BUSINESS EMAIL COMPROMISE

A MALICIOUS SCAM THAT CAN DESTROY ANY BUSINESS

THE THREAT

Business email compromise (BEC) is a sophisticated email scam in which an attacker compromises or impersonates an executive's email account with the aim of obtaining access to sensitive business information or other assets.

ANATOMY OF A BEC ATTACK

Step 1:
Compromised or spoofed executive email account is used to send fraudulent transfer instructions to a finance employee

Step 2:
Recipient transfers the payment to an account controlled by the attacker

Step 3:
Cyber criminal gets paid

THE DAMAGE

Financial loss

Compromise of sensitive data and critical business accounts

Reputation harm

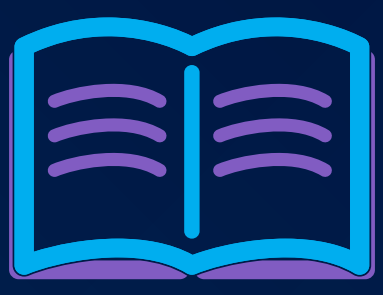
THE NUMBERS

Between 2016 and 2019, BEC resulted in **$26 billion** in reported losses for companies worldwide.

HOW TO BECOME SPOOF PROOF

Protect corporate email accounts with two-factor authentication(2FA)

Educate employees



Verify wire transfers

Most importantly: Implement a threat-ready, multi-layered cloud email security solution

Guardian Digital™

www.guardiandigital.com