Cybersecurity Solutions
Mimecast CyberGraph

Introduction

Organisations and employees are targets for increasingly sophisticated email attacks designed to penetrate their defences. Sure has partnered with industry leading experts in cybersecurity, Mimecast, to use Artificial Intelligence (AI) techniques to mitigate the risks you face, as well as reducing the complexity of protecting your email.

CyberGraph

Mimecast CyberGraph combines three key technologies to protect you from targeted email threats:

- Email tracker protection
- Identity graph machine learning
- Dynamic contextual banners embedded in emails

Benefits

During the reconnaissance phase of an attack, Cybercriminals can embed trackers into emails that pull information from a remote server.

This discloses the device IP address, location, the recipient's engagement level with the content and the device's operating system and browser type.

CyberGraph replaces trackers and "proxies" the content, shielding the recipient's location and engagement levels. This helps prevent the attacker 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.

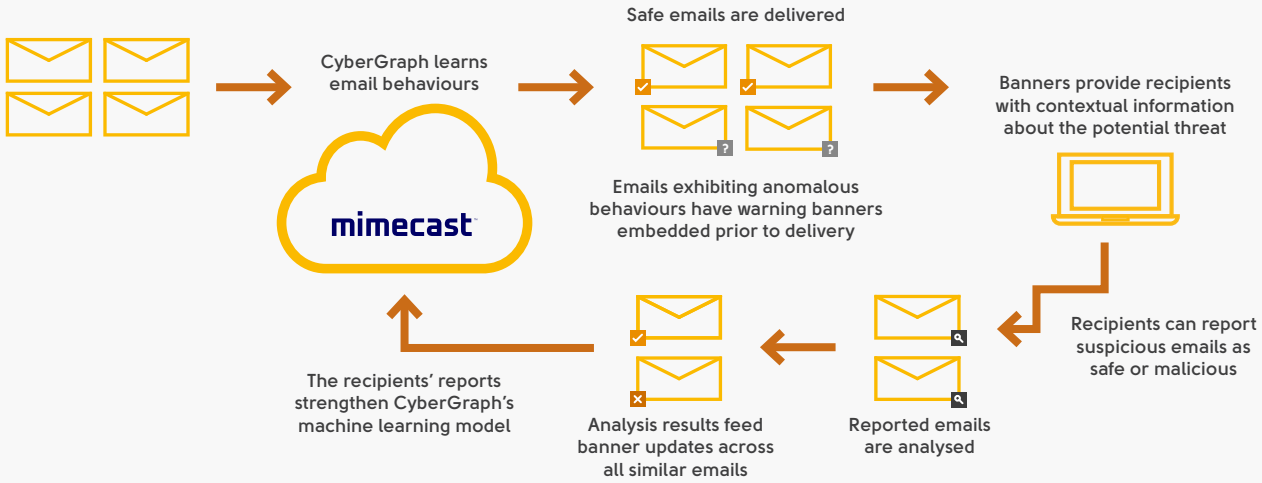
Key Benefits

- Limits intelligence gathering that can help cybercriminals craft a highly targeted attack
- Helps prevent disclosure of potentially exploitable software vulnerabilities
- Identity graph technology detects sophisticated, highly targeted email threats
- Machine learning 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 by soliciting their view of whether an email is malicious or safe

Artificial intelligence detects targeted email threats

Artificial intelligence learns behaviours to create an identity graph. This stores information about relationships and connections between all senders and recipients, including the strength or proximity of the relationships. It learns what is "normal" and detects anomalous behaviours that can be combined with other indicators to determine the risk associated with an email.

How it works



Warning banners alert recipients to risk

Coloured banners that indicate the level of risk are added to suspicious emails prior to delivery. They provide the recipient with enough information about the nature of the threat to inform them at the point of risk, when they are about to action the email. The banners and wording for each indicator can be tailored to meet the needs and knowledge levels of your organisation's users.

Banners are displayed, regardless of the device type or email client, and they do not interfere with the display format of the email preview or subject lines.

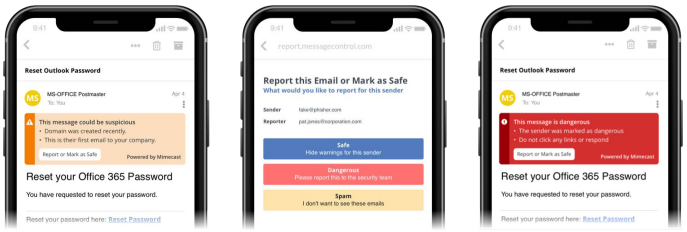
Recipients are empowered to strengthen protection

Recipients can report emails as malicious or safe. This reinforces the machine learning model and updates CyberGraph with information about trust relationships between senders and recipients. The information can also be crowdsourced to feed Mimecast's threat intelligence and benefit all customers.

Dynamic banners rapidly inform users of new threats

Links to the banners are embedded in emails as they are inspected and classified suspicious. This enables banners to be updated with new information about the risk indicators, including changing its colour, at any time. e.g. An email with a blue information banner is reported as malicious and this is verified when analysed.

The banner can be automatically changed to red, and next time any recipient of a similar email opens it, they are presented with a red banner. This is a highly effective way to maintain user engagement, rather than static banners that users become "blind" to.



Advisory & Design

At Sure we have a team of specialist consultants with extensive expertise in cybersecurity solutions. We can help you audit your infrastructure and processes, identify risks and vulnerabilities and implement robust security systems and policies.