Phriendly Phishing

5 Common Types of Business Email Compromise (BEC) Attacks

Understanding the most frequent types of BEC attacks will help keep you and your organisation safe.

BEC scams are used by hackers to access money or goods from companies through fraudulent email, instant message, SMS and social media tactics.

CEO Fraud

A scammer impersonates the CEO (or other executive) and sends scam emails trying to coerce an employee to transfer funds or confidential information.

Lawyer Impersonation

A scammer impersonates 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. The scammer impersonates the supplier and requests 'unpaid bills' be paid to a 'new' account.

Account Compromise

A scammer hacks into the email account of an employee (usually from Finance) and contacts your organisation's customers stating a problem with a payment. Requests include payments are made to a 'new' account.

Data Theft

A scammer impersonates targeted employees (usually HR). The scammer then messages all employees requesting personal information verification and updates.