Northbridge® Insurance | CYBERSCOUT A TransUnion® Brand

RISK INSIGHTS

BUSINESS EMAIL COMPROMISE: TIPS TO STAY ON TOP OF PHISHING SCAMS

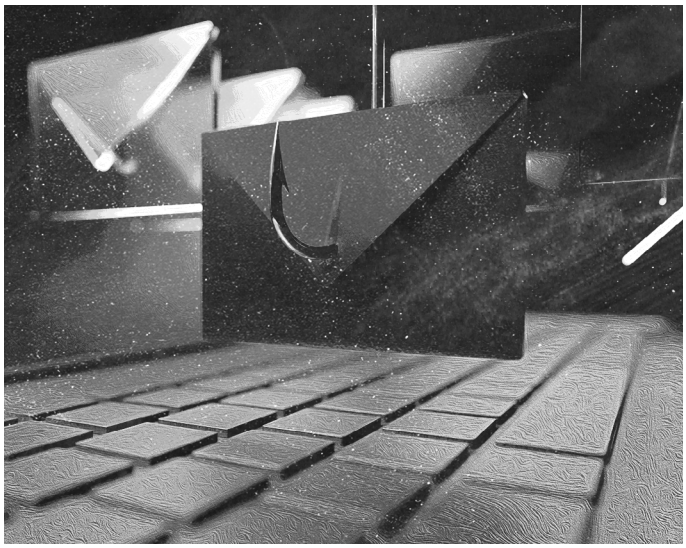
You've heard the old saying: "*Don't open an email from someone you don't know.*" You assume your employees understand how to spot a phishing scam and won't click on suspicious hyperlinks or open unknown attachments.

But what if they receive an email that appears to come from your financial adviser, a trusted vendor or even you?

Business email compromise (BEC) has become increasingly popular amongst cybercriminals seeking money and personal information from companies.

Scammers target businesses that utilize wire transfers and companies that rely on foreign suppliers and third-party vendors or customers. Impersonating these existing, trusted business relationships makes BEC almost impossible to detect and difficult to manage after the fact.

According to recent cybercrime statistics, spear-phishing, which includes BEC, continues to be one of the top reported scams out of about 40 fraud types recorded by the Canadian Anti-Fraud Centre (CAFC). In 2020, the CAFC received reports of almost $30 million in losses to this scam and over $26 million in losses have been reported in the first half of 2021 alone.



FOUR METHODS OF BUSINESS EMAIL COMPROMISE SCAMS

The difficulty in detecting BEC lies in the way scammers use existing professional relationships to gain access to a business' funds or personal information. Criminals use BEC to execute four specific types of scams.

Method #1: business executive scam

CEO's email is hacked or impersonated
The imposter contacts the finance department to request a wire transfer.

Finance department authorizes wire transfer
Request email will typically indicate *transfer must be done quickly and quietly*.

Funds are deposited into fraudster's account
The false wire transfer is delivered to the criminal's fake bank account.

Scammers will use an executive's email address to contact an employee responsible for your company's finances, requesting a large wire transfer into their fake bank accounts. Since most businesses utilize email as their main form of communication between employees and departments, this type of BEC is almost always detected after the transfer occurs.

Method #2: bogus invoice scam

Employee's email is hacked or impersonated
The imposter sends emails through a compromised account to the company's vendors and customers requesting false invoices.

Customers and vendors pay false invoices
Request email will typically indicate *new* or *changed* invoices.

Funds are deposited into fraudster's account
The false wire transfer is delivered to the criminal's fake bank account.

The second method targets your customers or third-party vendors, hoping to collect their money through false invoice requests. Fraudsters can hack into your employees' emails and send out urgent invoices, similar to the method used with overseas suppliers.

Method #3: supplier swindle scam

The third method targets a company's foreign suppliers or overseas vendors in hopes of getting wire transfers authorized to a fake account. Criminals hack into a supplier's email account and request a wire transfer to a "*new*" account, disclosing that the supplier's location overseas has moved or changed.

Method #4: personal data scam

Human Resources' email is hacked or impersonated
The imposter uses a compromised account to request personal information.

Employees send sensitive documents or fill out fake online forms
Request emails will typically indicate that information was never collected, lost or needs to be updated.

Fraudster obtains personal information
Personally identification information (PII) can be used to steal identities or sell on the black market.

Unlike the first three methods, this final method focuses on stealing employees' personal information. Fraudsters target the human resources' email accounts to obtain **personally identifiable information (PII)**. Emails are sent from an HR representative's hacked email account to other employees, asking them to either provide or verify their sensitive information.

TIPS TO PROTECT YOUR BUSINESS

Business email compromise scams can have many layers of potential compromise and can impact anyone associated with a business. By following these tips, you can help keep yourself, your employees and vendors in the know about BEC and other business scams:

1. **Develop and implement a company-wide security awareness program**
   Make it everyone's business to protect company information.

2. **Don't rely on email alone for transfers**
   Confirm requests for transfers of funds by using phone verification or face-to-face meetings. Use known phone numbers to authenticate transfer requests and verify the requests in person whenever possible.

3. **Carefully scrutinize all email requests regarding the transfer of funds**
   Check for small variations in the email addresses that are out of the ordinary.

4. **Harden your networks, especially for mobile**
   Threats to mobile devices may include spyware, unsecured Wi-Fi connections, and even fake networks. As employees use personal mobile devices for business email and other work purposes, cyberthieves often target them to create gateways into your network.

For more information on making your business safer, contact your broker or visit us at **www.northbridgeinsurance.ca**.

> Spear-phishing, which includes BEC, continues to be one of the top reported scams out of about 40 fraud types recorded by the Canadian Anti-Fraud Centre (CAFC).

[4040-001-ed03E | 04.2023]

Northbridge® Insurance | CYBERSCOUT® A TransUnion® Brand