PHISHING

WHAT IS PHISHING?

Phishing is a type of **cyber attack** sent to potential victims on personal and work devices through calls, e-mails, text messages, and social media posts or accounts. Phishing messages often appear to originate from trusted sources, such as government agencies (e.g. Canadian Revenue Agency) or large corporations (e.g. banks, telecommunications). The goals of phishing attacks are to steal your sensitive data (e.g., passwords, banking information) or to deploy malware onto your device

HOW IT HAPPENS

BAIT

Individuals are tricked by 'bait' or 'lures' into sharing sensitive information.

Popular 'bait' or 'lures' include:

- Links to popular websites and login pages (e.g. Microsoft 365, Google, Facebook, etc.) prompting users to enter their credentials.
- Using themes from major world events to prompt individuals to provide personal information (e.g. donations to humanitarian relief efforts, cryptocurrency investment opportunities, etc.)
- Municipal, provincial or federal government impersonations, exploiting and mis-representing themselves as trusted government organizations (e.g. Canadian Revenue Agency) and compelling victims to share personal information via links

HOOK

Once the victim has clicked on the link or opened the attachment , the victim is re-directed to a fake website. While on the fake website, victims are prompted to enter their credentials and/or share personal information (e.g., answer security questions).

ATTACK

Credentials, accounts and personal information entered are stolen and accessed by scammers. Using a victim's account, scammers can send new phishing emails to the victim's contacts.

After their credentials have been stolen, victims are often redirected to the legitimate website they thought they clicked on, leaving them unaware that their credentials/information have been compromised.

THINK BEFORE YOU CLICK

RANSOMWARE ATTACKS

A link in a phishing scam may result in you inadvertently downloading something that can cause harm to your computer, like ransomware.

Ransomware, is a malicious software, also known as malware, which infects a computer and denies access to the system or data. A sum of money (ransom) is often demanded by the criminal in order to restore the system. In some ransomware attacks, victims may receive an on-screen alert stating that their files have been encrypted.

PROTECT YOUR INFORMATION!

- Avoid sending sensitive information over email or text and limit personal information posted on social media
- Filter spam emails
- Check for bad grammar
- Verify caller origin (if claiming to be calling from a specific organization, hang up, locate phone number from a reputable source, and call back the phone line associated to that organization)
- Use anti-phishing software & multi-factor authentication

You can report phishing attacks and other instances of online fraud to the Canadian Anti-Fraud Centre, or calling 1-888-495-8501. You can also report the incident to your local police department

References:

1. Canadian Centre for Cyber Security | Don't take the bait
2. IBM | What is Phishing?
3. Royal Bank of Canada | Don't Bite! How to Protect Yourself Against Phishing Scams
4. Canadian Anti-Fraud Centre | Phishing