

Business Email Compromise

Don't Be the Next Victim

Business owners are becoming the most vulnerable victims and targets for cybercrime.

\$3 Billion

in BEC losses in 2025
according to the FBI

What is it? Business Email Compromise is a fraud scheme in which cybercriminals use **email impersonation** to deceive businesses into sending money or sensitive information.

WARNING SIGNS: BEC INDICATORS

- ✗ Look-Alike Domains**
Slightly altered domains, such as adding a hyphen or swapping characters (for example, replacing an "l" with 1).
- ✗ Fraudulent Payment Requests**
Watch for new or unfamiliar bank details, like "we've changed banks" or "use this new account," without formal notice.
- ✗ Spoofed Email Threads**
Thread hijacking leverages existing trust and context: attackers compromise an account, watch active conversations, then inject a message when it aligns with legitimate business activity.
- ✗ Unusual Tone or Language**
The writing style, grammar, or phrasing does not match how the sender normally communicates.
- ✗ Bad Timing**
Transactions initiated near end of day and before a weekend or holiday.
- ✗ Incorrect Signature Lines**
Incorrect or abbreviated signature lines for the supposed sender.

PROTECT YOUR COMPANY

- ✓ Verify Out-of-Band**
Always verify payment instructions using a trusted method, such as calling a known phone number on file, not one provided in the email.
- ✓ Require Dual Approval**
Require at least two individuals to approve wire transfers, ACH originations, and changes to payment instructions. Strong internal controls help prevent fraudulent transactions.
- ✓ Examine Email Addresses**
Look for slight misspellings, extra characters, or altered domains in sender email addresses. Fraudsters frequently use spoofed or look-alike accounts.
- ✓ Train Employees Regularly**
Provide ongoing fraud awareness so employees can recognize phishing attempts, spoofed emails, and social engineering tactics.
- ✓ Consider Getting Cyber Insurance**
Ask your insurance agent whether a cyber policy can help cover losses from fraud and other cyber incidents.

