NEED TO KNOW NEWSLETTER | SEPTEMBER 2025

Be Aware of BEC!

Everyone knows about phishing attacks. “Click on this message to download important documents right now!” But a specific type of phishing attack targets businesses or organizations through email, and their goal is to drain your resources. This is called a **Business Email Compromise**, or BEC. In this month’s newsletter, we’re pulling back the curtain and showing you the truth about BEC attacks.

All BEC is phishing, but not all phishing is BEC.

Phishing is when an attacker uses fraudulent communications to trick someone into revealing sensitive information. A phishing attack is considered BEC if it specifically uses email to target a business or organization and steal money or data.

Hackers impersonate professional contacts, such as vendors who work with the organization.

The key to a BEC scam is sending a message that their target believes to be ordinary business. For example: impersonating a vendor and telling your organization that the vendor’s payment information has changed. Now your company is paying fake invoices directly to the scammer’s account.

Executives and members of the finance department are the top targets.

BEC scammers want to subvert the people who control the organization or its money. If they can convince an executive to hand over critical data, or talk the CFO into authorizing phony payments, then it’s payday for hackers.

Email accounts can be impersonated or taken over.

To run a BEC scam, hackers may make a near-identical email (john,smith@example instead of john.smith@example) or take over an existing account via malware or credential theft.

Don’t let BEC break your security

- **Verify any unusual requests.** Why is payment data suddenly changing? Is this person who they say they are? Don’t be afraid to ask questions.
- **Are you using MFA?** Multi-factor authentication protects your credentials, making it difficult for hackers to steal them for BEC scams.
- **Don’t be pressured!** Hackers want you to act fast and not ask questions.

How do you lose $46 million?

In 2015, networking company Ubiquiti lost millions in one BEC attack. Hackers impersonated company executives, including its founder, and ordered wire transfers for the supposed purpose of a secretive company acquisition. The company’s chief accounting officer believed the messages, and millions disappeared into scammers’ pockets.