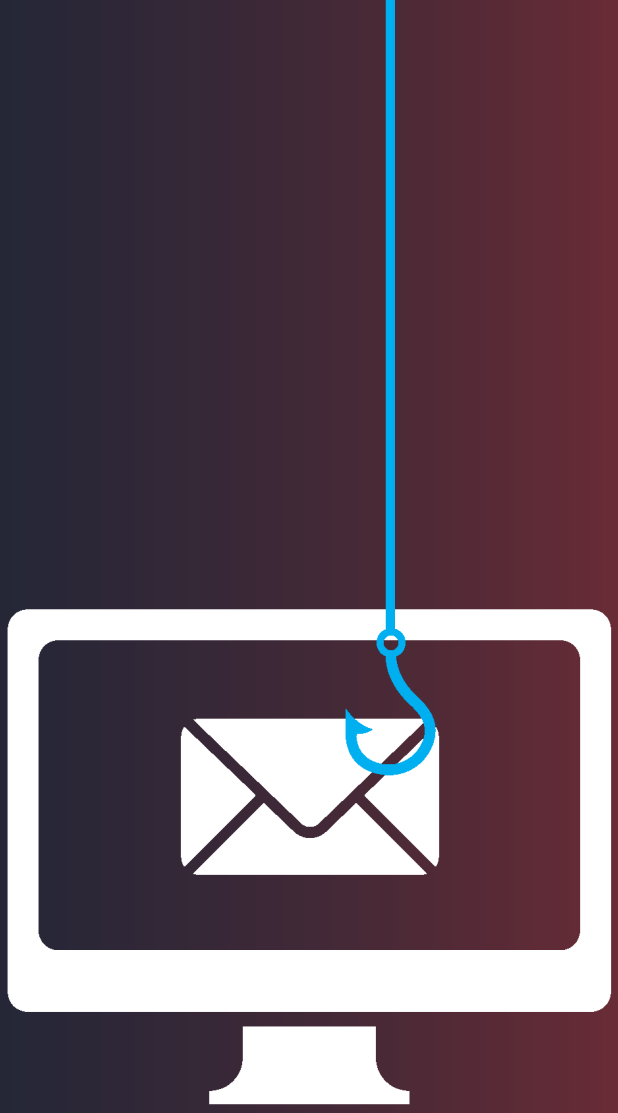

An End-to-End Strategy for Taking Phishing Off-Line

MARKET TRENDS REPORT

govloop COFENSE carahsoft

Introduction

Tactics may change, targets may change, but phishing never sleeps. Despite the best efforts of anti-phishing software and other security measures, it continues to grow as attackers' preferred tool for infiltrating networks and compromising data. Phishing is credited as the initial attack vector for more than 90% of federal government breaches that result in successful data exfiltration. Most recently, phishing has taken advantage of the pandemic, luring victims with COVID-19 themes, as public- and private-sector operations accelerated their digital transitions and became a bigger target for cybercriminals and nation-state actors.

Whether broad phishing campaigns or targeted spear-phishing emails, the threat shows no signs of abating. And with attackers nimbly shifting tactics faster than security solutions — and procurement processes — can adapt, agencies desperate to protect their data can't rely solely on security software and routine user awareness programs. They must adopt a comprehensive approach that combines the latest technology, including real-time detection and automated response, with crowdsourced human intelligence, turning phishing simulations into an effective tool for detecting and mitigating the real deal.

To learn more about how agencies can implement a comprehensive anti-phishing strategy, GovLoop teamed with Cofense, which provides an end-to-end phishing defense solution that combines human detection with cutting-edge, automated technical response. This report explains the need for an in-depth strategy and what agencies can do to keep pace with the threat. It also outlines how phishing simulations can make users essential to defending against tactics that consistently have been able to get around software defenses and secure email gateways.

By the Numbers

32%

of confirmed data breaches in 2019 involved phishing.

96%

of phishing attacks arrive via email.

88%

of organizations experienced spear-phishing attempts in 2019.

Source: Verizon's 2020 Data Breach Investigations Report

65%

of groups carried out targeted cyberattacks using spear-phishing emails.

96%

of targeted attacks were focused primarily on intelligence gathering.

Source: Symantec 2019 Internet Security Threat Report

$3.92 million

was the average cost of a data breach in 2018.

Source: IBM's 2020 Cost of a Data Breach Report

90%

of phishing attacks delivering malware are found in environments with secure email gateways.

75%

of verified phishing emails target credential theft.

Source: Cofense

"If you saw an email from [Federal Trade Commission] Chairman Joseph Simons, it wasn't. From him, that is. Scammers pretending to be him are emailing, though. They're trying to trick you into turning over personal information."

Source: An October 2020 FTC blog post

THE CHALLENGE
An Evolving Threat

Phishing tactics have steadily evolved, either in response to new defensive measures from security companies, increased awareness among users or a change in attackers' priorities.

For example, 10 years ago, a common tactic was to send a phishing email with a malicious attachment that, if opened, would install malware on a victim's computer, said Aaron Higbee, Cofounder of and Chief Technology Officer at Cofense.

"What's changed significantly over the last few years is the tactic has shifted more to credential theft," Higbee said. There are various ways of trying to trick a user into disclosing a username and password. As a result, credential theft has become phishing's No. 1 objective, he said, a conclusion supported by Symantec's 2019 Internet Security Threat Report.

But although cyber attackers will adapt and evolve in response to new defenses, they won't change if they don't have to. Attackers using machine learning and artificial intelligence (AI), for instance, can turbocharge highly targeted spear-phishing attacks, culling information from social media and other sources to use in a phishing attack. Security researchers have demonstrated that advanced algorithms are effective at profiling targeted users, and that users are more likely to click on a link in those personalized emails. So, AI-generated phishing attacks would seem likely to be widely used.

"In practice, we're not seeing the adoption of those techniques at all," Higbee said. Email gateway security has been stagnant, with no third-party labs or research agencies currently testing it even though that typically leads to improvements. This "complete drought of innovation" has allowed attackers to rely on current tactics, without having to use new techniques. "We're not seeing attackers using advanced algorithms or machine learning in order to boost their efficacy because they're doing fine right now," he said.

Regardless of tactics and techniques, the one constant in phishing's evolution has been the users, who have been widely saddled with the designation of being the weakest link in any security chain. No matter how many layers of security an organization has in place, a user who is duped into sharing a password or other sensitive information puts the organization's data at risk. A comprehensive anti-phishing solution needs to start with them.

THE SOLUTION: THE STRENGTH OF THE 'WEAKEST LINK'

Interactive simulation programs that engage users with the look and feel of actual phishing emails condition them to be an active part of phishing defense.

Government agencies have been slow to use simulations, often using them somewhat passively, as only a facet of user education. Many agencies ran simulations on their internal network, which couldn't match the realism of simulations coming almost directly from the internet. And users weren't an active part of the defense.

But users who are conditioned by doing up-to-date simulations to spot a suspicious email and report it quickly can give agencies a jump on stopping attacks. For example, they can quickly collect and analyze data on potentially harmful emails and initiate an effective response.

Private organizations have seen the results of that approach. Users trained with phishing simulations that accurately reflect the current state of actual phishes — and who have a visible "report phishing" button on their email screens — can become adept at recognizing and reporting suspicious emails. Combined with threat intelligence, real-time analysis and incident response, simulations can form an essential component of comprehensive phishing defense.

BEST PRACTICES
5 Factors Needed to Beat Phishing

A comprehensive phishing defense will combine human and automated elements, allowing an organization to rapidly detect, analyze, prioritize and respond to phishing emails. Here are some essential features of an effective solution.

User Training and Awareness

Users have an active role in defending against phishing emails. Training that includes realistic simulations and a system that allows them to easily report suspicious emails — sending those emails to the right place within the organization with the entire message intact — turn users into an initial line of defense. Training should be interactive, using a system that provides user feedback on emails they've reported and prioritizes reports from users proven to be adept at spotting phishing emails.

Fast Detection and Remediation

Security operations centers (SOCs) already handle alerts from the tools that defend networks, so adding user alerts can be overwhelming. Phishing attacks' success depends on the speed with which attackers can innovate and execute their campaigns. Agencies need phishing defenses that operate at the same speed. A system that quickly analyzes suspected phishing emails, eliminates false positives and groups emails based on payloads brings the most critical threats to the forefront and hastens response.

Security Controls and FedRAMP Authorization

The Federal Risk and Authorization Management Program (FedRAMP) establishes the security standards for agency use of cloud services, with Impact Levels of Low, Moderate and High. At the far ends, Low (with 125 controls) covers publicly available data and High (421 controls) covers highly sensitive data, such as that found in law enforcement and health care. Most agencies should look for a service authorized at the Moderate (325 controls) level, which covers protecting controlled and unclassified information, such as personally identifiable information.

Threat Intelligence

Even highly targeted phishing emails don't exist in a vacuum; a system with a global network of data on current threats and phishing campaigns helps cut through the noise. In addition to the troves of data supplied from around the world, crowdsourced human intelligence adds to the analysis and threat intel necessary to define and remediate attacks.

Automated Response

Speed is essential in stopping attacks before they can do damage, so a solution with a powerful, configurable rules engine and automated defensive steps is essential to a SOC's response.

CASE STUDY
Simulations Help Users Learn the Ropes

Phishing simulation programs have an established pattern of improving an organization's security.

Employees who participate in accurate phishing simulations learn quickly to identify the look and feel of a phishing email. Higbee said that when PhishMe was introduced a decade ago, it was common to see high failure rates — users clicking on phish during simulations — in organizations that had never done simulations. "Over half of the population would fall for the first phish," he said. But in subsequently simulated phishes, users immediately showed progress. Before long, organizations reached the point where more users reported a suspicious email than fell for it in a simulation.

Once they get the feel for it, users can also add a layer of defense that might be beyond a software solution's reach.

For example, security software can scan a URL in the body of an email to determine if it's malicious. But if an attacker then puts the URL into a PDF document and lures the user into opening it, the attack can get by a secure email gateway — at least until a patch or update for the software is developed, distributed and applied. However, a user who's gotten into the habit of spotting tactics such as phony URLs could report it quickly.

"People are providing cover until the technology catches up," Higbee said. Even with AI, attackers can't model human behavior with 100% certainty. Users can provide an element of instinctual defense that is beyond the capacity of machines. "We need humans in that sort of gray area."

HOW COFENSE CAN HELP

Cofense pioneered phishing simulations, introducing PhishMe more than 10 years ago. The company has since worked with public and private organizations on implementing a comprehensive approach to simulations.

Its simulations draw from current phishing emails actively in use and are updated weekly to reflect current trends. PhishMe's Reporter button has proved to be a critical tool in engaging users, making it easy to report suspicious emails quickly, keeping those emails intact and directing them to the right location. Cofense's Triage workflow tool, which can run on premises or in the cloud, allows operators to organize emails, incorporate user reports, write filter patterns to detect particular tactics and share phish information with the entire ecosystem of Triage customers.

Cofense PhishMe has received Agency Authority to Operate (ATO) from the Department of Health and Human Services and is in the final stages of achieving FedRAMP ATO-Moderate authorization.

Cofense also provides security teams with the tools for rapid enterprisewide searching and quarantining once suspicious emails have been reported through the Cofense Vision product.

For more information, please visit www.cofense.com

Conclusion

Phishing has been a favored tool of cyber attackers for the past couple of decades, whether to distribute malware, compromise credentials or initiate other exploits. It's the foot in the door for attackers bent on stealing sensitive information, compromising systems, exfiltrating data and exploiting compromises for financial gain. And because it works, it's likely to remain a major threat.

An effective defense against phishing needs to involve users who can add a layer of defense that complements other security tools in place. A solution that combines user reports with wide-ranging threat intelligence, effective analysis and automated responses is essential to preventing the kind of exploits and data breaches that expose vital data, ranging from the personal information of employees and constituents to sensitive communications and transactions. It can give agencies the best chance for a defense that functions at the speed of attackers.

ABOUT COFENSE

Cofense®, the leading provider of intelligent phishing defense solutions worldwide, is uniting humanity against phishing. The Cofense suite of products combines timely attack intelligence on phishing threats that have evaded perimeter controls and were reported by employees, with best-in-class security operations technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global organizations that understand how changing user behavior will improve security, incident response and reduce the risk of compromise.

Visit www.cofense.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop