PHISHING

Phishing is a common tactic cyber criminals use to trick you into sending money or giving up sensitive information. Phishing messages are typically sent by email or text (also known as smishing).

WHAT DOES PHISHING LOOK LIKE?

Phishing and smishing messages are made to look like they've come from real companies. Some signs to look out for are:

- Asking you to **validate your account** information by clicking a link.
- Informing you that **there's a "problem" with your account** that can be resolved by clicking a link.
- **Threatening you with action** (such as closing your account or taking legal action) if you don't respond immediately.

DID YOU KNOW?

6.4 BILLION PHISHING EMAILS ARE SENT EACH DAY[1].

- **1 in 10 Canadians** have unknowingly replied to a phishing email[2]
- Phishing is the third most commonly reported scam in Canada[3]
- **29** per cent of Canadians are most concerned about phishing scams[4]

HOW YOU CAN PROTECT YOURSELF

Be aware and be skeptical. If you receive an email that seems suspicious, here are some things you can do to defend yourself:

- **Verify that it's legitimate by calling the company or service provider.**
- **Don't click any links or give up any personal information.**
- **Check the email address for suspicious spelling or characters.**
- **Look for inconsistencies like pixelated logos or misspellings.**
- **Verify the hyperlink behind the link's text or button by hovering over the text**
- **Take a moment to analyze the situation before doing anything rash.**

[1] Valimail, 2018 Email Fraud Landscape, 2018

[2] Public Safety Canada, Survey of Internet Users Regarding Cyber Security, EKOS Research Associates, 2018

[3] Canadian Anti-Fraud Centre, Fraud Prevention Toolkit, 2020

[4] Communications Security Establishment, Survey of Internet Users Regarding Cyber Security, EKOS Research Associates 2020 (when Complete)

Communications Security Establishment

Canada