CANADIAN ANTI-FRAUD CENTRE BULLETIN

Spear Phishing: What's in a fraudster's toolbox? 2023-03-14

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 our social media and visit our website for fraud prevention information. Don't forget to use #FPM2023 on all fraud prevention posts!

Spear phishing

Spear phishing fraud is one of the most prevalent frauds targeting businesses and organizations. Fraudsters take their time to collect information on their intended targets, so they can send convincing emails from a seemingly trusted source. Fraudsters will infiltrate or spoof a business or individual's email account. They create a rule to send copies of incoming emails to one of their own accounts and will comb through the emails to:

- study the sender's use of language.
- look for patterns linked to important contacts, payments, and dates.

Variations of spear phishing attacks include:

- A business receives a duplicate invoice with updated payment details supposedly from an existing supplier or contractor.
- An accountant or financial planner receives a large withdrawal request that looks like it's coming from their client's email.
- Payroll receives an email claiming to be from an employee looking to update their bank account information.
- Members of a church, synagogue, temple, or mosque receive a donation request by email claiming to be from their religious leader.
- An email that seems to come from a trusted source asks you to download an attachment, but the attachment is a malware that infiltrates an entire network or infrastructure.
- An email that seems to come from trusted source asks you to buy gift cards.

What's in a fraudster's toolbox?

Impersonation:

- Fraudsters will spend time studying how your business and organization works so that when they strike, it will seem credible.

Spoofing:

- The fraudster will either hack into a business or organization's account or spoof one.
- By pretending to be an authority or person of business influence (i.e. senior executive, religious leader, client, Human Resources, Accounting, etc.) they rely on you not questioning the reason behind their request for financial transfers or information sharing.

Urgency:

- In addition to authority, the fraudsters will use urgency to get you to send the money or information before you have time to verify with other people if the request is legitimate.

What's in your toolbox?

Time:

- Don't let a fraudster rush you into making a regrettable decision; there is always time to verify a request. Run the request by your management or the appropriate department. Don't use the contact information provided by the person making the request.

Instinct and reason:

- If a request is unusual, look into it before completing it.
- If you are contacted by someone who wouldn't normally contact you, like a senior official, look into it.
- Take a few seconds to hover over an email address or link and confirm that they are correct.

Privacy and security:

- Restrict the amount of information shared publicly and show caution with regards to social media.
- Avoid opening unsolicited emails or clicking on suspicious links or attachments.
- Create strong passwords and update them regularly.
- Routinely update computer and network software.
- Consider getting your business certified with CyberSecure Canada.

Business procedures:

- Put in place detailed payment procedures.
- Encourage a verification step for unusual requests.
- Establish fraud identifying, managing and reporting procedures.

Employee awareness and training:

- Remain current on frauds targeting business and educate all employees.
- Include fraud training as part of new employee onboarding.

Learn more tips and tricks for protecting yourself.

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.