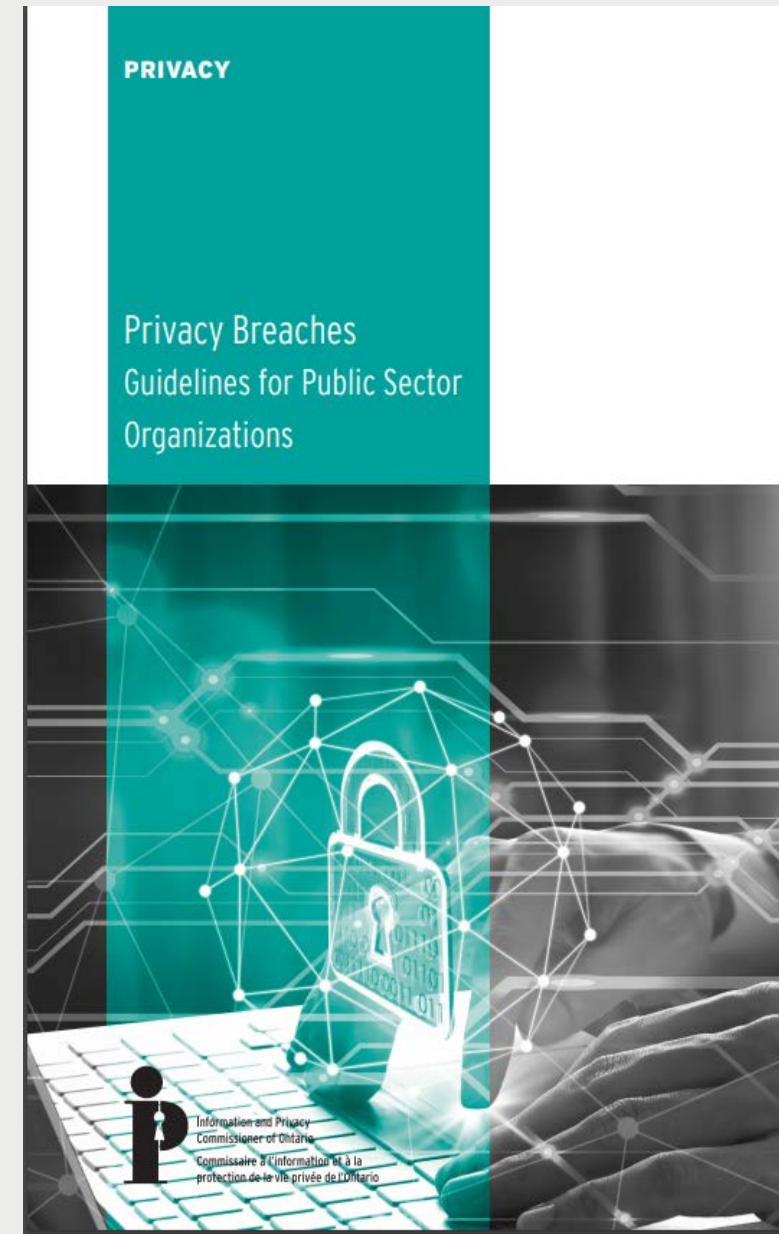
Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

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.

Responding to a Privacy Breach

- 1. Contain breach**
 - initial investigation
 - notify police if theft or other criminal activity
- 2. Evaluate risks**
 - personal information involved?
 - cause and extent of breach
 - individuals affected
 - possible harm?
- 3. Notify**
 - affected individuals
 - Privacy Commissioner
- 4. Prevent future breaches**
 - security audit
 - review of policies and practices, staff training, 3P service contracts



Reducing Risk of Privacy Breaches Best Practices

Administrative	Technical	Physical
<ul style="list-style-type: none">• privacy and security policies• auditing compliance with rules• privacy and security training• data minimization• confidentiality agreements• Privacy Impact Assessments	<ul style="list-style-type: none">• strong authentication and access controls• detailed logging, auditing, monitoring• strong passwords, encryption• patch and change management• firewalls, anti-virus, anti-spam, anti-spyware• protection against malicious code• Threat Risk Assessments, ethical hacks	<ul style="list-style-type: none">• controlled access to premises• controlled access to locations within premises where PI is stored• access cards and keys• ID, screening, supervision of visitors• secure disposal <div data-bbox="1595 911 2155 1196" style="border: 1px solid black; padding: 5px;"><p>NOTE – when determining appropriate safeguards consider</p><ul style="list-style-type: none">• sensitivity and amount of information• number and nature of people with access to the information• threats and risks associated with the information</div>

LifeLabs Breach

- cyberattack involving **unauthorized access** to its computer systems in 2019
- up to 15 million Canadians affected
- information included health card numbers, names, email addresses, passwords, date of birth, test results of some individuals
- joint investigation by the Information and Privacy Commissioners of Ontario and BC.



LifeLabs cyberattack one of 'several wake-up calls' for e-health security and privacy

CEO says information related to about 15 million customers may have been breached



Casino Rama Investigation

2016, OLG reports to IPC that Casino Rama Resort subjected to **cyberattack**

IPC launched **investigation** into circumstances of the breach and whether **reasonable security measures** were in place to protect personal information of Rama customers

investigation revealed **weaknesses in cyber-security practices** – particularly with response to suspicious activity

OLG/Casino Rama have taken steps to address the weaknesses identified – IPC satisfied

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