MISA
London Region Professional Network

PRIVACY CHALLENGE

Phishing

What is it?

Essentially, phishing is an attack that attempts to trick you into taking action. Email is the primary method of attack because so many people depend on email for communication and work. The phishing email might look like it comes from someone you know and trust such as your bank. It may attempt to get you to click on a link to a fake website that looks like your bank's website where you enter your login and password for them to steal and access your real banking website.

The link in a phishing email may not be a link at all but an infected file that, when clicked on, infects your system and compromises your board's network. Scammers use a wide range of tricks to get your information and to get their software onto your computer.

Protect Yourself

- ✓ Check the url. Hover over the link in the email to display the url and see where it is actually going to take you. Compare it with the url of the official site.
- ✓ Instead of clicking the link in an email, use your browser to go to the website you want to visit yourself by typing in its real url or using your bookmarks.
- ✓ Don't click on pop-ups that say you have a virus.
- ✓ Learn to use your browser's security features.

Resources

- Click here for a guide to understanding malware.
- See the Ontario government's Little Black Book of Scams to learn more.
- Here is the Privacy Commissioner of Canada's Top Ten Tips to protect yourself from malicious attacks.
- Learn why "https" no longer means "safe & secure". Click here.

Challenge: Find out if you have an account that was compromised in a data breach making your information vulnerable: https://haveibeenpwned.com/

Know Phishing!

• • •

1. It creates a sense of urgency demanding immediate action. They don't want you to take time to think this through.

2. It entices you to click on a link to verify or update your credentials. A bank or Paypal would never ask you to do that.

3. It asks you to open an attachment that it claims is an important letter from, e.g., Canada Revenue Agency.

4. It tries to sell you something, a too-good-to-believe deal.

5. The salutation is generic or odd, e.g., "dear customer!!" or "dear friend"

6. There is poor grammar or spelling even though the email claims to be from an official source.

7. The email claims to be from someone you know but the language and the tone just doesn't sound like him or her.