



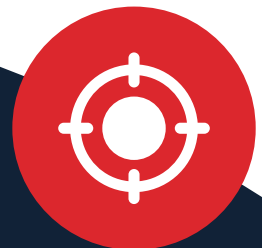
Cofense Research determined that ransomware accounts for more than 97% of all phishing emails. With such alarming numbers, how do you prevent your enterprise from becoming another statistic? Cofense PhishMe empowers employees to become your last line of defense with industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts—transforming one of your biggest liabilities into your strongest defense. Cofense 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.



## Key Benefits

- ✓ Unique and comprehensive phishing-specific incident response solution
- ✓ Full integration with Cofense Reporter™ allows threat prioritization 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 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.



Cofense’s Enhanced Analytics reporting is invaluable. Using that data, we were able to modify our phishing defense programs 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**

## Customizable Content and Relevant Training

Cofense PhishMe 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 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

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 pentested 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 analyzed over time, provide insight into organizational susceptibility 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 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 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.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.



**W:** [cofense.com/contact](https://www.cofense.com/contact) **T:** 703.652.0717  
**A:** 1602 Village Market Blvd, SE #400  
 Leesburg, VA 20175