Submerge Customer Session Titles

Using Cofense PhishMe™, Cofense Reporter™, and Cofense Triage™ to Build the Best Enterprise Defense Program in the Industry

The recipient of the 2018 Enterprise Defense Program of the Year shares their insights, lessons learned and best practices to achieve industry-leading reporting, susceptibility, and resiliency rates, along with steps taken to make the program even better in 2019. These steps include: introducing a global rewards program with points employees can redeem for prizes; improving the Top Phish employee competition and various awards categories to push reporting rates from 50 percent to over 60 percent this year; using data analytics and UX best practices; creating KPIs to quantify risk and performance; and much more.

Phishing and Incident Response: A Methodology

It's not a matter of whether or not your company will be compromised, it's a matter of when it will happen. Therefore, every cybersecurity team will need to be able to respond to incidents. How do you prepare for such incidents? How do you contain and neutralize them? What lessons can be learned after the fact? This talk will explore the six steps of incident response, how to apply them to the threat of employees clicking on phishing emails, and how Cofense tools can be leveraged during an incident.

1. **Preparation:** (Cofense PhishMe simulations and Cofense Reporter)
2. **Identification:** How do phishing analysts identify a reported email as malicious? If it is malicious, what questions do we need answered? (Cofense Triage)
3. **Containment:** Will depend upon type of phish, and how to stop the bleeding. (Cofense Vision)
4. **Eradication:** Cleaning up the mess (Cofense Vision)
5. **Recovery:** System validation, restore, and monitor
6. **Lessons Learned:** Document and follow-up report

How to Identify Repeat Clickers, Address Risky Behaviors and Reduce False Positives

How well do you know your phishing data? Many organizations want to identify and address risks from users who repeatedly click on phishing links. Discover how a leading bank tackles this problem, assesses risks tied to these employees, and identifies potential false positive clicks when an end user didn't legitimately fail an exercise. While false positive events can be few and far between, a phishing link can be tripped by automated applications, an occasional careless incident response employee, and other issues. See how to best communicate with repeat clickers, their managers, and business lines.

Using Cofense Solutions to Identify High Risk and High Value Target Employees

Find out how a Cofense customer uses data from Cofense PhishMe, Cofense Reporter, and Cofense Triage to identify two types of employees: high-risk employees (aka repeat offenders) who work in critical areas like HR and finance and high-value employees who are targets of spear-phishing campaigns. Learn how this organization uses this data to provide additional training as well as harden defenses to protect employees and networks.

Digging Through the Trash: Value and Importance of User-Submitted Phishes

For this organization, deploying Cofense Reporter gave them an important piece of the puzzle. Learn how they remove and gather intel from the phishing emails users report; these are messages that get through Symantec, firewalls, and mail filtering controls. See real-world examples of how Cofense solutions have helped reduced risk and minimize attack success that can apply to your organization. Get best practices for leveraging threat intelligence and gathering, sharing, and using intelligence to stay a step ahead of attackers.

Intelligence-Led Anti-Phishing

Phishing is one of the greatest threats facing organizations and customers. It has become one of the most preferred and effective vectors of compromise in cyber criminals' arsenal. This session will cover how intelligence feeds an anti-phishing program. Discover some of the tools, technologies, teams and processes designed to identify and prevent phishing from affecting either our organizations or customers.

Posse vs Cattle Rustlers: Deputizing Users with Cofense Reporter

Every time users click the Cofense Reporter button, they are temporarily deputized. Welcome to the Security Team! Your phishing program can't be punitive if you want employees to be on your side. Give them useful tips they can use at home. Stop talking only about risk to the company and start demonstrating how you have THEIR best interest at heart beyond the workplace. Then show them how they can be deputized onto the security team.

Using Responsive Delivery to Enhance your Phishing Incentive Program

Learn how one organization began using Responsive Delivery from Cofense PhishMe to send simulations when folks are actually in Outlook. Along with rolling out Cofense PhishMe for mobile, this has enabled the business to reach more users and optimize simulations. Discover also how this Cofense customer reworked its awareness program, now basing it on legitimate phishing emails reported vs. being "first to report," resulting in less spam and more valuable intelligence. See metrics showing how these changes have improved the program's effectiveness.

Holy Mackerel: Reducing Phish Click Rates with Targeted Training

Over 90 percent of breaches began with a phishing email in 2018. How do you determine if your user training is effective? How do you identify repeat clickers and at-risk populations and effectively prepare them to face phishing threats? Understand how to use threat intelligence to identify at-risk populations and A/B testing to verify and implement effective training mechanisms for reducing susceptibility. See a use case showing how to identify employees most likely to be targeted by spear phishing campaigns or high volumes of phishing emails. Grasp the importance of A/B testing to improve an awareness program.

Building a Strong Security Culture with Cofense

Learn how a customer implemented the Cofense Reporter button and how their progression to utilizing Board Reports and Cofense Intelligence™ increased the value of their phishing defense program. Discover how this organization introduced Cofense Reporter into its culture step by step, from executive buy-in to employee security awareness training. Find out how the company uses various Cofense reports to enhance its overall security.

21st Century Security: The Human Factor

The 21st Century firewall isn't technology. It's people. See how a Cofense customer uses a risk-aware, evidenced-based security strategy that includes an integrated Behavior Management and Communications service line. Their use case illustrates a multi-modal approach to cybersecurity that includes both active and passive elements. Through persistent engagement and direct feedback, the program builds awareness, educates staff about the realities of cybercrime, and empowers them to become more security conscious. Discover how this company pursues two main goals: to inspire staff to want to learn about cyber security and to transform information security from a choice to a habit.

Phishing and Security Awareness on a Smaller Scale

How does a smaller sized company build security awareness? Hear from a company with 750 users and no full-time security team. Learn how using the best combination of Cofense solutions has allowed them to secure the organization. Discover how utilizing Cofense Triage via the Cofense Phishing Defense Center enables this company to focus their efforts on real threats that employees report. Understand the roles of Cofense PhishMe and the LMS tool in their phishing defense. Find out how the program manager succeeds, though "it's not my full-time job."

The Importance of Metrics and Communicating the Success of Your Security Program

Learn how mid-size organizations can build a security program. See how to do it on a budget, how to get executive buy-in, what metrics to share in your program's initial stage, and how working with Cofense on security awareness can benefit an organization. Get the perspective of a speaker with 10 years of building three security programs from the ground up—and now working on a fourth!

Practicing Safe Cybersecurity

Aligning your cybersecurity program to the core mission and values of your organization is critical to sustained success. See how one organization, from the CEO down, makes safety its first value. Learn how over the past year they have intensified efforts to promote workplace safety, including: using metrics from Cofense PhishMe during monthly safety meetings; categorizing click rate as a "near miss"; describing Cofense Reporter as a "first responder" that helps colleagues in need; planning the annual safety day around the use of technology; developing and supporting cyber champions; and much more.

The CEO Doesn't Trust You: How to Communicate to Your Clickers

Cofense solutions include a strong educational component for repeat clickers, but getting them to read and absorb educational messages can be a challenge. In an organization where one click can make the difference between a nuisance email or a crippling cyberattack, finding the best ways to reach and train repeat clickers is vital. Discover approaches that can help your organization succeed in curbing the "click impulse."

How Cofense Made "Cents" in Our InfoSec Spending Plan

Threats are constantly growing, but security budgets are not. Learn how one organization prioritized security investment priorities and why Cofense Triage, Reporter, and PhishMe made sense to them. See how these solutions worked well with the products they already had and helped plug holes in their cyber defense. In particular, learn how this company looked at its budget against the cyber kill chain to help make spending decisions. Find out how in less than six months the company increased its phishing resiliency, proving the value of its investments.

Improving Phishing Defense Through Recurring Phishing Simulation and User Awareness

Learn how a consumer-directed benefits company invested in Cofense solutions to improve phishing response and containment. See how this Cofense customer uses a combination of preventative, detective, and corrective security techniques. Discover how they established an ongoing phishing simulation program using key terms and campaigns often seen within their email gateway (O365, Online File Repositories, Signature Services, Financial ACH processes). Find out how they use Cofense Triage to help automate and accelerate responses to malicious emails, plus metrics for targeted simulations to improve user awareness.

Suspicious Email Analysis... For Free!

Your organization has purchased Cofense Reporter and you've started to receive suspicious email submissions. What do you do now? Learn to use free tools, such as online sandboxes and URL analyzers, to perform analysis on anything your employees throw at you while demonstrating on today's most popular malware (Emotet, Hancitor, and Formbook, for example). Gain an understanding of virtual environments that utilize analysis operating systems available at no cost, along with forensic and general-use tools for deep dive/sandbox aware malware. Discover how Cofense Triage can help automate and improve analysis of suspicious emails. Learn to become an analysis rock star using Cofense solutions!

If You Are Not Sending Phishing Emails Every Week, You Are Doing It Wrong

Users need regular reminders of phishing emails observed in the wild. Learn why weekly phishing emails are the bare minimum to maintain awareness. Anything less than this frequency will not be effective and is, at best, a checkbox solution for compliance. Take full advantage of your investment in Cofense PhishMe by using it weekly to achieve the best ROI.

Welcome to the Circus: Quantitative Culture Shifting

Get an introduction to quantitative culture shifting, a systematic approach to measuring behavior across the organization while conveying progress to leadership and remediating concerns. Discover a behavioral index that depicts key security behaviors, including phishing activities, access to high-risk websites, privileges, and other indicators to gain a holistic view. The core objective is to strengthen your culture of information protection by maintaining security consciousness and sustaining change across the user base.

Catch the Phish – Phishing Awareness Strategies in a Multi-National Company

While nothing new, phishing attacks become more and more difficult to prevent. Cyber criminals' strategies have become so convincing that malicious emails are virtually indistinguishable from harmless emails. Conscious of the rising threat posed by phishing, the organization has introduced a set of phishing awareness measures aimed at catching employees' interest in this topic and improving the company's security culture.

The Current State of Phishing: CTO Keynote

Aaron Higbee, and Co-Founder of Cofense will provide a behind-the-scenes look at the pioneering threat intelligence work that's underway at Cofense Labs. He'll share unique insights on real threats we see – both reported and in the wild – and share cutting edge techniques to identify, respond, and mitigate those threats.

The Cofense Product Overview and Road Map

Keith Ibarguen, Chief Product Officer of Cofense, will unpack the latest innovations available today within the Cofense platform as well as share a preview of what's coming in 2020.

Guest Keynote

Hear Kevin Mandia, FireEye CEO and security expert, discuss the state of phishing and the threat landscape.

PhishMe & Content Tips & Tricks

Learn tips and tricks to make your experience with Cofense PhishMe and Cofense Content even more advanced. Are you an experienced operator? We'll show you some "hidden features."