From Training to Technology: Building a Comprehensive Defense-in-depth Strategy Against BEC

Presented by

IRONSCALES SAFER TOGETHER | OSTERMAN RESEARCH

Business Email Compromise (BEC) attacks are becoming more frequent, more expensive, and more difficult to detect with traditional email security solutions. This infographic uses data from Osterman Research[1] to **highlight the measures businesses are taking to address the BEC threat** and how effective some of these strategies are.

CULTIVATING SECURITY AWARENESS

More than two out of three respondents say that multiple educational approaches are highly important for educating the employees to detect BEC attacks–ranking the following approaches as "important" or "extremely important."

74% Phishing Simulation Testing

71% Security Awareness Training Videos

69% Email Banners for emails from outside the organization

67% Email Banners that contain specific warnings

DEFENSE IN DEPTH

Gartner® recommends in the 2023 Gartner Market Guide for Email Security[2] that organizations should **"look for email security solutions that use ML- and AI-based anti-phishing technology for BEC protection to analyze conversation history to detect anomalies."** They also recommend that companies **"invest in user education with a particular focus on BEC-type attacks with no payload, and implement standard operating procedures for the handling of financial and sensitive data transactions commonlytargeted by impersonation attacks."**

While most respondents agree that using a defense-in-depth approach that combines technology and employee education, most organizations are leveraging a combination of tools with known limitations against BEC attacks

Additionally, despite the importance of using Phishing Simulation Testing and Security Awareness training, few are using both.

59% Phishing Simulation Testing

55% AI-powered anti-phishing tools

32% Dark Web Monitoring

80% **of organizations use this combination with limited success**

82% Secure Email Gateway

82% Mutli-factor Authentication

83% Security Awareness Training

IRONSCALES research shows that Secure Email Gateways miss **50% of phishing threats**[3]

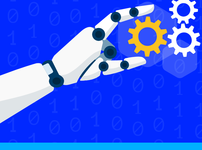
IRONSCALES COMBINES AI POWERED PROTECTION WITH HUMAN INSIGHTS

IRONSCALES is the only email security solution that integrates AI and human insights to effectively combat advanced phishing attacks like BEC, ATO, and VIP impersonation. **Our solution is powerful, simple, and adaptable, making it easy to implement, integrate into your tech stack and manage without requiring security expertise.** Protect your company with the only solution that truly addresses the entirety of the phishing problem.

With IRONSCALES, over **10,000 customers** are protecting their organization from advanced phishing threats by:

Artificial Intelligence

- Analyzing communications to create a social graph for each user to understand writing style and who they communicate with
- Reducing the effort to detect and remediate phishing threats using AI-powered phishing protection that automatically detects and quarantines polymorphic attacks across the entire organization
- Automatically grouping and remediating similar threats across your entire organization to address polymorphic attacks



Human Insights

- Ensuring that employees are a strong line of defense with access to more than 100 different security awareness training videos
- Regularly testing employee's security awareness by quickly launching prebuilt recommended phishing simulation testing campaigns based on seasonal trends, current threats, and more
- Reinforcing awareness by alerting employees of potential threats with dynamic, straightforward email banners
- Empowering employees to participate in the fight against phishing with the ability to report suspicious messages using Report Phishing Button quickly
- Viewing how security peers have classified a suspicious email in using IRONSCALES to help make informed decisions

For more information download Osterman Research report **"Defending the Enterprise: The Latest Trends and Tactics in BEC Attacks"**

DOWNLOAD HERE

IRONSCALES is a leading email security company focused on fighting back against today's modern phishing attacks. Our self-learning, AI-driven platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO) and more. We believe our powerfully simple email security solution is fast to deploy, easy to manage and keeps our customers safe. Founded in Tel Aviv, Israel in 2014 by alumni of the Israel Defense Force's elite Intelligence Technology unit, IRONSCALES is headquartered in Atlanta, Georgia. We are proud to support thousands of customers globally with our award-winning, analyst-recognized platform.
Visit https://www.ironscales.com and connect with us on LinkedIn to learn more.

IRONSCALES SAFER TOGETHER

[1] Osterman Research, Defending the Enterprise: The Latest Trends and Tactics in BEC Attacks at https://secure.ironscales.com/defending-the-enterprise/report-download

[2] Gartner, Market Guide for Email Security, Ravisha Chugh, Peter Firstbrook, Franz Hinner, 13 February 2023, at https://secure.ironscales.com/gartner-market-guide-email-security

[3] IRONSCALES, New Research: Nearly Half of Phishing Emulations Bypass Microsoft ATP and Top SEGs, at https://ironscales.com/blog/emulations-bypass-segs-research/