DATASHEET

Mimecast Advanced BEC Protection

Block business email compromise with an AI-powered email security solution, providing integrated protection for your communications.

The Problem

Email is how business gets done, whether exchanging sensitive information or facilitating major transactions. With so much dependence on email, it becomes the perfect target for Business email compromise (BEC) that seeks to exploit these high-value moments. BEC lures are constantly evolving requiring tools that do not rely on signatures or heuristics, resulting in the use of AI based solutions. The challenge of making these technologies working together is the complexity and overwhelming amount of data to interpret, whilst constantly requiring tuning and human oversight due to the high number of false positives generated by AI only solutions.

The Solution

To prevent BEC attacks, security teams need to integrate multiple proven methods. A comprehensive BEC solution leverages threat feeds, email authentication protocols and advanced AI-driven detection capabilities.

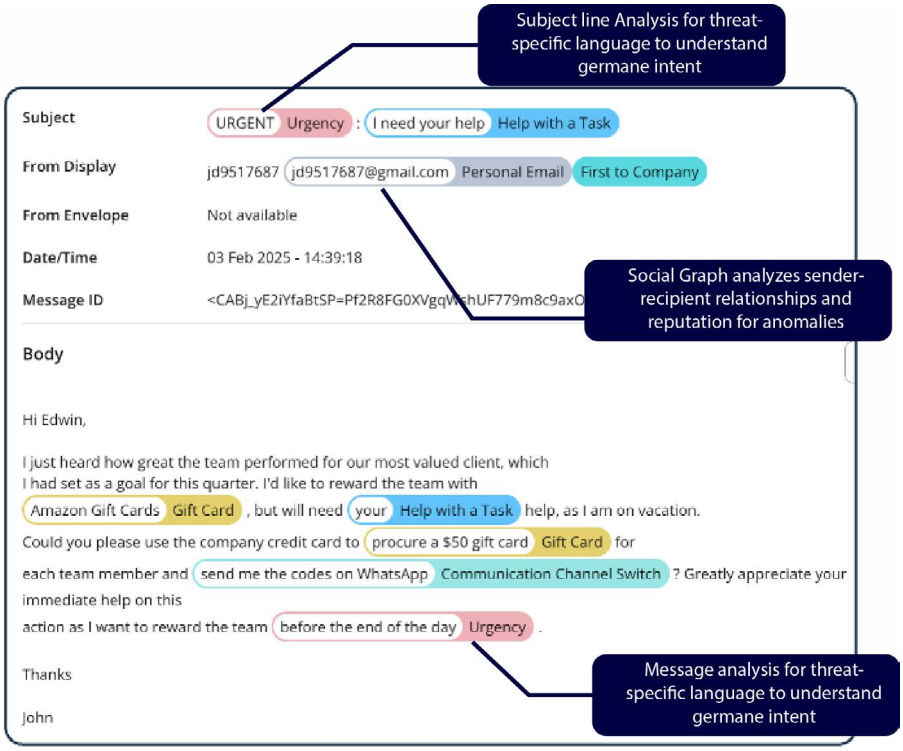
To confidently identify anomalies and suspicious emails, Mimecast's advanced email security includes authentication protocols, reputation checks, threat feeds, proprietary signatures and AI to stop attacks at the point of detection. But with Mimecast, AI is more than just a last line of defense. Billions of signals across our platform strengthen our AI detection to continuously identify and block advanced BEC attacks, adapting to evolving threats.

Our protection doesn't stop there. Mimecast's unified detection capabilities protect against any type of email-based attack – not just BEC.

$2.9 BILLION in losses due to BEC in 2023*

25% of financially motivated attacks utilize BEC**

* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
** https://www.verizon.com/business/resources/reports/dbir/



About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.