Check yourself:
5 signs an email message might a BEC attack

Business Email Compromise (BEC) scams are a growing threat with devastating financial consequences. In 2024 alone, these attacks led to more than **$2.7 billion** in losses across the U.S.

As cybercriminals increasingly leverage AI to execute more sophisticated scams, it's critical to stay vigilant.

Use this checklist to help identify key red flags of a BEC attack and protect yourself from falling victim to these evolving threats:

1. **Email domain misspellings or atypical sender addresses:** Even minor variations in spelling or punctuation can indicate a compromised or impersonated account. **TIP:** Check the email address, not just the sender's display name.

2. **Requests to switch communication channels:** Legitimate senders rarely ask you to move conversations to another platform. If an email directs you to respond via WhatsApp or another channel, it's likely a scam.

3. **Fake email threads or fabricated history chains:** Cybercriminals often create fake back-and-forth email threads that appear to come from colleagues to build trust and legitimacy.

4. **Unusual tone, grammar, or writing style from a known sender:** Think about how the sender normally communicates and ask yourself, *does this message match*? If intros or basic sentence structures feel off, this could be a sign of compromised access.

5. **Unexpected or urgent requests:** Attackers often create false urgency to get you to bypass standard verification processes. For instance, they may ask you to make an immediate purchase on their behalf. Always verify these requests first.

Realizing you've seen a few of these instances before in your own email?

You're not alone. Protecting your business and employees from BEC attacks requires an intelligent approach that leverages AI for predictive threat prevention. **To find out how you can unify AI-driven insights, automation, and human-centric security, book a demo with us today.**