SOLUTION BRIEF

Comprehensive Phishing and BEC Protection

Integrated Multi-Layered Solution to Address Phishing and Business Email Compromise Attacks

The Problem

Email is how business gets done, whether exchanging sensitive information or facilitating major transactions. Enabling seamless collaboration across organizations, it has become a prime target for cybercriminals seeking to exploit interactions through phishing and Business Email Compromise (BEC) attacks.

Phishing, which includes BEC, poses a significant and evolving threat. Cybercriminals use increasingly convincing tactics to trick recipients into revealing sensitive information, clicking malicious links, or downloading harmful attachments. These attacks range from mass-distributed generic lures to highly targeted spear-phishing attempts that mimic trusted contacts or organizations.

This dynamic nature of phishing and BEC attacks has driven the adoption of AI-powered email security solutions. These technologies aim to detect subtle anomalies and patterns that human analysts might miss. However, implementing these AI systems comes with challenges. The sheer volume of data that must be analyzed to prevent phishing and BEC attacks can be overwhelming. This often results in a high number of false positives, requiring time-consuming manual review and continuous fine-tuning to maintain effectiveness while ensuring legitimate emails and links aren't blocked.

Key Benefits

- **Get the best protection**
  Harness AI-powered detection to block phishing and business email compromise.
- **Strengthen defenses with integrated protection**
  One platform to protect collaboration – regardless of the attack.
- **Gain visibility into threats targeting your users**
  Empower admins to make informed decisions with actionable insights.

The Solution

Effective prevention of phishing and BEC attacks demands more than a single-solution approach due to the limited view of the threat. In this context, relying solely on artificial intelligence is insufficient, as AI alone may not catch all the nuanced tactics employed by cybercriminals. While AI is a powerful tool in detecting anomalies and patterns, it works best when complemented by other security measures.

Implementing robust email authentication standards helps verify the legitimacy of email senders and prevents email spoofing—a common tactic in phishing attacks. These protocols work together ensuring incoming emails are from the claimed sources, significantly reducing the risk of impersonation attempts. Threat intelligence feeds play a vital role in this integrated approach. These feeds provide real-time information about emerging threats, known malicious actors, and current attack patterns.

AI detection capabilities, while not sufficient on their own, are a crucial element of anti-phishing and BEC strategies. Machine learning algorithms analyze vast amounts of email content, embedded links, sender behavior, and communication patterns to detect subtle signs of social engineering or fraudulent activity.

By utilizing a combination of threat intelligence, authentication protocols, and AI-driven detection, creates a comprehensive defense strategy against phishing and BEC attacks. This layered approach addresses various aspects of the threat, from preventing malicious emails from reaching inboxes, detecting sophisticated social engineering attempts and blocking access to malicious links.

$2.9 BILLION
In losses due to BEC in 2023.[1]

60 SECONDS
Users fall for phishing attacks in under 60 seconds.[2]

#2
BEC sams were the second most profitable cybercrime in 2023.[3]

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[2] https://www.verizon.com/business/resources/reports/dbir/

[3] https://www.interpol.int/es/content/download/20960/file/INTERPOL%20Global%20Cybercrime%20Conference%202023%20-%20Outcome%20Report.pdf

Strengthen Defenses with Integrated Protection

Mimecast delivers comprehensive protection against both the preparation and execution phases of BEC attacks. With the help of Mimecast's connected human risk management platform, we can identify and take down resources created for phishing and BEC email delivery, safeguard against phishing links and attachments, and thwart payloadless attacks.

Our comprehensive approach to Business Email Compromise (BEC) and phishing attacks employs a sophisticated, multi-layered strategy that combines various signals and technologies. We begin with pre-filtering threats using authentication protocols, extensive reputation checks, threat intelligence feeds, and proprietary threat signatures. Our inspection capabilities are further enhanced through natural language processing (NLP) and other artificial intelligence and machine learning capabilities. By integrating complementary detection mechanisms, we can confidently identify anomalies and suspicious activity and block it at the point of detection.

Intelligent BEC Prevention

Mimecast's Advanced BEC Protection solution examines relationship and reputational features derived from social graphs to identify anomalous patterns that may indicate an attack. Emails flagged as suspicious undergo analysis through an NLP text extraction model, which identifies phrases commonly associated with BEC attacks. The relationship and reputational features alongside risky phrases are fed into a threat model. Emails are subsequently blocked based on configurable policies. For emails that don't meet the threshold set within the policy, social graphing provides context to display dynamic, interactive warning banners to users.

Total Phishing Protection

Phishing protection employs a two-stage approach: pre-click and post-click analysis. Pre-click analysis involves reputational checks, categorization, pattern matching, and QR code identification and inspection. Post-click analysis is more thorough, beginning with resolving the final page including redirections. Our multi-stage detection continuously inspects suspicious links extracted from the resolved page. During the inspection process various techniques will be applied which include URL machine learning, credential theft protection, HTML analysis, phish kit identification, and AI phishing page detection - for high-risk file sharing sites, we simulate user interaction.

Integrated and Coordinated

We've tightly integrated our attachment and URL scanning capabilities, enabling thorough examination of attachments identified during phishing identification. Direct downloads from links are subjected to static file analysis and sandbox testing, with dangerous file types being blocked outright. The results from all these analyses are combined using a weighted average, continuously adjusted using machine learning model.

Mimecast's approach goes beyond utilizing AI as a last line of defense. Our AI detection capabilities are continuously strengthened by analyzing billions of signals across the platform. Allowing our machine learning models to adapt and evolve with shifting tactics, ensuring highly effective detection. By consolidating multiple security capabilities into an integrated solution, organizations can streamline defenses, improve visibility, and enhance their overall resilience against the ever-changing landscape of email-borne cyber threats.

Case Study Reference

Use Case
Defend Against BEC Threats

Challenge: BEC threats utilize payloadless attacks with no malicious content, requiring users to determine if any emails are suspicious based solely on their content.

Solution: Advanced BEC Protection blocks emails with no malicious payload through:

- Email authentication protocols, threat feeds and customer signatures
- The generation a social graph of user interactions to identify anomalous activity
- Analysis of risky phrases and semantic intent to determine an email's purpose prior to delivery.

Benefit: Prevents financial losses and security breaches by detecting advanced BEC attacks, while safeguarding sensitive information, ensuring

Use Case
Fragmented Administration Experience

Challenge: Efficiency is hampered by the dispersion of management tasks across multiple interfaces and systems, which complicates oversight and coordination.

Solution: A centralized dashboard across the Human Risk platform provides visibility into the top targeted users, malicious senders, and sources of threats, with searches to determine their scale and severity. Detection summaries categorize threats by impact, type, and details, and include explanations, evidence, and actions affecting users. Data can be exported via API for seamless integration with other security tools.

Benefit: Empower administrators with actionable insights through real-time alerts, incident analysis, and trend visualization to enable informed decisions.

Use Case
Prevent Access to Phishing Links

Challenge: Phishing links are pervasive and require a multi-layered solution to safeguard users from falling victim to scams, data breaches, and other cyber threats.

Solution: Mimecast Advanced Email security is designed with phishing protection in mind, employing a multi-stage approach against a wide range of malicious links and websites before and after click:

- Pre-click analysis quickly checks for basic safety indicators and QR codes
- Post-click analysis performs a thorough examination. This includes following redirects, scanning all linked pages, and applying various detection methods like machine learning and custom rules. High-risk sites and downloads receive extra scrutiny.

Benefit: Safeguard critical data, prevent financial fraud, and protect business reputations from breaches and supply chain attacks. Enhance productivity by reducing security-related disruptions due to phishing.

> **"Email presents the largest risk for threats like phishing, and with more people working remotely than ever before, it's even more critical to protectour email communications. That's why we turned to Mimecast for help."**
>
> **Erik Hart, Chief Information Security Officer at Cushman & Wakefield[4]**

Read Case Study