Data Sheet

mimecast

Social Engineering Defense

Detect targeted email attacks and limit attacker reconnaissance with Mimecast's AI-powered CyberGraph solution

Email threats are getting more targeted and sophisticated, with cybercriminals relying on tactics like social engineering and malware-less attacks to evade detection. With more and more information available about people and the organizations they support, the ability to craft highly-personalized phishing and impersonation emails grows, making employees more vulnerable than ever. And simple mistakes, such as clicking on a malicious link - can have devastating consequences.

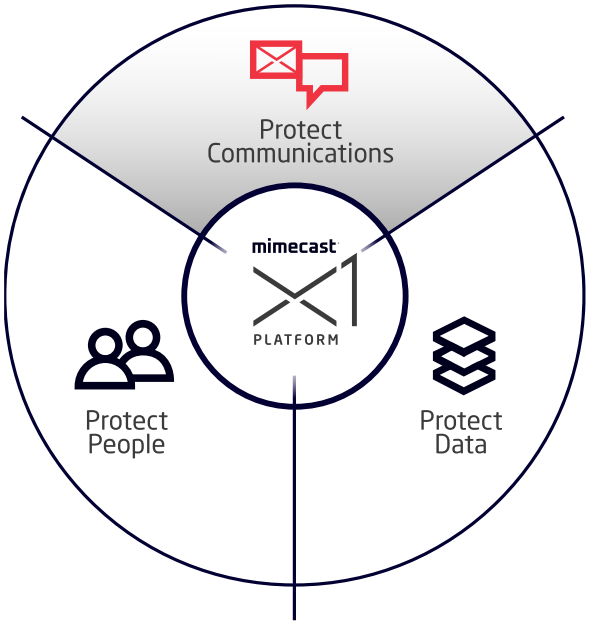
Make employees part of the solution

Mimecast's CyberGraph solution defends against highly targeted and evasive email-based attacks, using AI, Machine Learning, and Social Graphing to map communications patterns and get smarter over time. This solution surrounds employees with continuous protection by delivering four key capabilities.

Key Benefits

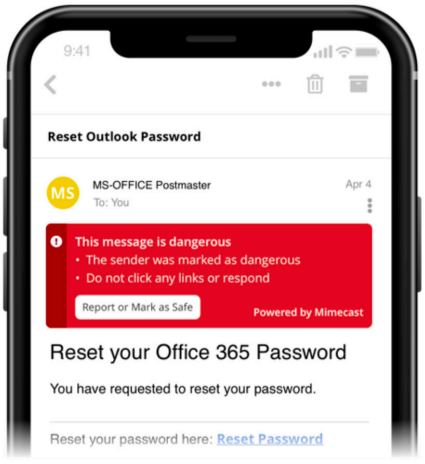
CyberGraph

- Limits intelligence gathering that can help a bad actor craft a highly targeted attack
- Detects sophisticated, highly targeted email threats with social graphing technology
- Strengthens protection without the burden of rule configuration
- Engages users at the point of risk with warning banners embedded only in suspicious emails
- Empowers users and strengthens the machine learning model through user reporting
- Automatically updates email warning banners for all employees across all devices when risk levels change
- Alerts employees to potentially misaddressed emails to help prevent data leaks
- Stops mistakes from developing into security incidents



Identification of targeted email threats

Through the power of Social Graphing and Machine Learning, CyberGraph maps your organization's communication patterns and builds an identity graph that includes the relationship strength and proximity of senders and recipients. The solution then identifies anomalies that could be indicative of a malicious email. The information gathered feeds a Machine Learning model that powers a real-time alert and reporting system, combining on-going Social Graphing, employee-sourced threat intelligence, and email analysis to get smarter over time.



Dynamic warning banners

CyberGraph empowers employees with color-coded, contextual, dynamic warning banners embedded in suspicious emails. Employees can report emails as safe or malicious. When risk levels change, banners for all similar emails are updated automatically for all employees across all devices. Importantly, banners are only applied to emails that warrant them. The result? Employees stay engaged and become part of the solution, rather than tuning out.

Employee tracker protection

A bad actor, during the reconnaissance phase of an attack, can embed trackers into emails that pull information from a remote server. This discloses the device IP address, location, the recipient's engagement levels with the email content and the device's operating system and browser versions. CyberGraph replaces trackers and "proxies" the content, shielding the recipient's location and engagement levels. This helps prevent the attacker from understanding whether they might, for example, be targeting the correct individual for a financial scam. It also limits their ability to gather essential information that can help them craft an extremely authentic spear phishing email, e.g., by mentioning the target's location.

Detects potentially misaddressed emails

Using Artificial Intelligence and Social Graphing, CyberGraph identifies and prevents possible instances of data loss caused by employees sending emails to the incorrect recipient. By alerting senders of potentially misaddressed emails immediately after they click send and prompting them to release or hold the email, this solution prevents simple mistakes from developing into security incidents. CyberGraph administrators maintain full visibility into emails identified as potentially misaddressed, including supplemental information and the reason why they were held.