Business Email Compromise

What you need to know and how to protect yourself

Overview

Criminals are always looking for ways to target your business and Business Email Compromise (BEC) is another type of attack you need to be on the lookout for. According to the Canadian Anti-Fraud Centre, Spear Phishing and BEC accounted for over $14.5 million dollars in losses in 2020 with close to 500 victims.[1] Find out how to minimize the impact your business bottom line, and how to prevent your employees from falling victim to BEC.

Business Email Compromise, also known as BEC, is a type of phishing attack where criminals use impersonation in order to gain access to funds. Executives within the company, employees or even other companies like suppliers or vendors, are examples of commonly impersonated parties. This type of scam is not new but has evolved over time taking advantage of our increased online presence to conduct business.

How Does it Work?

Criminals will attempt to impersonate vendors, colleagues or your business leader and try to convince you to send money or confidential information to them. They will try to trick you by using different techniques such as lookalike domains or email address that are meant to fool you into thinking it comes from a reliable or recognizable source. For example, the email address accounts.payable@1nterac.ca could be easily overlooked and appear coming from a legitimate email address from Interac. The criminal impersonating a vendor would attempt to convince the employee they need payment and to send it to this new email address set-up for all new invoices.

Business Email Compromise can take on many forms however here are the most popular types:

- **CEO Fraud:** Here the criminals represent themselves as the CEO or executive of a company and typically emails an employee who has responsibility to remit payments on behalf of the company, requesting them to send funds urgently and confidentially to a specific beneficiary.

- **Email Account Compromise:** An employee's email account has been infiltrated and the attacker sends funds to a fraudulent account.

- **False Invoice Scheme:** The criminal impersonates an existing supplier often within the same invoice giving notification of a change/different bank account which is controlled by the criminal.

Business Email Compromise

What you need to know and how to protect yourself

How to Protect Yourself and Your Organization:

- **STOP:** If someone is asking an "out of the norm" request for confidential information or money, take a moment to reflect and ask yourself why someone would change the current process.
- **SCRUTINIZE:** Is this an unusual request that is asking for a change to established processes/ protocols and does your instinct tell you something is off? Verbally verify any changes to existing payment details.
- **SPEAK UP:** Ask additional questions to confirm the legitimacy of the sender and the nature of the request. Validate the information with colleagues and report it to law enforcement if it is confirmed fraudulent.

How To Protect Your Organization and Employees:

- Set up multifactor authentication and have more than one employee responsible for approving outgoing transactions.
- Hold regular employee awareness training. Make cyber security awareness a priority with monthly training including password security and best practices.
- Reach out to your financial institution and ask them how they can help protect your organization.

The protection of your organization, employees and customers should remain top of mind. Share this information with your staff and vendors to remain vigilant against Business Email Compromise fraud.

[1] Canadian Anti Fraud Centre February 2021