Menlo Security
IT'S SAFE TO CLICK

PHISHING ISOLATION FOR FINANCIAL SERVICES INSTITUTIONS

The Problem

Financial services and insurance institutions (FSIs) are the top targets of phishing attacks

Despite deploying an array of email security products including anti-spam, anti-virus, data security, and encryption, FSIs and their employees—and even customers—continue to be severely impacted by phishing. Phishing attacks on FSIs range from pinpoint, surgical spear phishing attacks targeting specific executives with personally-crafted emails, to broader-focused phishing attacks directed at certain, more vulnerable departments, all using social engineering. These often result in the theft of critical user credentials, malware that steals sensitive data, and ransomware attacks.

Legacy email security products deployed by FSIs rely on a 'good vs. bad' determination provided by third-party data feeds or internally via large-scale email traffic and data analysis. Because spear phishing attacks target specific individuals within a financial services organization, the email link is usually unique, as is the target user. Therefore, no third-party reputation data is available, nor is there enough data for internal analysis to make an accurate 'good vs. bad' determination. And, if the determination is incorrect, the first targeted 'patient-zero' individuals are sent directly to a website where their credentials can be stolen, malware can be downloaded, or a ransomware attack launched. A single 'false negative'—as well as a single employee or contractor clicking on a link embedded in an email—can initiate a string of costly and damaging cyber attacks on an FSI, culminating in productivity, revenue, and reputation loss.

Attackers are much cleverer when launching attacks on FSIs. There are an increasing number of attacks where a targeted spear phishing or broader phishing attack has been a smoke-screen for a more dangerous, nefarious cyber attack. In these situations, avoiding or quickly alleviating the camouflaged phishing attack can aid in discovering and stopping the deeper, more insidious cyber attack.

About Menlo Security

Menlo Security is making it safe to click via isolation, protecting organizations from cyber attack by eliminating the threat of malware from web and email. Menlo Security's Isolation Platform (MSIP) isolates all active content in the cloud, enabling users to safely interact with websites, links and documents online without compromising security.

Menlo Security is trusted by some of the world's largest enterprises, including Fortune 500 companies and financial services institutions. The company was founded by security industry veterans, in collaboration with acclaimed researchers from the University of California, Berkeley, and backed by General Catalyst, Sutter Hill Ventures and Osage University Partners,

For more information,
visit menlosecurity.com

Menlo Security
IT'S SAFE TO CLICK

2300 Geng Rd, Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1795
info@menlosecurity.com

The Solution: Menlo Security Phishing Isolation

Phishing security based on isolation technology avoids the difficulties in distinguishing between legitimate and malicious emails and content. Isolation inserts a secure, trusted execution environment, or isolation platform, between the FSI's users and potential sources of attack. By executing user sessions away from the endpoint and delivering only safe rendering information to endpoint devices, users are protected and their endpoints insulated from malware and malicious activity.

Menlo Security's Phishing Isolation solution eliminates the credential theft, drive-by malware exploits, and ransomware instigated by email attacks. By integrating Phishing Isolation with an FSI's existing mail server infrastructure—such as Microsoft Exchange, Gmail, or Office 365—all email links can be directed to pass through the Menlo Security Isolation Platform. Deployment is streamlined, requiring no changes to existing email platforms and, more importantly, to the user's experience. When users click on an email link, they are 100% isolated from all malware threats, including ransomware. As cyber attackers are becoming more sophisticated and devious in their phishing methods, it also ensures that zero-day and emerging phishing techniques are stopped. Websites opened from links within emails may also be rendered in read-only mode, preventing users from entering critical credentials or sensitive information into malicious web forms.

With users safely isolated, administrators can monitor behavior statistics and customize time-of-click messages to help reinforce anti-phishing awareness training in real time. Administrators can also define workflow policies for groups or individuals to determine if or when read-only may be relaxed. With zero dependency on error-prone threat detection methods, such as data analytics, Menlo Security Phishing Isolation is the only email security solution that protects every FSI user's email the instant it's deployed.