4 Ways to Stop Business Email Compromise (BEC) Attacks

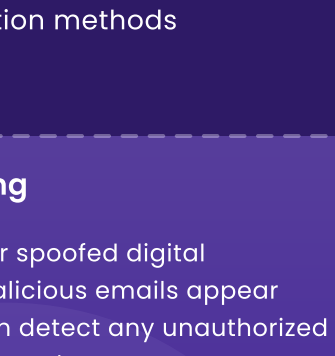
BOLSTER

Over **40%** of Successful Social Engineering Attacks are Business Email Compromises or Imposter Attacks

Almost half of Social Engineering Attacks are **BEC Attacks**

2023 BEC Losses Totaled Over **$2.95B** for Businesses, more than Ransomeware Attacks

BEC attacks cost **6X** more than data breaches



How Attackers Target Your Server

STEP 1

Identify Targets

Ideal targets can be new employees, those connected to HR or accounting, or with access to financial and account data.

STEP 2

Register Lookalike Domain

Next, hackers register domains mimicking a business's legitimate domain; these domains are registered with real hosting providers but obtain some sort of spoofed element to deceive visitors.

STEP 3

Set Up Mail Server

Hackers set up an MX server to enable the messaging process. Registered domains may sit untouched for days, weeks, or months before any activity is registered, making them hard to spot.

STEP 4

Send Email to Potential Targets

Finally, hackers begin contacting unsuspecting victims. Emails may mimic a coworker, executive, or close vendor contact, and can sound urgent in nature.

4 Ways to Stop BEC Attacks

Hackers might be getting more sophisticated, but so are the prevention methods organizations can take.

1 DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) prevents unauthorized use of an email domain by enabling organizations to track the origin of an email and better identify BEC scams.

Cons Attacks can only be identified once they are already in flight.

2 Certificate Monitoring

Attackers often use forged or spoofed digital certificates to make their malicious emails appear legitimate; organizations can detect any unauthorized certificates & take necessary action to prevent BEC attacks.

Cons Monitoring certificates solely focuses on one indicator of BEC attacks.

3 Email Filtering & Anti-Phishing Solutions

Implementing robust anti-spam solutions can help identify and block suspicious or fraudulent emails that are commonly used in BEC attacks before they reach end-users.

Cons Stopping phishing emails as they enter your employee inboxes is a reactive approach once the threat is already live.

4 Bolster

Utilizing AI-detection engines, Bolster identifies the early indicators of BEC attacks. Before emails can hit inboxes, an email server must be established on a lookalike domain. When these nefarious activities occur, **Bolster identifies and takes down phishing websites before emails can be sent.**

Bolster conducts takedown at **STEP 2**

STEP 1

Identify Targets

Ideal targets can be new employees, those connected to HR or accounting, or with access to financial and account data.

The Bolster Answer

Bolster's Multi-Channel Phishing and Scam Protection solution exemplifies a preventative, proactive approach, that stops BEC attacks at the source. With the ability to determine threat levels and conduct takedowns in under two minutes, organizations can remove threats earlier in the attack chain, preventing impending BEC attacks and any lateral attack movement.

Interested in learning more about Bolster, and how we prevent BEC attacks at the source?

Get a Demo →

Read Our Whitepaper →