

CEO FRAUD

A scammer impersonates the CEO (or high ranking executives) then sends scam emails trying to get an employee to transfer funds or confidential information.



ATTORNEY IMPERSONATION

A scammer impersonates a law firm, or someone from a law firm, usually requesting that funds be transferred into an account to settle an 'overdue bill'.



FAKE BILLING

A scammer hacks into the email account of a business that has a relationship with a supplier. They then impersonate the supplier and request that 'unpaid bills' be paid to a 'new' account.



ACCOUNT COMPROMISE

A scammer hacks into the email account of an employee (usually Finance) and contacts customers on the contact list stating a problem with a payment and requesting that payments are made to a 'new' account.



DATA THEFT

A scammer impersonates targeted employees (usually HR) and then sends out requests to employees and executives requesting personal information verification or updates.



5 COMMON TYPES OF BUSINESS EMAIL COMPROMISE (BEC) ATTACK

PHISHING AWARENESS TRAINING AND SIMULATION

www.phriendlyphishing.com

support@phriendlyphishing.com

