Business Email Compromise (BEC)

Bank of America Merrill Lynch

Business Email Compromise is a constantly evolving trend and it's occurrence continues to rise.

A growing wave of email phishing known as Business Email Compromise is finding success across organizations globally. It makes up nearly 27% of all email fraud.[1] BEC is a sophisticated scam characterized by tricking businesses into making fraudulent changes to supplier and customer accounts and targeting individuals that perform wire transfer payments. Bad actors compromise legitimate business email accounts through social engineering or computer intrusion to conduct the unauthorized transfer of funds.

What you should know

BEC scams are continuously changing

BEC scams continue to grow, evolve and target all size and business segments. Between January 2015 and December 2016, there was nearly a 2400% increase in this type of scam. BEC is reported in all 50 states, in 131 countries and the latest figures show that it's exceeds $12B in total losses since 2013.[2]

Top Email Schemes

- **CEO scam** – a fraudulent message appears addressed from a senior executive within the company to execute a payment.
- **Supplier email** – an email is addressed from a supplier's spoofed email address requesting a change in beneficiary account.
- **Attorney email** – A business acquisition email appears addressed from an attorney with a fraudulent payment account because the bad actor has compromised a third party.
- **Non-financial data phishing scheme** – a spoofed Instruction to send personal information other than payments, like payroll records.

Best Practices

If you receive a suspicious email, be mindful of the following:

If you "don't recognize" the sender:

- Avoid clicking on links or opening attachments.
- Do not "reply" to the email, as you will be responding to a bad actor and not the legitimate contact.
- Report the email to your IT or information security department; suspicious emails can also be sent to: abuse@bankofamerica.com.

Validate using other communication channels.

- Pick up the phone and call the sender using the company directory or vendor information on file. *Do not call the number on the correspondence.*
- If email is necessary due to time differences in geographic location, have another associate draft an email from another PC, using the email address from your company's source documentation to validate the instructions received.

[1] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-email-fraud-yir-180212.pdf

[2] https://www.ic3.gov/media/2018/180712.aspx

Develop procedures for changes to non-standard payment requests.

- Request the old payment instructions *as well as* the new payment instructions.
- Ask the sender to provide past invoice numbers and associated payment amounts to authenticate the new instructions.
- Request the sender to remit the new payment instructions on company letterhead and validate the letterhead.
- Create an approval process for implementing new beneficiary accounts.
- Call the contact with the phone number you have listed in your master vendor file and not the information provided on the email request.
- Develop a process within your organization to flag beneficiary changes to established relationships. Ensure that the individual approving the payments know a beneficiary account has changed.
- Once you have a new vendor relationship, create a communication structure for future beneficiary account changes.

Develop a security culture

It is important to develop a culture in your organization that all individuals feel comfortable taking the necessary time to validate new payment instructions. Associates should always feel as though they are able to double check details if they are unsure of a suspicious email or validity of instructions. Successful programs incorporate recognizing individuals for identifying phishing emails and bringing them to the attention of appropriate parties within a company.

For more information

For more information about BEC, visit our Fraud and Cybersecurity Education site at: www.bofaml.com/fraudandcybersecurity.