Business Email Compromise

What is it?

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or "out of office" messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions.

How It's Done

Fraudster monitors officer's accounts for patterns, contacts and information.

After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account.

Fraudster uses the compromised or impersonated account to send payment instructions.

Payment instructions direct the funds to an account controlled by the fraudster or a money mule.

Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- ✓ Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume it's a cybersecurity problem.
- ✓ Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, payment methods (e.g., ACH to wire), or pressure to act quickly or secretively.
- ✓ Be old-fashioned! Verbally authenticate any changes via the telephone.
- ✓ Review accounts frequently.
- ✓ Initiate payments using dual controls.
- ✓ Never provide password, username, authentication credentials, or account information when contacted.
- ✓ Don't provide nonpublic business information on social media.
- ✓ Avoid free web-based email accounts for business purposes.
- ✓ A company domain should always be used in business emails.
- ✓ To make impersonation harder, consider registering domains that closely resemble the company's actual domain.
- ✓ Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.

> **"The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone. Don't rely on email alone."**
>
> **– FBI Special Agent Martin Licciard[5]**

[5] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

jbt Bank on a Smile.

jbt.bank

Member FDIC

EQUAL HOUSING LENDER