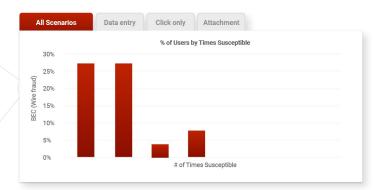# Cofense PhishMe™

EMPLOYEE CONDITIONING FOR RESILIENCY AGAINST PHISHING

Cofense™ research determined that ransomware accounts for more than 97% of all phishing emails. With such alarming numbers, how do you prevent your enterprise from becoming another statistic? Cofense PhishMe empowers employees to become your last line of defense with industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts–transforming one of your biggest liabilities into your strongest defense. Cofense PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% – preparing your last line of defense to recognize and resist tricky phishing attempts.

All Scenarios	Data entry	Click only	Attachment

% of Users by Times Susceptible

Key Benefits

✓ Most effective simulations – The Cofense Intelligence™ product provides the latest phishing tactics and threats which we then turn into the most up-to-date and real-life phishing emails used in Cofense PhishMe to keep your users ahead of the most recent attacks.

✓ Automate scenario deployment with Playbooks - automate your phishing program over the course of a year by leveraging built-in playbooks.

✓ Recipient Management made easy, just upload your user list and Cofense PhishMe will do the rest.

✓ All compliance and awareness modules are included with the award winning Cofense PhishMe product.

✓ Cofense PhishMe Certification - The first and only industry-certification for phishing simulation programs.

✓ Customers are able to implement the Cofense Reporter™ button which provides end users with easy one-click reporting of suspicious emails from their computers or mobile devices.

✓ Board reports providing customers with executive level customized reports.

✓ Gartner lists Cofense is a leader in the computer awareness computer based training (CBT) space.

✓ Forrester case study showed a 336% ROI for Cofense solutions with a 2.7 month payback.

✓ HTTPS for Scenarios allows you to educate your employees on the increasing use of fake SSL certificates in phishing emails and websites.

What is Cofense PHISHME?

Cofense PhishMe is a purpose-built SaaS platform that improves employee response to phishing attacks and empowers employees to provide real-time threat intelligence by immersing them in a real-world spear phishing experience. The solution's customizable scenarios focus on emulating the most relevant threats and providing in the moment feedback and education to recipients who fall victim to these exercises.

Our patented technology provides an unmatched range of cyber attack themes, content and customization, and delivers detailed analysis and reporting for each scenario. Cofense's world class customer support ensures exercises are conducted in a controlled manner that does not compromise security or create negative backlash.

Customizable Content and Relevant Training

Cofense PhishMe's scenarios can be customized to simulate a variety of attack techniques including drive-by, malware, and social engineering attacks, as well as more advanced tactics such as Business Email Compromise (BEC), conversational phishing, and highly personalized spear phishing. Additionally, customers can run scenarios to benchmark their progress against Cofense's growing number of customers.

Customers can build their own scenarios or use one of dozens of customizable pre-built templates. Our expanding library of content covers a multitude of security topics such as phishing, security awareness, compliance, and social media in various formats, including HTML5 templates, videos, and a game module. With multilingual content and education, Cofense addresses the diverse cultural needs of regional and global businesses.

For organizations that require more comprehensive training, Cofense offers fully SCORM compliant educational content that covers general security topics. Available training covers the following topics:

- Spear phishing awareness
- Malicious links
- Malware
- Password security
- Data protection
- Mobile devices
- Safer web surfing
- Social engineering
- Social networking
- Physical security
- Working outside the office
- Reporting suspicious activity
- Ransomware
- Business Email Compromise (BEC)
- Advanced spear phishing

Secure Delivery Platform

The Cofense PhishMe SaaS platform is certified as a Service Organization Controls (SOC) 2 Type I environment with regard to security, availability, and confidentiality principles defined by the American Institute of Certified Public Accountants (AICPA). Cofense PhishMe environments are regularly audited by internal and external auditors. Cofense never collects sensitive data from customers when they are using data-entry scenarios in Cofense PhishMe product.

Detailed Analytics

Each scenario provides metrics to track a multitude of data points that, when analyzed over time, provide insight into organizational suspceptibility and offer a path for continuous improvement.

Cofense PhishMe's reporting tracks, for example:

- Geolocation
- Timestamps
- Individual responses
- Trends
- Time spent on training
- Time to first report (Reporter required)
- Browser enumeration
- Organizational Resiliency (Reporter required)

Ensure Customer Success

Each Cofense PhishMe license includes access to Cofense's world class customer support. In addition to ensuring proper delivery of email-based scenarios, our support team provides expert advice for implementing Cofense PhishMe, reviewing email scenarios against industry best practices, tailoring the program to an organization's culture, leadership, and user base, and providing assistance for new features and scenarios.

If resources are limited, organizations can also leverage Cofense PhishMe as a partially or fully-managed solution with a dedicated professional assigned to their account who creates, executes, and analyzes the results of campaigns. Programs are customized for an organization's requirements and culture.

ONE SOURCE COMMUNICATIONS