The latest in fraud tactics

(can fool even the most vigilant employees).

Fraudsters are turning to increasingly deceptive schemes to trick employees and defraud businesses. Some of the latest fraud tactics are so convincing and realistic, they raise little to no suspicion — including Business Email Compromise (BEC). With email as the cornerstone of communication in business, it has become one of the most appealing channels to cybercriminals.

What is BEC?

BEC involves email-based fraud schemes. It's an especially deceptive tactic, because the fraudster poses as a known business contact — often a fellow employee or a vendor the victim already works with.

Business email compromise cost victims more than $2.3 billion in losses in 2023.*

How BEC typically works:

Phase 1: Research and Reconnaissance

Fraudsters identify a target organization and gather information on employees, especially those in finance or executive positions. They hack into their email and then learn their internal and external contacts, business routines, and communication style.

Phase 2: Email Takeover

Fraudsters either infiltrate the targeted employee's email account or spoof it, creating a visually similar duplicate by cloning details such as the email header, display name, and signature.

Phase 3: Criminal Communications

Fraudsters send fake emails to potential victims from the hacked account. Targets may include other employees, such as an accounting contact or a customer of the person whose account has been hacked, usually requesting some sort of financial action or sensitive information.

Phase 4: The Payment

The person receiving the fake email recognizes the email address and company name as a contact they often do business with. Since it appears routine and legitimate, they perform the requested financial action.

KeyBank

* Source: FBI IC3's Internet Crime Report 2023.

BEC: A real-world scenario

Most financial institutions have received notice from clients impacted by BEC, and KeyBank is no exception. This is why we're committed to keeping our clients informed of these fraud schemes — so we can help them identify the red flags and take the appropriate preventive measures to avoid becoming victims in the first place. Here's a recent situation where criminals used BEC to defraud a KeyBank business client:

- Our client received an email that appeared to be from one of its vendors, but was actually spoofed by a fraudster.
- The email requested a payment that was large but typical for the vendor. It stated that the vendor's bank account information had changed and provided new payment instructions to our client.
- Since the email appeared to be from a known contact and requested a regularly occurring payment amount, our client authorized the payment without suspicion.
- A few months later, the true vendor notified our client that they never received their regular payment.
- Our client mentioned the new payment instructions, realized they had been defrauded, and contacted Key to to report the fraud.

Tips for protecting your business from BEC fraud

- **Ensure** all employees — particularly those authorized to initiate payments or with access to financial accounts — are aware of BEC, understand how it works, and know what to look for.
- **Enforce** a strict policy never to alter payment instructions without speaking directly to the contact who requested the change and verifying the legitimacy of the request.
- **Require** two levels of approval from authorized employees for all outgoing payments.
- **Scrutinize** all emails that request any sort of urgency, financial action, or sensitive information and confirm the email addresses and domains are accurate.
- **Verify** payment requests and confirm payment receipt via known contact information. **Do not** use any contact information from the emailed request.
- **Monitor** internal accounts frequently for suspicious transactions or unusual activity.

Let's fight fraud. Together.

KeyBank works diligently to try to recover any stolen funds. However, the more time that passes, the more difficult recovery is. If you think your business has been exposed to BEC or other fraud, **contact your banker or Payments Advisor, or call our Fraud Hotline at 1-800-433-0124. Dial 711 for TTY/TRS.**

KeyBank

This document is designed to provide general information only and is not comprehensive nor is it legal advice; particular situations may require additional actions. If legal advice or other expert assistance is required, the services of a competent professional should be sought. KeyBank does not make any warranties regarding the results obtained from the use of this information.

©2024 KeyCorp. All rights reserved. KeyBank Member FDIC. 240819-2739378