CANADIAN ANTI-FRAUD CENTRE BULLETIN

Phishing: What's in a fraudster's ~~toolbox~~ tacklebox? **2023-03-28**

FRAUD: RECOGNIZE, REJECT, REPORT

The Fraud Prevention Month campaign is held each March to inform and educate the public on the importance of protecting yourself from fraud. This year's theme is "**Tricks of the trade: What's in a fraudster's toolbox?**". Follow the Canadian Anti-Fraud Centre (CAFC) on social media and visit our website for fraud prevention information. Don't forget to use #FPM2023 on all fraud prevention posts!

Phishing

Phishing is one of the easiest ways for fraudsters to steal log in credentials, personal information or even infiltrate corporate networks. Fraudsters will use mass email and text message campaigns to send messages that appear to be from recognized institutions, companies or government agencies. These emails may claim that you need to update your account or that money is ready to be deposited.

The CAFC also receives many reports of phishing scam variations where the message contains malicious links or attachments. These emails or texts may appear to be a receipt from a purchase, delivery notification or a fraudulent notice to appear in court. If the link or attachment is clicked, your computer or device can potentially be infected with malware.

Financial institutions are often impersonated by fraudsters in an attempt to make their frauds sound more convincing. Phishing scams often target businesses luring employees to open an attachment or click on a link, which can potentially allow access to the company's network, lead to ransomware or spear phishing attacks.

What's in a fraudster's tacklebox?

Impersonation and spoofing:

- Fraudsters will pretend to be a familiar business, organization or financial authority requesting something from you or offering you a refund. They're able to change the way their email address and name appear in your inbox.

Refunds and E-transfers:

- Fraudsters will spark excitement by providing a reason for offering you a refund or e-transfer, just click the link and enter your credentials and/or financial information. Don't let the temptation trick you!

Mass messaging:

- Phishing messages are sent in mass with the hopes that at least a few will be lucrative. It's likely you are targeted by one every day.

What's in your tacklebox?

Spellcheck:

- Spelling mistakes in communications from someone claiming to be a legitimate organization should be a red flag. Because of how many approvals organizational messaging needs to go through, there shouldn't be any spelling errors.

Certainty:

- The Government of Canada will never send funds by email or text message – this is certain. If you get a message like this, report it to the CAFC.

Caution:

- If you get an unsolicited email or text asking you to click a link or open an attachment – don't do it!
- If unsure, research the contact information for the company and reach out directly to them. Don't use the contact information provided in the message.
- Never click on a link or attachment from an unsolicited message.
- Set-up multifactor authentication for all online accounts.

Training:

- Businesses should implement cyber security training for new employees.

Learn more tips and tricks for protecting yourself from fraud.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the Canadian Anti-Fraud Centre's online reporting system or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.