

Business Email Compromise

Business email compromise, or BEC, is an advanced phishing scam that impersonates people, organizations, or entities that the victim knows. It works by manipulating email addresses so the sender appears to be legitimate.

4 COMMON EXAMPLES OF BEC

1.) FRAUDULENT INVOICES

By impersonating vendors or other account representatives, scammers can trick people into wiring funds to fraudulent accounts. This is often accomplished by sending fake invoices that look almost exactly like an invoice the victim typically receives.

2.) CEO FRAUD

How likely are you to respond to an email that appears to come from your boss? CEO fraud involves a cybercriminal attempting to impersonate upper management and sending out requests for wire transfers of money or confidential information.

3.) ACCOUNT TAKEOVER

When someone falls victim to a phishing attack, they may lose control of their email account. This then allows the attacker to distribute phishing emails to the victim's contact list. Since the recipient recognizes the account, they are likely to engage with the attacker.

4.) EMPLOYEE DATA THEFT

Those who work in bookkeeping or human resources have access to an abundance of employee information. Cybercriminals often target those people in hopes of stealing data such as full names, SSN and ID numbers, home addresses, and phone numbers.



Thwart Attacks By:

Verbally confirming. If you receive a request for payment or confidential information, it's always a good idea to confirm with them via an alternative method before complying.

Not updating information based on an email request. If you receive an email to update information confirm the request with the company using a known source.

Carefully inspecting the sender's email address. Scammers often create addresses that appear to be legitimate but actually contain slight variations in the way they're spelled.

Paying attention to the tone. When you email regularly with someone, you are likely familiar with how they communicate via text. Unusual tone = untrustworthy email.

Avoiding attachments. Email attachments represent one of the most common ways malware gets distributed. Never open an attachment unless you have confirmed it's safe.



Regardless of the delivery method, almost all phishing attacks attempt to manipulate people into doing something they shouldn't, such as clicking a link, downloading a malicious attachment, and revealing confidential information. **DON'T FALL FOR IT! USE EXTREME CAUTION BEFORE YOU CLICK, DOWNLOAD, OR SHARE ANYTHING CONFIDENTIAL.**