Advisory for Phishing

Phishing is a type of security incident that can lead to a privacy breach. A breach means a loss of, unauthorized access to, or unauthorized disclosure of personal or individually identifying health information. Based on breach reports the Office of the Information and Privacy Commissioner (OIPC) receives, senior leaders and employees in all sectors are regularly subject to phishing incidents. These incidents can expose the personal or health information of employees, customers, patients or anyone otherwise affiliated with a private sector organization, health custodian or public sector body (collectively referred to as organizations in this document).

What is Phishing?

Phishing is defined as a social engineering attack carried out via electronic communications, typically email, but also instant messaging, text messaging and phone calls.

The objective of phishing attacks is for perpetrators to get individuals to divulge information for malicious purposes (e.g. for financial gain via fraud or theft or by selling personal information to other malicious actors, or to cause embarrassment, hurt or harm to an individual's or organization's reputation).

Phishing may occur in combination with other security incidents. For example, a third party (hacker) may gain unauthorized access to an email account belonging to an employee of an organization. The hacker then uses that account to send emails to other employees or contacts. These emails appear to be from the employee, and any replies may be redirected to a different email account controlled by the hacker.

Phishing attacks are often intended to obtain access to login credentials, such as usernames or passwords or other verification details (e.g. "forgot your password" answers) for specific websites, programs or portals that may contain information of value to perpetrators.

How is Phishing Executed?

Many phishing attempts are done in bulk where a message will be crafted and sent to numerous email recipients, with the intent that a few people will become victims. However, there are highly targeted and sophisticated phishing attacks that may seek personal employee information, such as social insurance numbers, salary details or other employee information (which may be referred to as "whaling" or "spear-phishing" attacks). These latter types of phishing attacks (i.e. business email compromises) are often used against organizations.

A common scenario is when an employee of an organization receives an email that appears to be a request for tax forms from the organization's CEO. Believing the email is legitimate, the employee replies to the message but it is sent to the unauthorized individual posing as the organization's CEO.

Office of the Information and Privacy Commissioner of Alberta

May 2019

What to Watch For

As the example above illustrates, phishing works by luring an intended victim using "bait" (hence the term "phishing"). For example, the "bait" may be that the email, call or text appears to be coming from a trusted source, such as an employer, a vendor/contractor, or a reputable organization.

To make it easier to distinguish legitimate requests from phishing attempts, the latter usually include one of the following:

- Requests for sensitive information (account information, passwords or social insurance numbers)
- Threats with imminent consequences ("your computer is infected", "I have compromising pictures of you" or "the CEO has asked for this ASAP")
- Rewards that seem too good to be true (promises of vacations or monetary gain)

Mitigating the Risks of Phishing

To mitigate risks of phishing incidents, organizations must consider various safeguards that will help to educate all employees, including senior leaders. Safeguards may include the following:

- Implementing policies and procedures, and providing privacy and security training for staff.
- Developing policies for reporting privacy and security incidents when they happen. Fostering a culture that encourages employees to report issues or incidents when they happen is helpful.
- Establishing password management policies that require employees not to reuse passwords across accounts. That way, one compromised account does not affect other accounts. For example, information from a compromised personal account could affect an employee's account within the organization – or vice versa.
- Confirming that a request for personal employee information is legitimate by contacting the sender.
- Providing "think before you click" guidance. Pausing and considering whether a request in an email is legitimate may provide the extra time it takes to prevent a breach from occurring.
- Considering flagging emails coming from external sources.
- Using multi-factor authentication that relies on email, mobile app prompts, or other authentication tokens, whenever possible.

When a Breach Occurs

Despite policies and guidance, breaches still occur. If an incident occurs, the OIPC has guidance available entitled "Key Steps in Responding to Privacy Breaches" available at **www.oipc.ab.ca**.

Certain incidents under the *Personal Information Protection Act* and *Health Information Act* must be reported to the OIPC, or may voluntarily be reported under the *Freedom of Information and Protection of Privacy Act*.

The OIPC has guidance on its "How to Report a Privacy Breach" webpage at **www.oipc.ab.ca** for reporting breaches to the Information and Privacy Commissioner.

The OIPC may be able to provide general advice or guidance for responding to the privacy breach and ensuring steps are taken to comply with obligations under privacy legislation.

Employees affected by a breach may need to take additional steps, such as:

- Changing credentials for various employee or personal accounts, if applicable
- Monitoring personal accounts (online, financial, health, etc.)
- Contacting or reporting the breach to the Canadian Anti-Fraud Centre