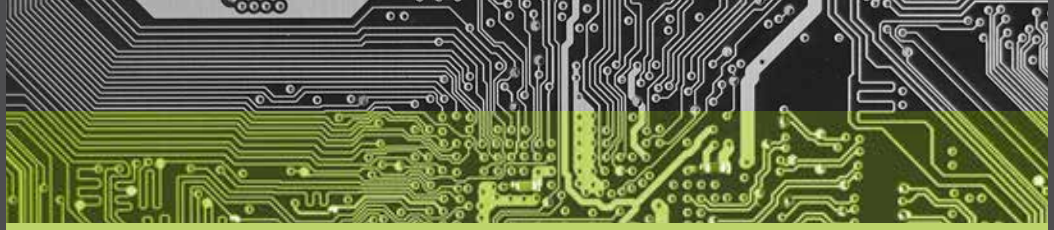

JULY 2019

TECHNOLOGY
FACT SHEET

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

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

- open email attachments that contain malware
- click on a link that leads to a fake website or page that installs malware
- enter usernames and passwords or other sensitive information on a fake website

The main goal of a phishing attack is to get the recipient to do something that compromises the security of their organization

IMPACTS OF PHISHING

The immediate effects of a successful phishing attack can include:

- unauthorized access to computer systems, networks and online accounts
- theft, loss and unauthorized use or disclosure of sensitive information, including personal information
- the destruction of or damage to records
- system failure and disruption of services

The effects of phishing are often not immediately apparent. Victims may not even be aware of an attack until the breach becomes more serious. Once the attacker gains access to confidential information, compromised accounts or computing devices, they may use other techniques to move throughout the network and collect more information. Ultimately, this can lead to crimes such as fraud, theft, or extortion.

Successful attacks can affect any organization, leading to negative consequences such as the loss of time, money, and reputation.

EXAMPLES OF PHISHING

Phishing attacks often imitate legitimate sources and work by exploiting people's trust, curiosity, fear, and desire to be helpful and efficient.

Phishing messages are often disguised as genuine messages and can include:

Phishing attacks imitate legitimate sources and exploit people's trust, curiosity, fear and desire to be helpful and efficient

- emails that look like official work-related items, such as full mailbox notifications, spam quarantines, password reset alerts, building evacuation plans, benefits enrollment, invoices, and confidential documents
- emails about business-related topics such as shipping confirmations, wire transfer requests, invitations to download documents from cloud storage services or to access an online file-sharing service to retrieve, create, or edit a document
- emails that try to replicate offers or accounts that people already have, such as bank, income tax or frequent flyer accounts, photo tagging, social networking, gift card notifications, and online shopping security updates

HOW TO RECOGNIZE PHISHING MESSAGES

Phishing messages can range from very basic to highly sophisticated. Common “red flags” include (see illustration on page 7):

- Suspicious sender or reply-to address: always treat messages from unknown or unfamiliar senders or accounts with extra caution.
- Unexpected message: messages from recognized senders that are unrelated to normal communications or job responsibilities can signal an account has been compromised or is fake.
- Suspicious attachment: messages with unexpected or unusual attachments can contain malware.
- Suspicious link: messages that encourage recipients to click and follow embedded hyperlinks may point to websites unrelated to the message and under the control of the attackers.
- Poor spelling: spelling and grammar errors may indicate a phishing attack since legitimate organizations typically avoid these mistakes in their communications.

Messages with unexpected or unusual attachments can contain malware

HOW TO PROTECT AGAINST PHISHING ATTACKS

You can protect your organization from phishing attacks by adopting the following best practices.

- Filter incoming messages: ensure that your IT systems screen incoming messages to reduce spam and other unwanted content. “Anti-spoofing” controls can verify the authenticity of senders and make it difficult for attackers to hit their target.
- Install malware detection and filters: your IT systems should automatically block or quarantine messages that contain viruses, ransomware or other malicious code. Use software that prevents, detects, and removes malware and performs real-time scans.
- Keep browsers and other software up to date: malicious attachments and malware often exploit security vulnerabilities made possible by outdated browsers and other software. Ensure that your IT staff regularly update all software and operating systems if it is not possible to set up automatic updates.
- Lock down workstations: hackers can exploit computers that allow software to be installed and settings to be configured by individual users. Restrict or disable administrative rights for normal users and limit the number of computers or accounts with high-level privileges or access to sensitive information. Individuals with high-level privileges should not share accounts or use them for non-work purposes.

- Require employees to use unique, complex passwords: the reuse of stolen passwords is a major phishing threat. Stronger authentication methods, such as one-time password tokens, cryptographic credentials, or biometric traits should be required for system administrators, users that handle sensitive information, and users with remote access to corporate resources.
- Identify external messages: you can detect phishing messages more easily if all external messages are clearly labeled as coming from outside the organization with a prominent message.

Detecting phishing messages is easier if all external messages are clearly labeled

CAUTION: EXTERNAL MAIL. DO NOT CLICK ON LINKS OR OPEN ATTACHMENTS YOU DO NOT TRUST

- Segment networks that contain sensitive data from other networks. You can limit the impact of compromised computers and accounts by restricting their access to other networks or systems. For example, public-facing webmail servers should be isolated from intranet systems or human resources databases.
- Use threat intelligence and endpoint protection tools. Advanced tools can detect, and in some cases, prevent attackers from gaining a foothold inside your network by flagging unusual patterns of system behaviour, such as irregular login attempts and large file downloads.
- Enable encryption on documents, devices, and databases that contain sensitive information, by default, to provide an extra layer of defence against unauthorized access, use, and disclosure by attackers.
- Conduct regular phishing awareness and training. Send simulated phishing attacks to employees to test their awareness and knowledge of how to respond. Routine tests raise awareness of security issues and help identify employees who need additional training.
- Enable users to report phishing and to request help. Organizations benefit from real-time feedback from employees on phishing threats. Make it easy for all your employees to report suspected phishing messages, and to request and get help in case of a possible attack.

Enable users to report phishing and to request help

Employees are often the last line of defence against phishing attacks. Awareness and training can and does improve security. In your guidance, include information about phishing red flags and instructions on how to manage suspicious messages.

- Verify the sender by carefully examining the “From” address, which should be consistent with the display name and the context of the message. For example, an email message claiming to be from a bank should not have an “xbox.com” address domain (the domain is everything after the @). Some phishing attacks use a sender’s email address that is similar to, but not the same as, an organization’s official email address. An example would be “omtario.ca” instead of “ontario.ca.”
- Do not provide usernames, passwords, or other access codes in response to an email request or unsolicited popup windows. Legitimate organizations never ask for this information via email and only collect it through their official websites or applications. When in doubt, follow up with the sender by phone.
- Do not open suspicious file attachments. If you receive an unexpected attachment, contact the sender (preferably by phone) to confirm that the attachment is legitimate. If you cannot confirm its legitimacy, report the attachment to your IT department, or delete it.
- Never click on suspicious links. Hover your mouse over parts of the message without clicking on anything. If the underlying hyperlink looks strange or does not match what the link description says, do not click on it — report it. Note that images can also contain suspicious links.
- Do not respond to suspicious or unwanted messages. Attackers benefit from learning more about potential targets. For example, asking to have an email address removed from a malicious party’s mailing list confirms that email is active, potentially leading to additional attacks. Downloading missing images confirms that the message was viewed. The best practice is to flag the message as spam or delete it.
- Report suspicious messages. When you receive a suspicious message, and especially if you click on questionable links or attachments, notify your IT department immediately. The IT department can confirm the threat and take action to minimize any risks to your organization.

Good planning and design can minimize risk and ensure that individual privacy is protected

Never click on suspicious links

RESPONDING TO PHISHING INCIDENTS

You should have a detailed incident response plan, which outlines how your organization will respond to a suspected data breach or cyberattack. A good incident response plan will help limit potential damage and ensure a swift return to normal operations.

Your plan should:

- designate key senior management, IT and legal staff contacts as part of the response team, and specify how each staff member will respond when incidents are reported

- identify potential threats. The plan should seek to quickly capture key evidence to determine the scope and severity of the threat. This may involve careful analysis of the phishing message, any attachments or embedded links, and the behavior of your staff and computer networks.
- prescribe steps to contain and remove any threats. Depending on the nature of the threat, your plan may include the following remedial measures:
    - disconnect infected computers from operational networks
    - change employee usernames and passwords
    - purge copies of infected messages or files from inboxes or servers
    - reinstall "clean" software or restore files from backup
    - heighten monitoring of computer and network activity
    - notify staff and report the incident to external parties (law enforcement, professional bodies, insurance companies)
    - update your preventative measures to address the weakness in security exposed by the incident.

You should communicate the incident response plan throughout your organization and practice it regularly so that when incidents occur, response will be quick and effective.

If a successful phishing attack has occurred, public 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**.

For information on protecting your organization from privacy and security breaches, and for guidance on responding to breaches, visit our website at **www.ipc.on.ca**

ADDITIONAL RESOURCES

- **Canadian Anti-Fraud Centre - Phishing**
- **Canadian Radio-Television and Telecommunications Commission (CRTC) — How to protect yourself from scammers**
- **Ontario Consumer Protection - Report a scam or fraud**

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

COMMON PHISHING "RED FLAGS"

FROM:

- The email appears to be sent from **someone inside the organization** and is **very unusual or out of character**
- The sender's email address is **from a suspicious domain**

TO:

- The email was sent to a group of people, but you **don't personally know** the other people it was sent to
- The email was sent to an **unusual mix of people**. For example, a seemingly random group of people at your organization whose names start with the same letter

SUBJECT:

- Subject line is **irrelevant**, **has bad grammar**, **poor spelling**, or **does not match** the message content

From: "Executive" <no-reply@Omtario.ca>
To: "You", "Yousef", "Yasmin", "Yves", "Yvonne"
Date: Sunday June 12, 3:01am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

Click here --> http://www.western-onion.com/jhvfz9oq.exe

Thanks so much, this really helps out!

Your CEO

DATE:

- Email was **sent outside of regular business hours, or at an unusual** time

ATTACHMENTS:

- Message includes an attachment that **you were not expecting** or that **makes no sense** in relation to the email message

CONTENT:

- Sender is asking you to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**

HYPERLINKS:

- When you hover your mouse over a hyperlink in the email message, the **link to address is for a different website**
- Email has a **hyperlink that is a misspelling** of a known website