

# Business Email Compromise Prevention

## The Latest Tips

More than 400 businesses receive fraudulent emails every day

### TOP EMAIL FRAUD SCAMS:



- #1 CEO scam – Fraudulent message appears to be coming from senior executives within the company
- #2 Supplier email – Email looks like it's coming from a supplier whose email address is being spoofed
- #3 Attorney email – Business acquisition email appears to be sent from an attorney
- #4 Non-Financial Data phishing scheme – Instructions to send personal information other than payments

### WHAT TO LOOK OUT FOR:



The following requests can be signs of a scam, which can have a sense of urgency or a need for confidentiality:

- Change a company profile within an internal system
- Add a new contact representing the company
- Update a payment account
- Request new payment for a business transaction
- Request a sudden change in business practice

### 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. You may inadvertently be communicating with fraudster instead of intended party
- Report the email to IT or information security
- If you have to communicate via email, have another associate create a new email from another PC, using the email address from the source documentation to validate the instructions

#### Validate using other communication channels

- Pick up the phone and call the sender — using the company directory or vendor information
- Ask the sender to send the new payment instructions from the company letterhead and validate the letterhead

#### Develop procedures for non-standard requests

- Create confirmation procedures for non-traditional requests
- Define the approval process for implementing new account number
- Authenticate the request by asking the individual to provide old invoice numbers or payment amounts
- When possible, ask your vendors to acknowledge the payments

[bofaml.com/fraudandcybersecurity](https://bofaml.com/fraudandcybersecurity)

**Bank of America**  
**Merrill Lynch**



\*Bank of America Merrill Lynch\* is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation (“Investment Banking Affiliates”), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA. Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed. ©2017 Bank of America Corporation. AR39BC6N

Source: <https://www.symantec.com/security-center/threat-report>