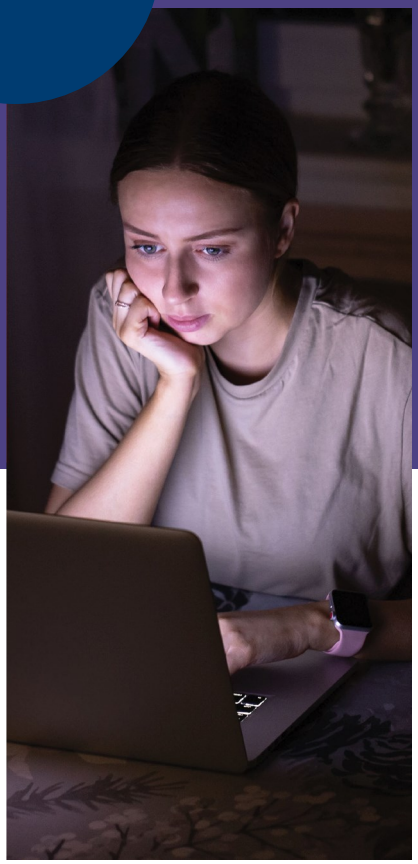
Unmasking the Impostors

How to Protect Your Business from BEC Scams

SECUR-SERV

secur-serv.com



Email is our reliable messenger in today's fast-paced business environment, bridging gaps and facilitating transactions every second. However, this convenience comes at a price – Business Email Compromise (BEC) has become a constant lurking danger.

So, first off, what's BEC, and how can we shield ourselves from it? Let's get down to the brass tacks.

Understanding Business Email Compromise

Let's start with the basics. BEC is when scammers or hackers pretend to be someone they're not to trick employees into sharing sensitive information or transferring funds. Sounds scary, right?

To give you a clearer picture, consider the fictional case of a well-established company that received an email from their "CEO" urgently requesting a transfer of $50,000 to a new vendor. The finance manager carried out the request swiftly, only to realize later that it was a scam. This event is BEC in action — a hoax where criminals play pretend to exploit businesses.

FBI records show domestic and international companies faced a colossal loss of $50 billion due to BEC scams. Moreover, the damage isn't just financial; it can often severely tarnish a company's reputation.

FBI records show domestic and international companies faced a colossal loss of $50 billion due to BEC scams

Identifying and Assessing BEC Risks

How do we spot the red flags? BEC scams often adopt tactics like spear phishing or CEO fraud. For instance, a company received an email from a "trusted vendor" citing an account number change to pay an outstanding invoice. Thankfully, their sharp-eyed manager caught the scam by verifying the information through a direct call to the vendor.

It's a challenging landscape currently, but vigilance can make all the difference. Spotting inconsistencies in email addresses, language use, and irregular requests can be clues to identifying these BEC scams.

Mitigating the Risks

Now that we know what we are up against let's talk solutions. Training is your first line of defense – Period. A study by Stanford University highlighted that 88% of cybersecurity breaches are caused by human error. So, empowering your team to identify and report suspicious emails is essential.

In addition to training, here are some golden rules to live by:

1. **Be careful with what information you are sharing online and social media -** scammers often use information found online to craft believable scams.

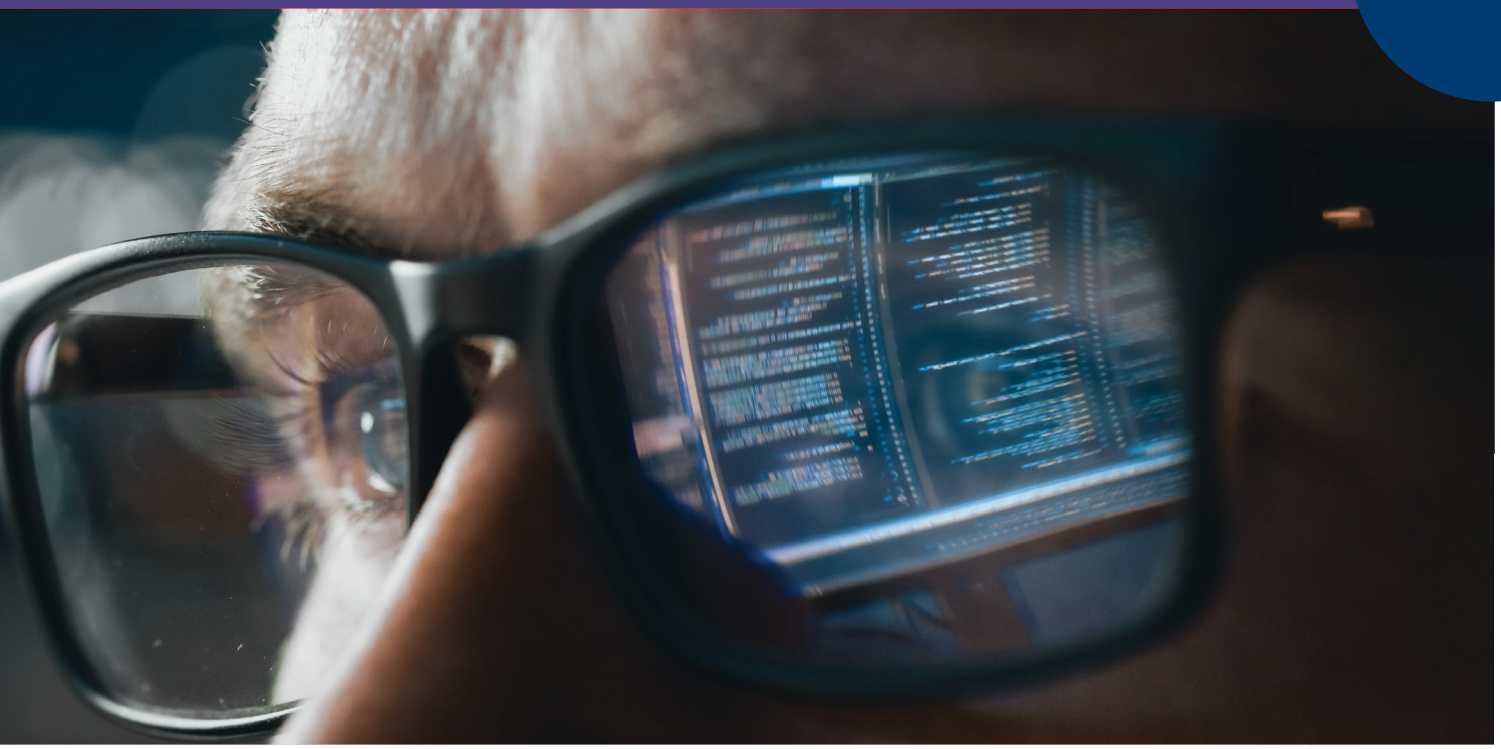
2. **Don't click on anything suspicious -** if it seems off, it probably is.

3. **Carefully examine email address, URL, and spelling that is used in correspondence -** sometimes, a small typo is a dead giveaway.

4. **Be careful what you download -** unwanted downloads can bring along unwanted troubles.

5. **Be wary if the requestor is pressing you to act quickly -** scammers love to create a sense of urgency to trap you.

Beyond training and adopting these rules, having robust technological measures, like email filtering and multi-factor authentication. And remember, always have a protocol for rapid response in case you detect a breach.



Standing Tall Against BEC Scams

In the grand scheme of things, BEC is like a cunning impersonator trying to deceive us in our own homes (well, in this case, in the business environment!). But with a vigilant eye and a well-prepared team, you can stand tall against BEC scams.

Let's work towards creating a safe email culture where we double-check before taking action and keep our business assets secure. **Contact us today.**

SECUR-SERV

800.228.3628

secur-serv.com]