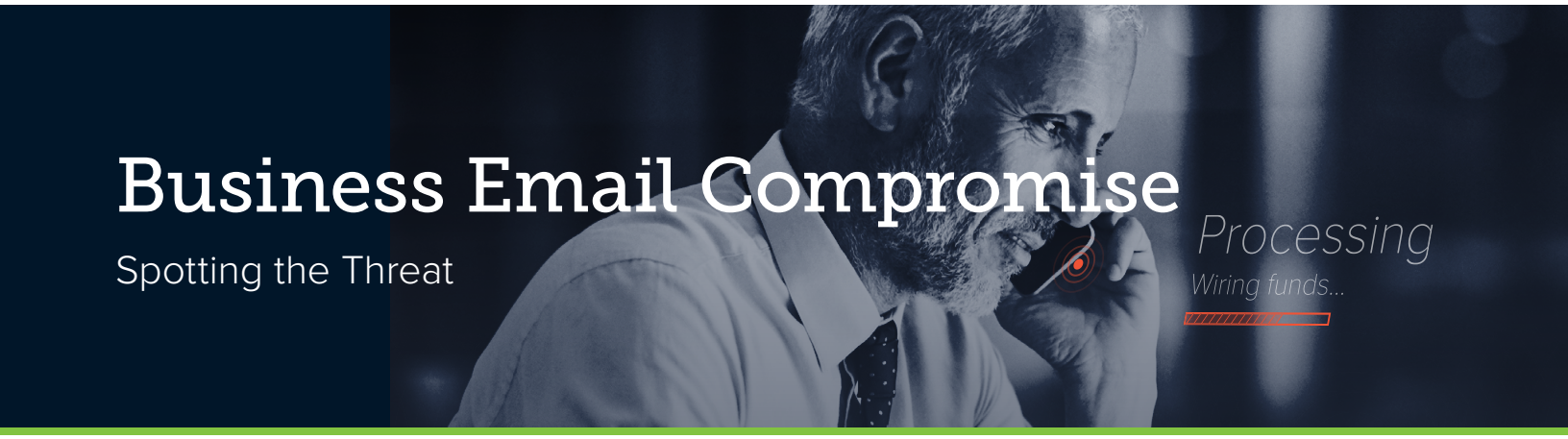

Business Email Compromise

Spotting the Threat

Did you know that the FBI reported $1.7 billion in Business Email Compromise losses in 2019? Here we take a closer look so you can spot the threat before it harms you or your organization.

In Business Email Compromise (BEC) attacks, scammers impersonate an employee in the organization in order to defraud the company, its employees, customers, or partners.

In most cases, attackers focus their efforts on employees with access to the company's finances or personal information, tricking individuals into performing wire transfers or disclosing sensitive information.

These attacks use social-engineering tactics and compromised accounts and are usually devoid of attachments and links found in typical phishing emails.

BEC emails may leverage authority to elicit a response. As such, they often appear to come from the CEO or other high-level executive.

How to avoid becoming a victim of Business Email Compromise:

- Be skeptical if you normally don't get emails from higher-ups.
- Keep calm if the email claims to be urgent.
- Verify the legitimacy of the email by calling the sender.
- Report the email to management or IT if you think it's a fraud.

Example

Hi {email:firstName}

Need your help asap. Someone new at our bank accidentally blocked our payroll account and needs us to verify our information.

Pain in the behind, I know, but could you visit the link below and just make sure our information is correct? We can't make payroll without it. I tried the link but the hotel wifi security settings won't give me access.

http://www.chasebanked.com

Thanks much for taking care of this right away—I appreciate the assist as much as all of us appreciate getting paid on time.

Geez, what a stupid mistake! I'll make sure you get a shout out to senior management for helping fix it.

Let me know how it goes, okay?

Chief Financial Officer
Office of the CEO

◀ Business email compromise scams usually involve urgent requests from 'higher-ups' in an effort to get targets to respond to authority.

◀ A fake domain name, easily overlooked, leads to a fake website that will track and keep account details.

◀ The promise of recognition by senior management is a strong incentive to engage.

◀ A scribbled signature without the printed counterpart is an attempt to look authentic.