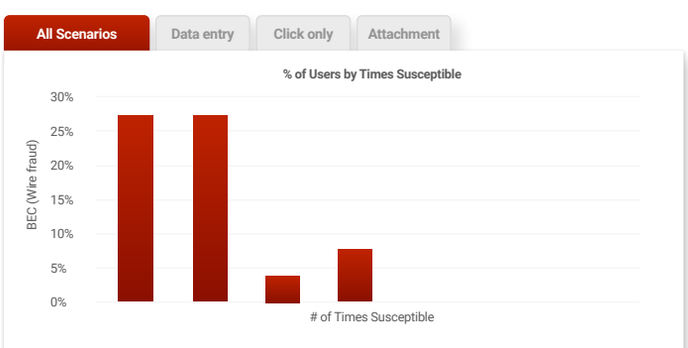
Cofense PhishMe™

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 defence with industry-proven behavioral conditioning methods to better prepare employees to recognise and resist malicious phishing attempts–transforming one of your biggest liabilities into your strongest defence. Cofense has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% – preparing your last line of defence to recognise and resist tricky phishing attempts.



Key Benefits

- Unique and comprehensive phishing-specific incident response solution
- Full integration with Cofense Reporter™ allows threat prioritisation based on user reputation, attributes, and threat intelligence
- Provides active report clustering to identify threats faster
- Integrates with security technologies such as sandboxes, URL analysis solutions, and SIEM solutions for enhanced detection capabilities
- Allows Incident responders to share results with upstream security teams to prevent future attacks

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 customisable 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 customisation, 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.

> Cofence's Enhanced Analytics reporting is invaluable. Using that data, we were able to modify our phishing defence programmes with more targeted education, specifically for those employees with high click rates in an effort to reduce that number.
>
> **Jim Stewart, CISO, United Community Bank**

Customisable Content and Relevant Training

Cofense PhisMe scenarios can be customised to simulate a variety of attack techniques including drive-by, malware, and social engineering attacks, as well as more advanced tactics such as conversational phishing and highly personalised spear phishing. In addition, 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 customisable 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 organisations 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

Our SaaS platform is deployed in a Tier III SOC 2 and SOC 3 certified facility in the United States and an ISO9001:2008 certified facility in Europe. Both are regularly externally penetration-tested and feature robust access controls. All data is encrypted at rest, and Cofense never collects sensitive data from customers during data-entry scenarios.

Detailed Analytics

Each scenario provides metrics to track a multitude of data points that, when analysed over time, provide insight into organisational 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
- Organisational Resiliency (Reporter required)

Ensure Customer Success

Each PhishMe licence 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 PhishMe, reviewing email scenarios against industry best practices, tailoring the programme to an organisation's culture, leadership, and user base, and providing assistance for new features and scenarios.

If resources are limited, organisations can also leverage Cofenes PhishMe as a partially or fully-managed solution with a dedicated professional assigned to their account who creates, executes, and analyses the results of campaigns. Programmes are customised for an organisation's requirements and culture.

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175