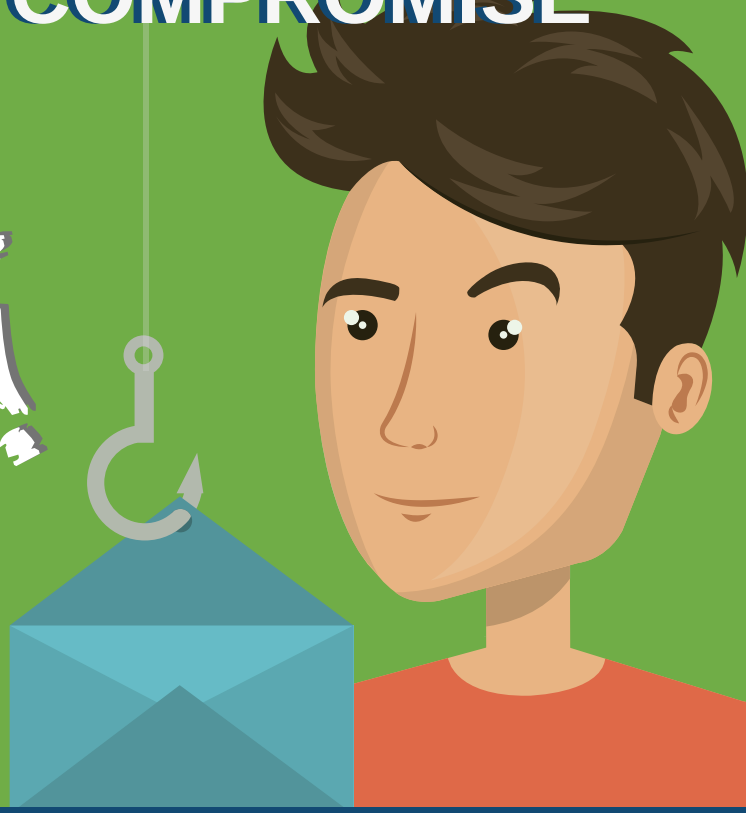


BUSINESS EMAIL COMPROMISE

DON'T BE
A VICTIM!



Business e-mail compromise (BEC) scams have resulted in companies and organizations losing billions of dollars. But as sophisticated as the fraud is, there are ways to thwart it by incorporating the right technology along with face-to-face or voice-to-voice verification.

The FBI Says:

"The best way to avoid being exploited by phishing scams is to verify the authenticity of requests to send money by walking into your CFO's office or speaking to him or her directly on the phone"



SAFEGUARD AGAINST BEC



Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail.



Verify the identity of the sender based on the sender/receiver history and classify email into tiers of trust groups.



Color code virtual correspondence so e-mails from employee/internal accounts are one color and e-mails from external are another.



Verify changes in vendor payment location by adding additional two-factor authentication such as secondary sign-offs.



Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication.



Educate employees about potential attacks using courses and online training at regular intervals.

ATSG

The right partner can help keep your business safe from attacks. Learn more by calling: 1-914-517-2919