Dollar Bank

Business Insights

The Growing Threat of Business E-mail Compromise:

Scammers hijack e-mail accounts, deceive employees and exploit accounts payable processes

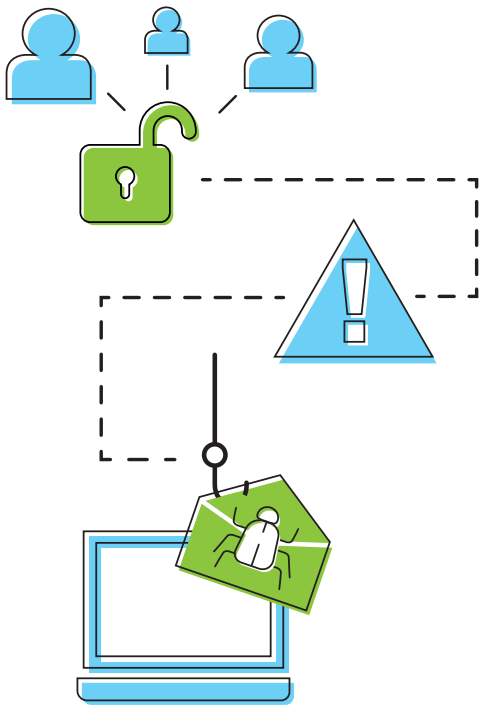
- Common BEC Scams
- Precautionary Measures

Business e-mail compromise (BEC), also known as e-mail account compromise (EAC), has become one of the most common types of fraud among businesses of all sizes. From 2017 to 2018 alone, financial losses resulting from BEC scams nearly doubled, to a reported $1.2 billion, according to the FBI's Internet Crime Complaint Center (IC3).[1] And while early BEC scams were limited to "CEO fraud," hacking the e-mail accounts of companies' top executives, today's BEC perpetrators have broadened their reach, targeting the business e-mails of employees regardless of their positions, as well as personal and vendor e-mails.

Here's how BEC has evolved: In 2013, complaints to the IC3 routinely involved hacked or spoofed CEO or CFO e-mail accounts. Perpetrators would send out messages through these accounts that would appear to be coming directly from the targeted executive, usually asking for wire payments to be sent to fraudulent accounts. Often this was done with a mobile signoff, such as "Sent from my tablet," so that the cyberthief would not need to know how the executive's official signoff appeared (an error could raise suspicion from the recipient), and to convey a sense of urgency so that the recipient would comply quickly, without verifying the validity of the request. This type of scam is referred to as "CEO fraud."

Today, CEO fraud continues to be a threat, but BEC criminals are developing more varied and sophisticated schemes to stay a step ahead of their victims. Through careful planning and social engineering finesse, scammers are thoughtfully selecting their victims (usually employees with access to company finances or payroll data), posing as someone they're not by creating authentic-looking e-mails, and then convincing their unsuspecting victims to divulge confidential information or transfer funds into the hands of the perpetrator.

Here are descriptions of several common BEC scams, followed by some of the precautionary measures you can take to protect your business from this type of illegal activity.



Common BEC Scams

- A perpetrator poses as an established supplier and requests immediate payment for an outstanding invoice but provides payment instructions that direct the payment to their own account. Similarly, a bogus vendor e-mail might announce a change in payment instructions. When the employee recipient makes this change, they unwittingly redirect funds to an illegitimate account.

- A scammer hacks the e-mail, including the address book, of a company decision-maker and directs an employee to make invoice payments right away to multiple vendors. These payments are then intercepted by the cybercriminal, and the crime isn't likely discovered until the vendors start asking where their payments are.

[1]2018 Internet Crime Report, Internet Crime Complaint Center, Federal Bureau of Investigations

- An e-mail posing as communication from internal tech support asks employees to click on a link that takes them to a website disguised to be part of the company's intranet. When asked for IDs and passwords, employees might not hesitate. With this sensitive information, the scammer can access payroll records and change payment instructions to direct deposit into their own account.

- In this true account, a scammer researched the target company's payment policies and then, posing as the company's new CEO (whose habits would not yet be familiar to members of the team), e-mailed a finance executive requesting a $3 million cash transfer to a business partner. The executive authorized the transaction without question. But the transfer didn't go to the business partner; rather it went to the scammer's illegitimate overseas bank account.

Precautionary Measures

Educate yourself and your employees. Everyone at your company should be aware of the various types of BEC scams and be able to identify signs of suspicious activity — unusual requests (especially those asking for funds transfers, passwords or other identifying information), signature lines that don't look quite right, requests made from mobile devices, etc. Ongoing security education is important as scams continue to evolve.

Put verification and reporting processes into place. Detail the steps that should be taken for verifying an unusual e-mail request or reporting a suspicious e-mail. This could be as simple as phoning a designated representative within the company to discuss the matter.

Ensure that employees use strong passwords. The easy to remember passwords of yesterday — a child's name and birthday, for example — don't hold up to the rigors of today's cybercrime, especially when used repeatedly. A password manager could help you safeguard accounts and communications by generating, storing, encrypting and retrieving unique passwords for everyone in your organization. Those offering two-factor authentication, requiring employees to enter a code sent directly to their phone, provide additional security. If employees sometimes work remotely, make sure they understand the importance of using strong passwords and two-factor authentication on any devices they use for business purposes.

Look into options for providing additional e-mail security. Among these are DMARC (Domain-based Message Authentication Reporting and Conformance), designed to prevent e-mail abuses such as BEC, and authentication techniques SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail). Also ask an IT or cybersecurity specialist to assess the strength and efficacy of your firewall and antivirus technology, and to recommend security measures employees should take when using a personal computer or device for business.

Powerful Tools Help Protect Your Business from Fraud

Businesses of all sizes are targeted by fraudsters. But smart strategies can help you reduce the vulnerability of your business checking accounts and stay ahead of the scams and schemes that continue to grow more sophisticated every day. Examples of some fraud tools are online banking, positive pay, Automated Clearing House (ACH), remote deposit and business credit cards.

Treasury Management Solutions to Meet Today's Challenges.

We know that the business environment keeps changing, and that having the right tools, backed by personal service, is essential to your company's financial success. Our treasury management solutions are designed to address your cash management, risk and liquidity concerns and to help you manage your finances with greater efficiency, control and confidence.

DollarBank®
Let's get you there.

Dollar.Bank

It's more than your business. It's the foundation of your future.

At Dollar Bank, we understand that your company is much more than a professional endeavor. It's your passion, your motivation — and the means by which you're making all your other dreams come true. That's why it's so important to choose a partner as committed as you are.

Let's talk @ 855-282-3888.