Solution Brief

mimecast

Advanced Phishing Protection

Mimecast Advanced Phishing Protection combines Mimecast CyberGraph and Browser Isolation to engage and educate users about potential phishing threats and protect them should they click a link to a phishing site.

Why Phishing is the Highest Concern for Security Teams[i]

A study by Osterman Research found that the issue of highest concern for security teams was phishing attempts making their way to end users. In second place, 64% of respondents rated employees falling for the phish as "concerning" or "highly concerning", and a data breach caused by ransomware came in third place at 61%. These concerns are hardly surprising given that 84% of respondents had experienced a security incident in the past 12 months that was related to phishing or ransomware.

Why Phishing is the Attack of Choice for Bad Actors

Phishing is the Swiss army knife of attacks. It can use multiple attack vectors, is cheap and easy, can evade security controls and lead to many positive outcomes for the attacker. These include credential theft and account compromise, ransomware and malware infection leading to data theft, and direct financial loss from BEC attacks. Around half of the respondents to the Osterman survey had experienced at least one such incident.

Kits Have Democratized Phishing

The availability of phishing kits and phishing as a service has made it easy for any non-technical cyber criminal to launch a phishing attack. Advanced phishing kits can be purchased for as little as $80. Compounding the problem, they're being rolled out onto newly registered domains at a rate that makes it extremely difficult for security vendors to track them.

Phishing Evades Security Controls

Phishing emails use many tactics to evade detection by both email security products and the email recipient. Attackers impersonate domains, senders and websites. Social engineering tactics entice the recipient to perform an action, and when they do, the evasion continues – phishing sites use blocklists to prevent their analysis by security providers, encoding techniques to obfuscate words and logos, and public cloud hosting to add authenticity to the phishing site.

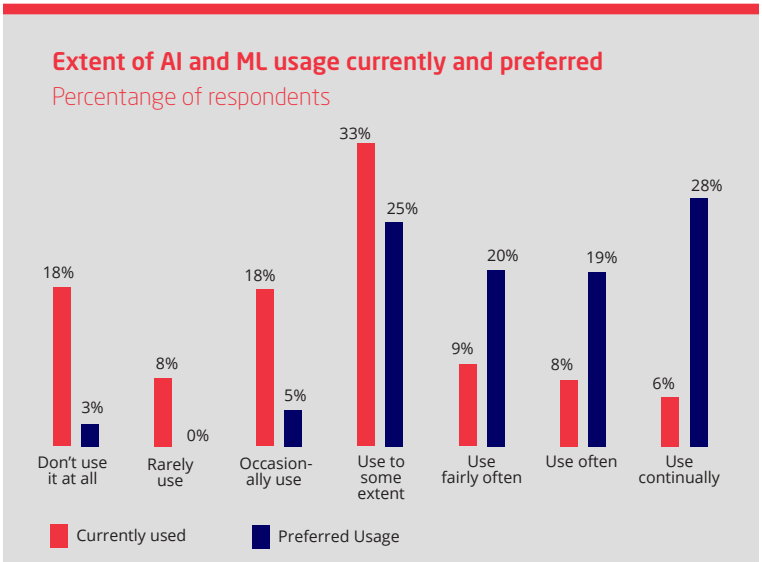
Users Require More Help

All security professionals recognize that users are the last line of defense and have deployed training programs to help their users recognize phishing attacks. Many also add warning banners to emails to reinforce this training and engage users. To some degree, this is working – Osterman found that, following training, 80% of users reported more suspicious emails to the IT team than before[ii].

However, only 45% of respondents to Osterman's survey suggested they were "Fairly Confident" or "Completely Confident" that their users could recognize email phishing attempts[i]. This is validated by the fact that, on average, 50% of user-reported emails were benign[ii]. This rate of benign emails incorrectly reported as suspicious did vary wildly and validates Mimecast's own experiences – the Mimecast SOC suggests that for some customers, it can be as high as 90%. This wide range across different organizations highlights the wide discrepancies in effectiveness of different training programs and other user engagement techniques. For example, 86% of companies add "External Email" warning banners to emails[ii]. These are clearly ineffective at engaging users, who are likely becoming "blind" to them due to the frequency at which they see them.

Security Teams Require More Help

The upshot of the increased number of emails reported by users, and the fact that many are benign, is that under resourced security teams are struggling to analyze and remediate them. In fact, 75% of companies do not analyze every reported email.[ii] Worryingly, 59% have technology to immediately remediate a reported email from all user inboxes.[i] This is worrying because, given the number of user reported emails that are false positives, it seems like a tactic that could have severe implications for a business.



Artificial Intelligence to the Rescue?

Many organizations see artificial intelligence (AI) as a solution, or at least a partial solution. Osterman found that there was a mismatch between current and preferred use of AI security technologies. Only 28% suggested they would like to use AI continually, implying that it is not seen as a silver bullet solution to all security challenges, but rather it has a part to play in the overall security program.[i]

i Osterman Research: How to Reduce the Risk of Phishing and Ransomware, May 2021

ii Osterman Research: Assessing Organizational Readiness To Deal With Increased Employee Cyber Awareness, May 2021

Mimecast Advanced Phishing Protection

Mimecast Advanced Phishing Protection combines two products in a cost-effective add-on solution for Mimecast Email Security customers. CyberGraph protects from highly evasive, suspicious emails by engaging the recipient and then, if the recipient does fall for a phish, Browser Isolation protects from credential theft and drive-by downloads. Both are integrated on the Mime|OS platform and configured and maintained using the Mimecast Administration Console.

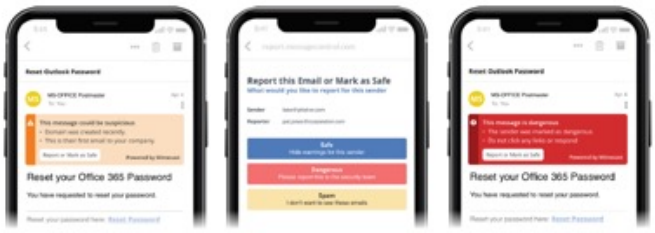
Mimecast CyberGraph

CyberGraph protects from sophisticated, highly targeted phishing attacks with three key capabilities.

Email tracker protection: Intended targets of a phishing attack are shielded from bad actors to limit reconnaissance and intelligence gathering. CyberGraph renders trackers embedded in emails useless to prevent inadvertent disclosure of critical information that could be used in a social engineering attack.

CyberGraph AI: CyberGraph detects highly targeted email threats using machine learning and identity graph technology to understand anomalies in sender and recipient behaviors that could be indicative of a malicious email.

Dynamic warning banners: CyberGraph empowers users with color-coded, contextual, dynamic warning banners embedded in suspicious emails. Users' opinions on whether emails are suspicious are solicited. Their input strengthens machine learning models and crowd sources threat intelligence, which is used to update banners in all similar emails across the organization.



CyberGraph Datasheet - Read More >

Mimecast Browser Isolation

Mimecast Browser Isolation for Email Security is a layer of protection that allows users to safely click on any URL. Web pages are opened in a remote, isolated web browser session in the Mimecast cloud and safely streamed to the user's browser. Mouse movements and keystrokes are transferred to the remote session, allowing the user to interact with the web site as usual.

Browser Isolation brings two key capabilities.

Credential phishing protection: Web pages can be rendered read only to block data input into web forms, protecting from phishing attempts for credentials and other sensitive information.

Malware containment: Files downloaded intentionally or by drive-by download are executed remotely, blocking attempts to infect the user's computer. This contains the threat, eliminates the patient-zero problem and ensures that ransomware cannot encrypt or steal information.

Browser Isolation Datasheet - Read More >

> **"Our email security added the same static warnings to all emails and our users became numb to them. The Mimecast banners convey engaging contextual information about the threat and are automatically updated as the artificial intelligence learns more about it."**
>
> IT Director, Chicago based PE firm