CANADIAN ANTI-FRAUD CENTRE BULLETIN

Success Story: CAFC and USSS freeze $615,820 2024-02-21

FRAUD: RECOGNIZE, REJECT, REPORT

On February 2, 2024, the Canadian Anti-Fraud Centre (CAFC) and the United States Secret Service (USSS), along with a financial institution froze a $615,820 fraudulent transfer. Since 2021, the USSS has assisted the CAFC in returning more than $3,000,000.00 to U.S. and Canadian citizens.

The victim's funds were frozen after a Canadian business reported to the CAFC that it was a victim of spear phishing fraud. As a result of the timely reporting, the business is well positioned to recover its funds.

Spear phishing fraud is one of the most prevalent frauds targeting businesses and organizations. In 2023, Canadian businesses reported losing more than $58 million to spear phishing fraud.

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 an accounts payable invoice has been identified.
It might look like a supplier or contractor sending an email to the customer's (victim) accounts payable department requesting an urgent payment to an alternate bank account for an invoice that is due. Fraudsters might set up a domain similar to the company's and make it appear as though the email is originating from a trusted source.

How to protect yourself

- 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 and show caution with regard to social media
- Upgrade and update technical security software
- Learn more tips and tricks to protect yourself

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