COFENSE PHISHME®

Turn Targets into **Defenders.**

The Problem

Did you know that security researchers identified a 48% increase in cyberattack attempts targeting email accounts in the first six months of 2022 and almost 70% of those attacks included a credential phishing link? The fact remains, no matter how good your perimeter security, email security threats still reach users and threaten to trigger breaches. Having a workforce conditioned to identify and report suspicious emails is a force multiplier in your battle against those that wish to do harm. Technology alone is not enough. Training your end users to recognize and report today's evolving attacks is crucial to success.

Our Solution

Condition users to identify (real) email threats. Cofense PhishMe educates users on the real threats and tactics facing your company. Our solution leverages crowd-sourced threat intelligence from a network of 35+ million human sensors worldwide and front line phishing defense resources that other providers lack. Through experiential learning—simulations of current email threats—you'll condition smarter email behavior, transforming vulnerable targets into your best line of defense.

The Cofense Phishing Defense Center™ finds that 90% of user-reported emails happen in environments with active Secure Email Gateways (SEGs) in place.

Cofense PhishMe conditions users to recognize and report bad emails, uniting your human defenders in the fight against email threats.

BE RELEVANT. For maximum impact, simulation programs need to focus on real threats to the organization. Security awareness teams have limited opportunities to send simulations – they have to make every opportunity count.

BE EFFICIENT. Save time through automation. Cofense PhishMe can automatically help ease the overhead of defining, scheduling, and delivering a security awareness program based on best practice and tailored to your organization's security needs and priorities.

BE CONFIDENT. Cofense pioneered this market and our wealth of experience allows us to deliver features and capabilities necessary to build a successful email security program to achieve maximum results. Cofense allows you to measure and improve individual resiliency so you can be confident that your users are absorbing security training and becoming active front-line defenders through reporting.

How Cofense PhishMe Works

Cofense PhishMe is a SaaS platform that immerses users in a real-world experience. The solution's customizable scenarios simulate the most relevant threats, like BEC (Business Email Compromise), and provide instant, relevant education to users who are the most susceptible to these attacks.

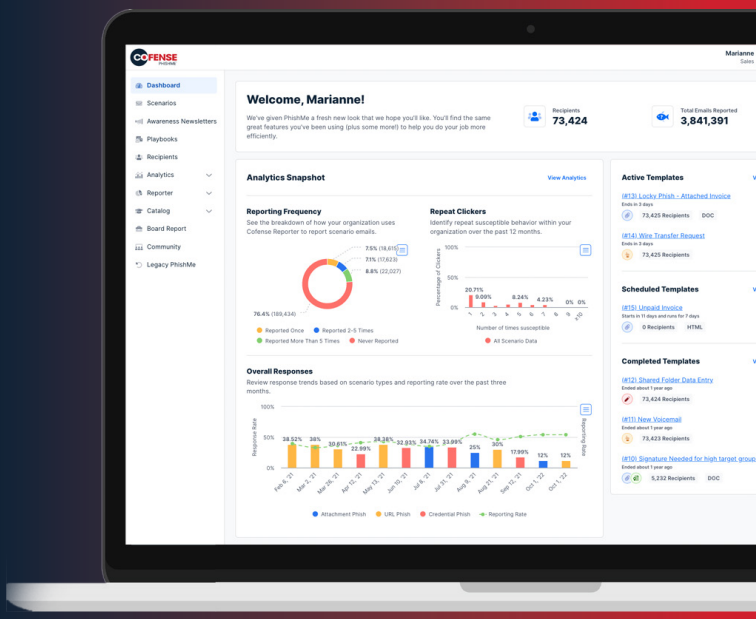
Our patented technology provides an unmatched range of cyber-attack themes, content, and customizations. It delivers detailed analysis and reporting for each scenario. Our customer support team ensures your exercises are conducted in a controlled manner that does not compromise security or create backlash.

Intelligent Automation

Increase operational efficiency while maintaining your Security Awareness program. Cofense PhishMe Playbooks provide a series of prepared scenarios, landing pages, attachments, and educational content to run throughout the year. With multiple Playbook support, you can easily execute simulations programs for different regions, languages, or competency levels. Our Smart Suggest capability recommends scenarios based on program history and industry relevance. With Responsive Delivery, you can maximize user engagement by delivering simulations only when users are active in their inbox. This also eliminates technical and time zone related scheduling issues. Automate user provisioning, updates, and deprovisioning of PhishMe recipients from your organization's user directory service using Recipient Sync.

Active Threat Scenarios

Cofense Intelligence™, Cofense Labs™, and the Cofense Phishing Defense Center™ all feed information on active threats into our scenarios. With our Active Threat templates, you can find email threat scenarios, like BEC, matching attacks against your company or industry. This conditions your users to more effectively spot and report real-world attacks that hit an employee's inbox. You can even search for scenarios based on phish observed to bypass secure email gateways, including those deployed at your organization—simply use the SEG Misses filter. If you're not teaching users about the most serious threats to your company, users won't be able to help security teams stop them. Our Active Threats scenarios keep your simulation awareness program aligned to the ever-changing tactics of today's threat actors.



Secure Delivery Platform

The Cofense PhishMe SaaS platform is certified as a Service Organization Controls (SOC) 2 Type II 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. Robust anonymization supports your privacy-sensitive environments.

Valuable Reporting Metrics

By encouraging end users to to report suspicious emails quickly, your employees will transform from potential liabilities into a strong front-line of defense for your organization. Over time, you'll switch your focus from click rates to reporting, the metric that matters most. For a true picture of program effectiveness and improvements to resilience, combine reporting data to understand and predict how users are likely to react during a real attack. Additionally, Board Reports allow your executives to monitor company performance and track the change in organizational resiliency to email attacks.

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, Cofense is the only comprehensive email security solution powered by a global network of 35+ million reporters which utilizes a combination of unique intelligence sources to identify, protect, detect and respond to all email security threats. Powered by the Cofense Phishing Detection and Response (PDR) platform, organizations that deploy the full suite of Cofense solutions can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact T: 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175