Protecting Your Company from the Growing Cyber-Threat of Business Email Compromise

Highlights

Learn how to minimize the threat of Business Email Compromise (BEC) scams to your business.

- BEC scams are sophisticated crimes targeting organizations that fraudulently induce employees to make funds transfer payments as a result of an impersonation of another employee (typically a manager), vendor, or customer
- They are carried out when a legitimate business e-mail account is compromised through social engineering or computer intrusion techniques

The FBI's Internet Crime Complaint Center reports that there have been more than 166,000 BEC incidents across the globe between June 2016 and July 2019, with more than $26.2 billion lost.

As the use of technology in banking increases, risks associated with cyber security also increase. Companies (owners/leaders, employees and even directors) must become well informed of these threats so that they can take actions to minimize the risk such scams pose to their businesses' operations, customers and overall reputations.

What are cyber-criminals doing to target banking information?

Scammers employ many methods to steal bank and other account login information. Email phishing and Imposter Fraud/ Business Email Compromise (BEC) are the most common. In one phishing approach, the scammer sends an email made to look like it is coming from a legitimate source, such as a vendor, financial institution, or even a colleague. The email includes an urgent call to action such as an account alert, request for payment, or a request for information. In all cases the recipient is encouraged to click on a link in the email- setting off a potentially damaging chain of events.

When the link is clicked on, the recipient is directed to a legitimate-looking website designed to copy the look of a financial institution. The individual is prompted to log in with their normal user ID and password credentials. The fraudster captures these credentials and personal information so they can pose as you on the real website and proceed to drain your funds or spend your money.

With their experience and success, phishers continue to perfect their techniques for disguising their emails and making them look more authentic, even personalizing them with information about you they find on the web. They send out thousands of these fake emails each day knowing that someone is going to bite.

Highlights

Business email scams can occur through:

- Businesses working with a foreign or domestic supplier
- Business executives receiving or initiating a request for a wire transfer
- Business contacts receiving fraudulent correspondence through compromised email
- Business executive, vendor and attorney impersonation
- Data theft

Informed employees and clear policies are the top ways to deter BEC fraud!

Source: Advisen, Ltd.

Common 'Red Flags' of a BEC Scam:

- A vendor/trusted business partner claims to change their bank and needs payment asap
- An urgent email from the business owner or senior executive about a late payment with new or updated wire/ACH instructions or requesting sensitive information (i.e. payroll file)
- A supplier asks for payment and gives account information, different from what is on file

What is Imposter Fraud/Business Email Compromise?

Imposter fraud occurs when a criminal (typically using email) pretends to be from a place you trust (e.g., vendor, business partner, etc.) and tricks you into sending them money and/or revealing personal information. Typically, criminals research the identity of a senior executive, owner, or business partner of the trusted party they want to impersonate, as well one or more employees responsible for managing a company's funds or with access to sensitive information. The criminal then impersonates the executive's or business partner's email address, sending a fake message to the targeted employee requesting an urgent transfer of funds to a fraudulent account number. Recently, the criminals are compromising the actual email account of the person they wish to impersonate to increase the success of the fraud.

These scams are sophisticated social engineering techniques that exploit human weaknesses and trusted relationships. Targeted employees are generally fooled by the urgency of the request (i.e. the executive is travelling or in a meeting) or a "chain of command" mentality and fulfill the request not realizing it is fraudulent. The employee acts without following procedures to validate the identity of the email sender or the request itself causing significant damage.

Business Email Compromise (BEC) scams target businesses of all sizes by deceiving employees with fraudulent email requests. The BEC scam is so effective that the FBI estimates that over $12 Billion has been stolen from legitimate businesses over email alone.

How does the BEC scam work?

The scam typically begins one of two ways:

1. You get a "spoofed" email that appears to come from a trusted source, but is actually a fake email account. The criminal asks you for something you may be able to assist with like sending an urgent payment or updating account information for a transaction.

2. You get an email from a hacked account of a company executive, business partner, or a vendor/supplier.

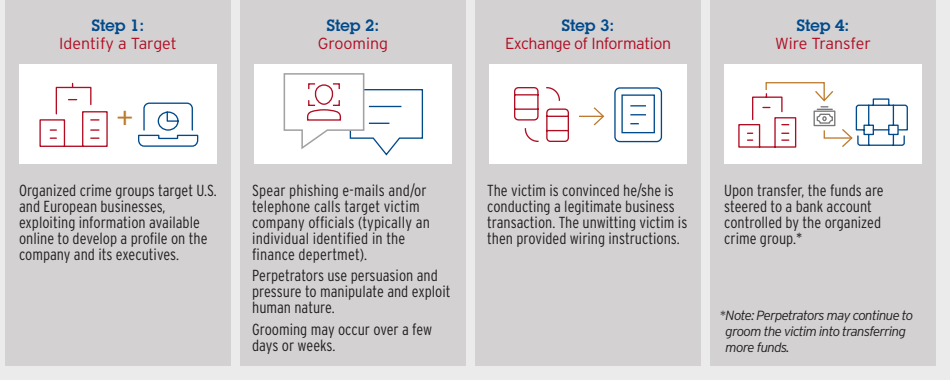
In both emails, the criminal asks you for something you may be able to assist with like sending an urgent payment or updating account information for a transaction. Similar scams have also been seen using SMS (text) messaging in addition to email.

What happens if I accidentally make a payment to a cyber-criminal?

Imposter and BEC frauds often request payments through wire transfers or ACH transactions. These payment methods involve a bank account number, a bank's routing number, and an authorization. If a scammer is able to obtain that information, he can attempt a fraudulent wire transfer to move the victim's funds into his own account. Once the money has been transferred, it usually cannot be reversed.

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups



Source: O'Reilly/Erdal Ozkaya

Highlights

Steps to take to minimize risks:

- Stay vigilant—continually reinforce employee training and awareness
- Pay attention to 'urgent' transaction requests or changes from company leaders and business partners. Require two employees to review and approve all transaction requests, including account changes
- Be wary of any communication that is exclusively email based; Validate transaction requests or changes via phone or in person with the requestor using contact information on record (do not reply to the e-mail)
- Check the full email address on any message and be alert to hyperlinks that may contain misspellings of the actual domain name

If you believe you are a victim of such a fraud, contact local law enforcement and your financial institution immediately. Unfortunately, there is typically little chance of recovering the funds once the transaction is made, because criminals immediately move the funds to a different account.

How can businesses better protect themselves from BEC Scams?

First and foremost, awareness. If something seems amiss, employees should trust their instincts and verify any request. Contact the requestor in-person or over the phone to confirm that any request for funds transfer is indeed legitimate.

It is important to know that these scams are not just an Information Technology problem. Because these frauds rely heavily on social engineering, employees, business owners and even outside directors need to be aware and ensure processes and policies to verify the legitimacy of payments and transfers or the sharing of information are in place and followed diligently.

Additional actions to take to protect your business:

- Don't supply login credentials or personal information in response to a text or email.
- Regularly monitor financial accounts.
- Review and update list of all individuals with authorized access to bank accounts, at least annually.
- Keep all software and systems up to date, and consider using an email security solution to detect and block email threats

Where can I get more information?

www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

www.ftc.gov/system/files/attachments/business-email-imposters/cybersecurity_sb_business-email-imposters.pdf

www.peoples.com/peoples/Footer/Security-Center/Security-is-Our-Focus