RCMP
ROYAL CANADIAN MOUNTED POLICE

BUSINESS E-MAIL COMPROMISE (BEC) BULLETIN

Recognize, Reject and Report it!

*According to recent cybercrime statistics, BEC has stolen more than **$5 billion** dollars from unsuspecting victims worldwide, including Canadian businesses[i]. BEC is the second highest for monetary loss out of over 40 fraud types reported to the Canadian Anti-Fraud Centre (CAFC). It's real, it's growing, but with increased awareness, it can be prevented.*

Bulletin 3. Version 1.0
March 2018

RECOGNIZE IT!

What is BEC?

BEC, also known as CEO fraud, wire fraud, or business executive scam, is a sophisticated scheme that tricks a business into paying a sum of money to a fraudster. The BEC scheme is executed through the use of social engineering[1] or computer intrusion techniques. Several types of BEC schemes have been observed in Canada:

- **BEC scheme #1:** Involves spoofed[2] or compromised[3] e-mail accounts belonging to high-level executives where an e-mail is sent from that account to another employee, often someone who conducts financial transactions for the company, requesting them to conduct a wire transfer for what appears to be a valid business reason.
- **BEC scheme #2:** Involves businesses that have well established relationships with suppliers. The criminal, using a spoofed or compromised e-mail account of the business, requests the supplier to provide payment via wire transfer to a fraudulent account.
- **Other BEC scenarios:** These include: requests for data such as tax information to later be used for fraudulent activity; requests for a "legitimate" invoice payment only to be discovered as false when the actual vendor calls seeking status of an invoice payment; and malicious actors contacting businesses and disguising themselves as lawyers claiming to be handling confidential or time-sensitive matters. There are additional variations of BEC, with new schemes being developed regularly.

REJECT IT!

How can I protect my business?

- Focus on education and prevention for employees by training them on good security practices.
- Be aware of seemingly legitimate but unsolicited e-mails requesting wire transfers with pressure to act quickly or requests for secrecy.
- Look closely at the e-mail address – it may look similar but is slightly altered: i.e. if the real address is: abc-123@mail.ca, then the spoofed address might be: abc_123@mail.ca or abc123@mail.ca.
- Create intrusion detection system rules that flag e-mails with extensions that are similar to the company e-mail and register all internet domains that are slightly different than the actual company domain. [4]
- Consider a two-step verification process for wire transfer payments. Contact the source through another means of communication (e.g. by phone) to confirm the request is legitimate. Do not rely on e-mail alone.
- Implement a dual-signature system with dual-authentication (the use of a security token), requiring at least two authorized signatures from two different personnel for wire transfers.
- Watch for poorly written communications with obvious grammatical errors or awkward language that is not commonly used in Canada. More sophisticated scams, however, will use familiar language and grammar used in your daily correspondence.
- Know the habits of your clients, including the reason, detail and amount of payments. Beware of any significant changes.
- Never open e-mails or click on attachments from an unknown address as they can contain malware used to compromise accounts.
- Start a new e-mail thread rather than replying directly to an e-mail request to transfer funds.
- Limit the personnel and financial information posted online to social media and company websites, including when a CEO or CFO is on vacation, and the names and positions of financial officers. Fraudsters will use this information to conduct research, time their scam, and develop future targets.
- Ensure all software, including anti-virus software, is up to date on all computers, servers and devices including mobile phones and tablets.

Other measures:

- Be wary of using free, web-based e-mail accounts for your business, which are more susceptible to being compromised.
- Be aware of an increase in phishing e-mails, as this may be an indicator of a future BEC attempt. Ensure all staff know to report these e-mails to the company's Information Technology Security branch.
- Consider using whitelisting for trusted e-mail addresses and/or trusted domains. E-mail from unknown addresses can be blocked or flagged.

1 – The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes (non-technical intrusion).
2 – Email spoofing is the forgery of an email header so that the message appears to have originated from someone other than the actual source.
3 – The e-mail account has been "hacked" into. A fraudster has access to the e-mail account.
4 – This in an increasingly used method and is also called a doppelganger domain name. A doppelganger domain name is a legally registered domain name that has been created by threat actors because it appears to be almost identical to the legitimate domain name of a targeted organization.

BUSINESS E-MAIL COMPROMISE (BEC) BULLETIN

REPORT IT!

How should my business respond?

1. If the e-mail is identified as fraudulent **AFTER** funds have been transferred:

A) **Immediately report** the incident to your financial institution. Share the following information:

- the amount
- the account destination
- other pertinent details from the request
- ask about recalling the transfer
- be sure they contact the recipient financial institution

B) **Report** the incident to local police. Identify the incident as "BEC" or wire fraud. The criminal code offences would be S. 380 (Fraud) of the Criminal Code of Canada (CCC) and/or S. 403 (Identity Fraud), CCC. This is NOT a civil matter. This also applies to cases of attempted BEC.

If a computer intrusion technique was attempted or used, there are additional criminal offences that have been committed such as S. 342.1, CCC (Unauthorized use of a computer) or S.430 (1.1), CCC (Mischief in relation to computer data). Be ready to share all details of the incident.

C) **Consider** developing a plan to respond to media inquiries about any potential loss.

D) **Report** the incident to the Canadian Anti-Fraud Centre (CAFC) online 24/7 at: http://www.antifraudcentre.ca/index-eng.htm, select "Report an Incident", and the link to the "Fraud Reporting System (FRS)", or alternatively call CAFC at 1-888-495-8501, between 9:00 am and 4:45 pm EST Monday to Friday and;

E) **Report** the incident to the Canadian Cyber Incident Response Centre (CCIRC) via **e-mail** at: ps.cyberincident-cyberincident.sp@canada.ca, or visit: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx for more information. CCIRC will assist in mitigation and prevention, especially in cases where a technical compromise may have occurred. Advise CCIRC whether the police have been contacted.

2. If the e-mail is identified as fraudulent **BEFORE** any funds are transferred:
   - Follow steps **1B, 1D and 1E** above.
3. If applicable to your business:
   - Brief senior management and/or board members of the incident.
   - Conduct an internal IT forensic investigation and consider bringing in outside security specialists to assist.
   - Investigate possible security policy violations, and develop a plan to resolve security deficiencies.

We strongly suggest that you REPORT THE INCIDENT for the following reasons:

- Regardless if funds were or were not transferred a criminal act has occurred. Please remember that every report counts and is a valuable tool for investigators.
- If the scam is not reported, there is no record of the incident; therefore the scale and scope of this fraudulent activity cannot be understood or investigated.
- Do not be afraid or embarrassed to report the incident. Perpetrators are using more sophisticated techniques that can deceive even the most informed businesses.

Additional information can be found at:

Get Cyber Safe – https://www.getcybersafe.gc.ca

Competition Bureau – http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html

FBI Internet Crime Complaint Centre (IC3) – https://www.ic3.gov/media/2016/160614.aspx#fn1

Global Cyber Alliance https://www.globalcyberalliance.org

In consultation with:

CALGARY POLICE SERVICE

PEEL REGIONAL POLICE

i – Latest FBI BEC stats found at: https://www.ic3.gov/media/2017/170504.aspx