CANADIAN ANTI-FRAUD CENTRE

Frauds targeting Businesses 2024-10-22

FRAUD: RECOGNIZE, REJECT, REPORT

This Cybersecurity Awareness Month, the CAFC is dedicated to helping protect your business and stay one step ahead of emerging frauds. From social media spoofing, business email compromise, payment redirection to ransomware, the threats are real and evolving. It's more important than ever to be aware, stay vigilant and protect your business against these growing risks.

Social Media Business Account Spoofs:
Business social media accounts are increasingly being spoofed by fraudsters. With the cloned or imposter accounts, fraudsters can target existing contacts and followers' clients and employees with fraudulent messages and offers. For instance, they can send messages to existing contacts and followers (identified on the legitimate company's profile) and make claims that they have won a free giveaway or contest. In order to collect their winnings, potential victims are required to provide their credit card information.

Top Tips to Protect Business

- Secure your social media accounts. Understand the terms of service for the social media platforms being used.
- Get "verified" on social media. "Verified" accounts provide a level of authenticity and credibility.
- Routinely monitor your social media accounts for unusual post and messages.
- Think about the information you share. Can it be used to create imposter accounts or solicit your clients and employees with fraudulent requests or offers?
- Routinely search social media platforms for imposter accounts.
- Provide clear instructions or details on any promotions, contests or giveaways.
- Provide fraud awareness messaging to clients and employees.
- Post warnings if, and when, spoof accounts are identified and report them to the platform.
- Learn more tips and tricks for protecting yourself.

Spear Phishing Fraud and Payment Redirections:
In these frauds, perpetrators 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 and create a rule to send copies of incoming emails to one of their own accounts. They will comb through the emails to: study the sender's use of language and to look for patterns linked to important contacts, payments, and dates.

Fraudsters launch their attack when the owner of the email account can't be easily contacted by email or by phone. It may look like a top executive sending an email to their accounts payable department requesting an urgent payment to close a private deal or it may look like an email from existing contractor providing new payment directions and requesting payment of an invoice.

Top Tips to Protect Business

- Remain current on frauds targeting businesses and educate all employees
- Include fraud training as part of new employee onboarding
- Put in place detailed payment procedures including verbal authentication for any urgent requests or changes in payment details
- Encourage a verification step for unusual requests
- Establish fraud identifying, managing and reporting procedures
- Avoid opening unsolicited emails or clicking on suspicious links or attachments
- Take a few seconds to hover over an email address or link and confirm that they are correct
- Restrict the amount of information shared publicly
- Upgrade and update technical security software
- Learn more tips and tricks for protecting yourself

Ransomware:

Most ransomware incidents start with a email phishing or spear phishing attack. The email will contain an attachment which can be an executable file, an archive or an image or a link. Once the attachment is opened or the link is clicked, the malware is then released onto the user's system. The malware can remain dormant for many days or months before files or systems are encrypted or locked. Other ways networks and devices can be affected are:

• Visiting unsafe, suspicious or compromised websites;
• Inserting an infected external device (USB drive) into a device;
• Exposing the systems to the internet unnecessarily or without robust security and maintenance measures.

Top Tips to Protect Business

• Be cautious of any unsolicited email;
• Do not respond to suspicious emails and do not click on any links in them;
• Ensure a backup plan for your data that is consistent and frequent;
• Use multi-factor authentication and anti-malware software;
• Ensure regular software and system updates/patches as well as frequent system-wide password changes;
• Publish and enforce an employee security policy;
• Work with law enforcement when developing and testing an incident response plan;
• Report, report, report!
• Visit the CAFC for more tips and tricks for protecting yourself;
• Visit the Canadian Centre for Cyber Security for additional information on ransomware and cyber security advice, guidance and services.

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 you are not a victim, it is still important to report the incident to the CAFC as reporting can prevent further harm.