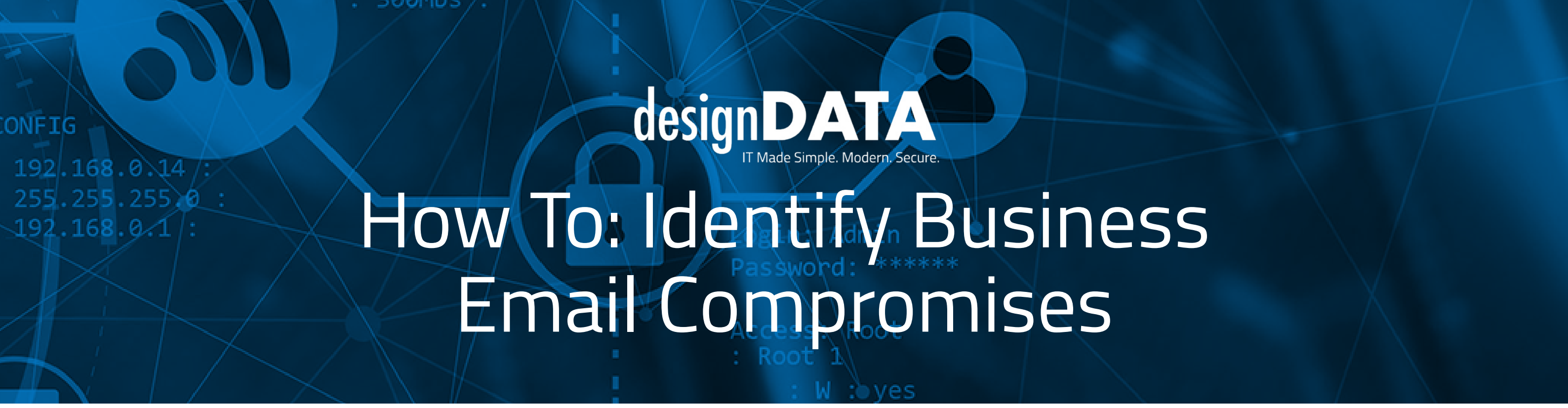

designDATA
IT Made Simple. Modern. Secure.

How To: Identify Business Email Compromises

Business email compromises (BECs) occur when a malicious person gains unauthorized access to an email login and uses that email account to impersonate a trusted individual. With that misplaced trust, they can trick accounting departments into issuing fraudulent transactions, convincing human resource departments to adjust direct deposit information, send false or modified invoices, perform data theft, or deploy malware.

BECs are becoming increasingly sophisticated; many of the tell-tale signs we all recognize in phishing emails, like misspelled words or incorrect domain names, are missing. This can make it nearly impossible for your team members to distinguish BEC emails from legitimate ones.

To address this, here are five crucial tips for identifying business email compromises:

01. Pay attention to the details. BEC email senders often imitate the writing style or word choices of the person they are impersonating, but the way they frame their message may tip you off that the message isn't legitimate. Pay attention to sentence structure and level of formality.

02. Have financial transfer authorization policies in place. Having requirements like **all wire transfers must be verified by at least two people** before being made can stop many BEC attacks in their tracks.

03. Have identity validation policies in place. Even if your CEO is allowed to authorize writing a check without a second approver, you can still have procedures in place to validate the request came from the CEO. If you get such a request via an email, validate it by having a policy that also requires voice validation: call your CEO on the phone to confirm that they issued this request. If you call the sender to validate the request, make sure you call them on a previously verified phone number, not the one the attacker provided to you in their email signature!

04. Resist requests to bypass your policies. BEC attackers often make their requests (like wiring money, writing a check, etc.) with a sense of urgency or request for discretion. Be wary if you receive such requests, even if the sender is familiar, as the attacker may be using social pressures to get you to skip your verification and validation steps. Fostering a culture of following policies correctly, every time, can also help defeat this social pressure.

05. Listen to your suspicions. If an email looks a little fishy, do some validation, even if not required by policy. If you suspect a case of email impersonation or business email compromise, take precautions and immediately notify your IT or cybersecurity team so they can take appropriate action.

Cybercriminals continuously devise new ways to attack companies. To remain confident that your sensitive data is secure, you must stay up to date on the latest cyber attacks and how to defend against them. We encourage you to take advantage of our **free cybersecurity resources**, and if you have questions or concerns about your current cybersecurity strategy, we would love to hear from you.

Talk With a Cybersecurity Expert

1425 K Street NW, Suite 500, Washington, DC 20005   **T:** 240 599 8340   **E:** cybersecurity@designdata.com