SECURITY UPDATES

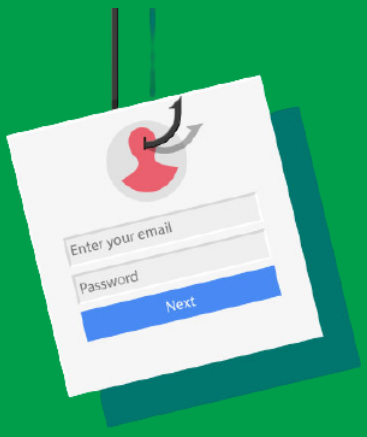
Business Email Compromise (BEC) Edition #2

CHARTERED PROFESSIONAL ACCOUNTANTS BRITISH COLUMBIA

INDEX

What is a BEC?	1
Three Stages of BEC	2
BEC Examples	3
5 Varieties of BEC	4
Defence Tips & Techniques	5

All examples are screenshots of real phishing attempts that CPABC has received



Prepared By Anthony Green - Security Engineer

What is a Business Email Compromise?

Also known as a BEC attack, it is a type of phishing attack in which a cybercriminal impersonates a high-level executive or other trusted contact and uses social engineering techniques to trick an email recipient into transferring funds into a fraudulent account.

CHARTERED PROFESSIONAL ACCOUNTANTS BRITISH COLUMBIA

1. Do the Research

The attacker will identify an organization and/or the targeted individuals. They will then gather information using social media channels, publicly available data, and phone calls, developing profiles they can draw on to create believable communications.

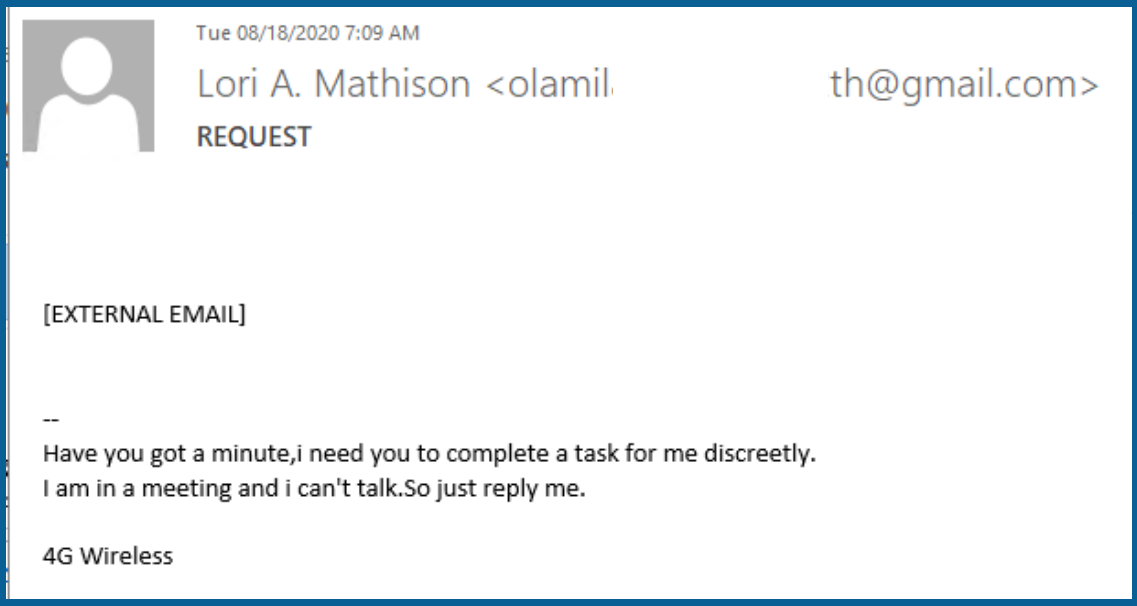
2. Lay the Groundwork

Attackers attempt to build relationships with individuals who have access to financial accounts. They often use a combination of phone calls and "spoofed" or hacked email messages, which appear as though they are coming from a trusted source (like a CEO,CFO, or firm). Multiple communications can take place over days, weeks, or even longer in order to create a sense of trust and familiarity.

3. Set the Trap

Ultimately, the attacker asks the target to initiate a wire transfer for a seemingly legitimate business reason. Because the target believes the attacker is someone they trust, they often act on the request without reservation.

Real Life Phishing Examples



Tue 08/18/2020 7:09 AM

Lori A. Mathison <olamil th@gmail.com>

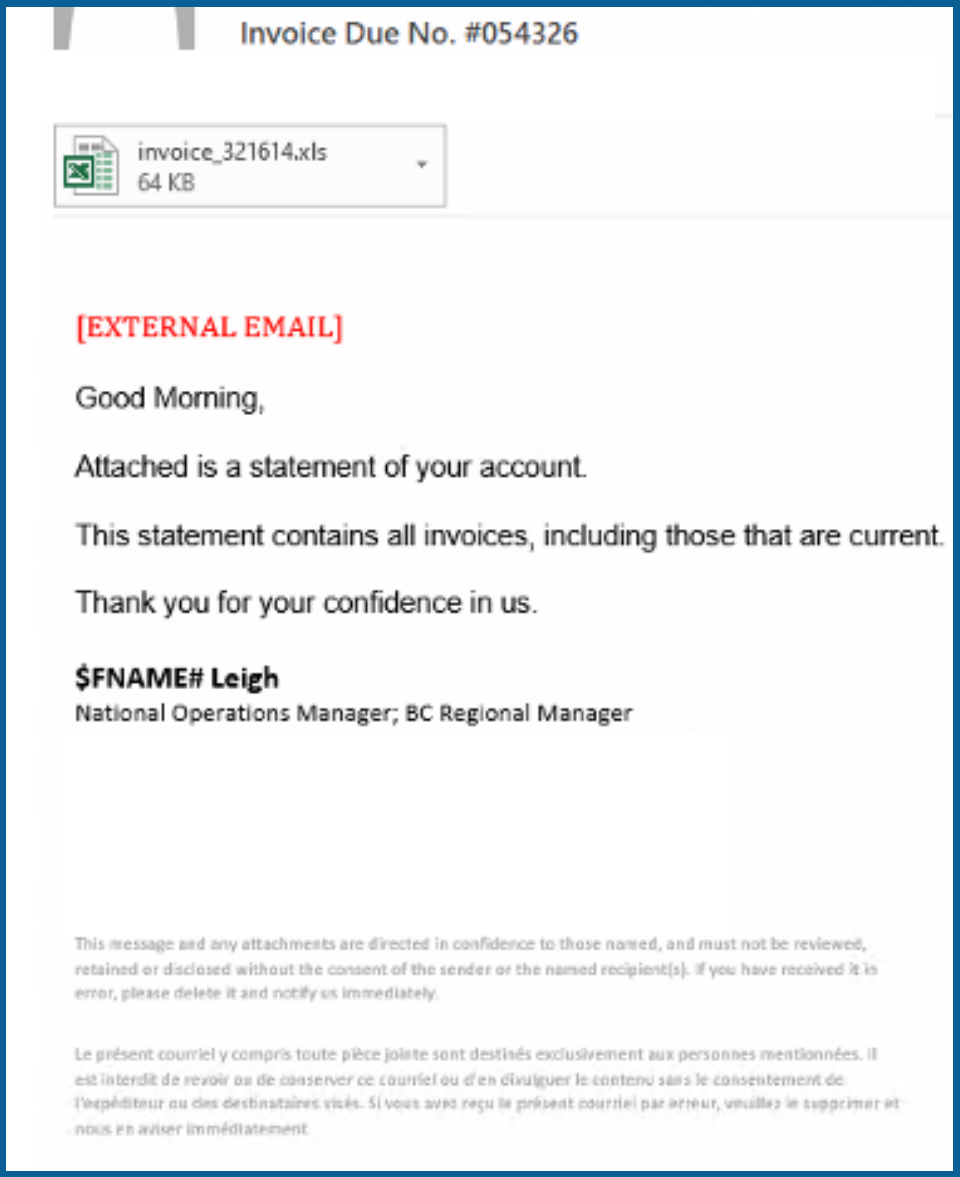
REQUEST

[EXTERNAL EMAIL]

--
Have you got a minute,i need you to complete a task for me discreetly.
I am in a meeting and i can't talk.So just reply me.

4G Wireless

In these 2 examples, you can see that the cybercriminal is reaching out as if they have already created a relationship. In both these cases, the attackers took over the accounts and sent emails impersonating the victim.



Invoice Due No. #054326

invoice_321614.xls
64 KB

[EXTERNAL EMAIL]

Good Morning,

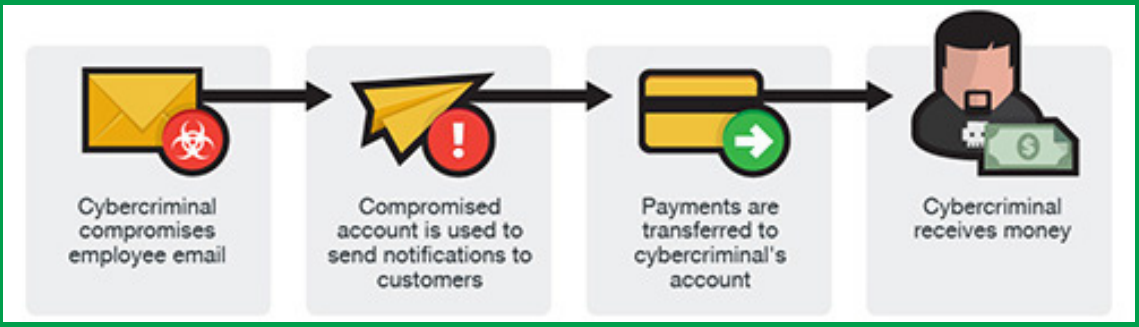
Attached is a statement of your account.

This statement contains all invoices, including those that are current.

Thank you for your confidence in us.

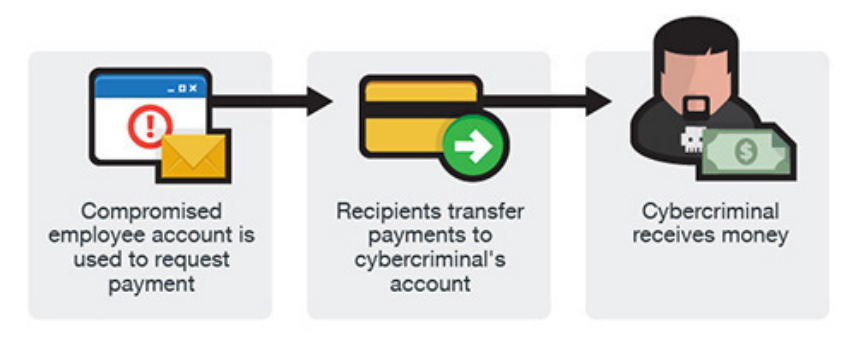
$FNAME# Leigh
National Operations Manager; BC Regional Manager

5 Varieties of Business Email Compromise

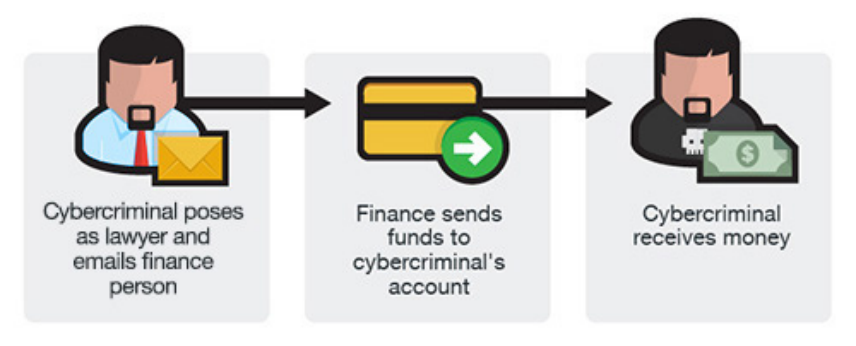


Bogus Invoice Scheme

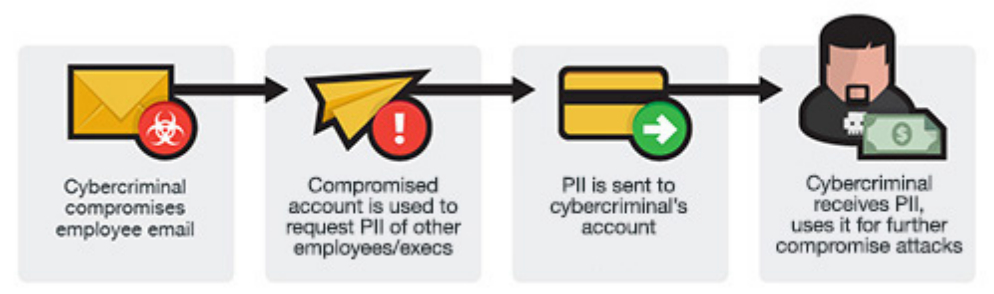
CEO Fraud



Account Compromise



Attorney Impersonation



Data Theft

PII - Personally Identifiable Information

How to Stay Ahead!

Tips & Techniques

- Be careful about your social media posts and connections, consider all information shared to be public and permanent.
- Be on guard with all unsolicited emails and phone calls. Even seemingly small pieces of information - like vendor names and vacation schedules - are useful to cybercriminals.
- Verify originating email addresses and phone numbers when sensitive requests are made. These details can be spoofed by attackers to make them look legitimate.
- Keep yourself protected by using preventive measures such as spam filters, antivirus or anti-malware software, two-factor authentication, and firewalls.
- If you receive an email from a source you know but it seems suspicious, contact that source with a new email or phone call, rather than just hitting reply.
- Report any suspicious-looking emails to your IT department.

Sources:
1. https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise
2. https://www.proofpoint.com/us/2020-cybersecurity-awareness-month-program