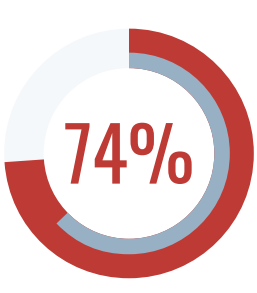
AVERTIUM®
A CyberMaxx COMPANY

BEC ATTACKS HAVE EVOLVED. HAVE YOUR DEFENSES?

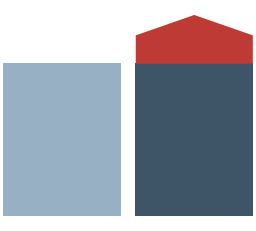
Stop business email compromise (BEC) earlier by disrupting account takeover before fraud impacts your business and erodes trust.

MARKET DYNAMICS

BEC ATTACKS ARE MORE SOPHISTICATED AND CONVINCING



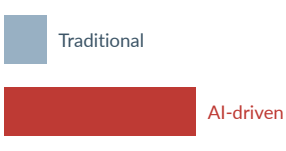
of organizations experienced BEC in 2025, up from 63% in 2024[1]



+32%

increase in identity-based attacks in the first half of 2025[2]

4.5x



higher click-through rate for AI-driven phishing than for traditional phishing[2]

THE CHALLENGE

THE COST OF MISPLACED TRUST

FINANCIAL LOSSES ADD UP

$3B

Reported BEC losses reached $3 billion in 2025, making it one of the costliest cyber threats.[3]

A successful attack can redirect wire transfers, payments, or payroll funds.

TRUSTED IDENTITIES ARE A PRIME TARGET

Attackers can hijack legitimate Microsoft 365 accounts to send requests that appear authentic.

Tactics like AiTM phishing, session token theft, and Auth abuse can bypass traditional MFA defenses.

AI IS CHANGING THE PHISHING PLAYBOOK

AI makes deception harder to detect and easier to scale.

AI-generated messages can be convincing and highly personalized, lacking the typos and red flags employees once relied on.

THE SOLUTION

STOP BEC BEFORE IT BECOMES FRAUD

01

VALIDATE AND STRENGTHEN EXISTING CONTROLS

Security controls only work when properly configured. Evaluate Microsoft Entra ID and M365 to identify gaps and reduce risk.

02

MAKE IDENTITIES HARDER TO COMPROMISE

Apply phishing-resistant authentication, Conditional Access, and identity protections to reduce the risk of account takeover.

03

DETECT AND RESPOND TO COMPROMISE EARLY

Monitor for signs of account takeover, like suspicious sign-ins and unusual inbox activity, and respond before attackers can act.

THE PROOF

TURN MICROSOFT SECURITY INTO STRONGER BEC DEFENSES WITH AVERTIUM



AWARD-WINNING MICROSOFT SECURITY EXPERTISE

Named a Microsoft 2026 Security Trailblazer, Avertium brings deep Microsoft platform expertise to help organizations strengthen identity, access, and Zero Trust protections across Microsoft environments.

PROGRAMMATIC APPROACH TO SECURITY AND COMPLIANCE

Avertium's Assess, Design, Protect approach helps organizations move from identifying risks to designing and implementing protections that reduce exposure to modern BEC attacks.



REAL-WORLD DETECTION AND RESPONSE

Avertium identifies BEC activity across customer environments and contains complex email-driven breaches, helping customers avoid compromise and resume operations without major damage in the event one occurs.

DEFEND AGAINST BUSINESS EMAIL COMPROMISE ATTACKS WITH IDENTITY-FOCUSED PROTECTIONS

LEARN MORE

CONTACT US TO GET STARTED

AVERTIUM®
A CyberMaxx COMPANY

[1] 2026 AFP Payments Fraud and Control Survey Report | AFP
[2] Digital Defense Report 2025 | Microsoft
[3] Internet Crime Report 2025 | FBI

Copyright © 2026 Avertium, LLC. All rights reserved.