CANADIAN CENTRE FOR
CYBER SECURITY

UNCLASSIFIED

DON'T TAKE THE BAIT: RECOGNIZE AND AVOID PHISHING ATTACKS

Phishing is an attack where a scammer calls you, texts or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source (e.g. from a bank, courier company).

Spear phishing: A personalized attack that targets you specifically. The message may include personal details about you, such as your interests, recent online activities, or purchases.

Whaling: A personalized attack that targets a big "phish" (e.g. CEO, executive). A scammer chooses these targets because of their level of authority and possible access to more sensitive information.

SMiShing: A phishing attack using SMS (texts). A scammer may impersonate someone you know or pose as a service you use (e.g. Internet or mobile provider) to request or offer an update or payment.

Vishing: A phishing attack using a voice over internet protocol (VoIP) system. A scammer can use an organization's phone number to trick you into believing they are legitimate.

SCAMMERS ARE AFTER YOUR:

IDENTITY

PASSWORDS

MONEY

SOMETHING MAY BE **PHISHY** IF:

- You don't recognize the sender's name, email address, or phone number (e.g. very common for spear phishing)
- You notice a lot of spelling and grammar errors
- The sender requests your personal or confidential information
- The sender makes an urgent request with a deadline
- The offer sounds too good to be true

WATCH OUT FOR:

- Attachments
- Hidden links
- Spoofed websites
- Log-in pages
- Urgent requests

PROTECT YOUR INFORMATION AND INFRASTRUCTURE:

- Verify links before you click them
- Avoid sending sensitive information over email or texts
- Call the sender to verify legitimacy (e.g. if you receive a call from your bank, hang up and call them)
- Back up information so that you have another copy
- Apply software updates and patches
- Use anti-phishing software that aligns with the Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy
- Filter spam emails
- Block IP addresses, domain names, and file types that you know to be bad
- Reduce the information you post online (e.g. phone numbers and extensions for employees)

32% THE NUMBER OF DATA BREACHES IN 2019 THAT INVOLVED PHISHING ATTACKS*

*Verizon's 2019 Data Breach Investigations Report

TRAINING AND AWARENESS CAN MAKE A DIFFERENCE:

Your organization's users should know the importance of keeping their personal information and the organization's information protected. Users who are not educated on the warning signs of social engineering attacks might reveal information or infect the network's devices unknowingly. Ensuring cyber security training is mandatory for all users in your organization can help reduce the risks of phishing attack being successful.