FRAUD AWARENESS

FRAUD TARGETING BUSINESSES AND ORGANIZATIONS

SUMMARY: Fraudsters are targeting businesses and organizations, including municipalities. Techniques used are commonly known as '*Spear Phishing*', '*Whaling*', '*Vishing*' or '*Payment Redirect*' scams – all aim to have the business or organization send funds or redirect payments to fraudsters posing as service providers, contractors, law firms, or business associates. Funds have been known to be sent to foreign accounts with very little recourse in getting the money back after the fraud have been discovered.

METHODS: Emails, texts, or phone. It may involve some form of 'social engineering' and/or data breach through hacking. 'Social engineering' is the act of trickery to obtain sensitive information through various innocuous means such as phone calls, emails, or open-source information. The information that is obtained is used by fraudsters to pose as a legitimate business or organization that have pre-existing financial dealings with the victim.

PREVENTION: This is not an exhaustive list but as an organization, it is vital to establish a system to protect your network, safeguard your information, and train your employees.

- Establish, maintain, and update security protocols for technology (requires specialized assistance).
- Hackers exploit vulnerabilities in an organization's hardware and software ecosystem.
- Firewalls, virus and malware protection, types of devices allowed to connect to work equipment, methods of authentication, password change protocols, use of work email protocols, personal vs work use of technology, and encryption are just some of the issues to consider.
- Establish redundancy and segregation of duties for financial payments – authorizing and making payments should not be done by one person. Payments should require dual signatories.
- Establish protocol for multi-step verification for any change in payment information request.
- Establish fraud identifying, managing, and reporting procedures.

WATCH OUT FOR:

- 'Spoofing'. Fraudsters have employed 'spoofing' techniques to make it look like it is coming from a legitimate phone number, email address, or website of businesses that you have dealings with.
- Pay close attention to minor errors in the email address or website URL. These errors can occur at the header or the body of the email text. Hover over the email address on the header, it may reveal the real email address.
- The body of the email may appear to have parts that are copy and paste.
- Be suspicious of payment redirect or wire transfer requests to foreign accounts. Especially when the business's country of origin and payment destination do not match.

EXAMPLE: An organization discovers that their network has been hacked. They suspect the hack was from a phishing email that employees have opened. The threat was believed to have been mitigated but almost a year later the organization discovers that they had unwittingly sent a large electronic funds transfer (2 million) to a foreign account belonging to the scammers. The scammers had posed as a client and the client's lawyer. It appears the scammers took the time to monitor the email traffic, gathered the pertinent information on the impending payment, and *spoofed* both the client's, as well as the client's lawyer's email addresses. Upon closer inspection, the email addresses are slightly different from the real ones. Further, the body of the email communications contain cut-and-paste sections from older emails and other minor errors. In this case, the organization could have avoided being victimized if they had separated the authorization and payment duties, type or copy the email address from their contact list instead of hitting the "reply" button, and called the client and the client's lawyer to confirm the information on the email communications.

WHAT TO DO:

- Stay informed on fraud trends and educate all your employees.
- Report incidents of fraud to police and the CAFC.
- Check the Canadian Anti-Fraud Centre (CAFC) to learn more.

https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

RCMP ROYAL CANADIAN MOUNTED POLICE

RCMP 'E' Division Federal Policing Prevention and Engagement (FPPE) *E_FEDERAL_FPPE@rcmp-grc.gc.ca*