TURN TARGETS INTO **DEFENDERS.**

COFENSE PHISHME™

YOUR **PROBLEM.**

No matter how good your perimeter security, phishing emails still reach users and threaten to trigger breaches. The Cofense Phishing Defense Center™ finds that 90% of user-reported emails are in environments using secure email gateways (SEGs). Every phishing email that reaches the user is an attack on your organization. When technology fails, users need to become human sensors and report phishing, so the SOC can remediate the threat. But how can users report if they don't recognize today's evolving attacks?

OUR **SOLUTION.**

Teach users to identify (real) phish. Cofense PhishMe educates users on the real phishing tactics your company faces. We leverage extensive research, threat intelligence, and front-line phishing defense resources that other providers lack. We believe that real phish are the real problem. Through experiential learning—simulations of current phishing threats—you'll condition smarter email behavior, transforming vulnerable targets into an essential layer of defense.

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

BE RELEVANT.

For maximum impact, phishing simulation programs need to be focused 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 phishing awareness program that is on best practice and tailored to your organizational security needs and priorities.

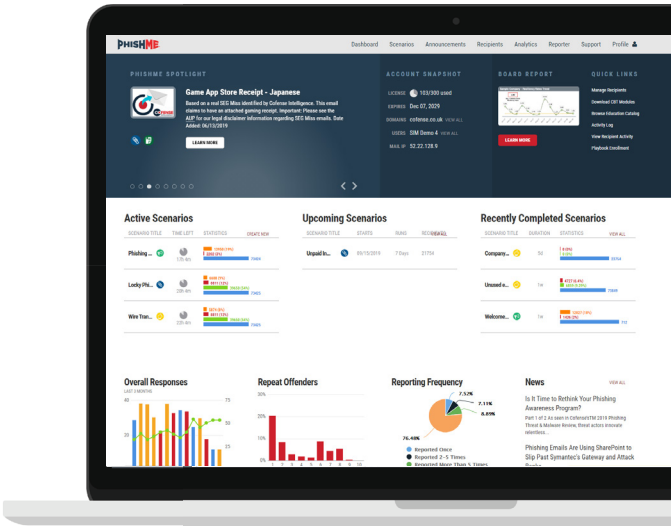
BE CONFIDENT.

Cofense pioneered this market and our wealth of experience allows us to deliver features and capabilities that let you organize a successful phishing program to achieve maximum results. Cofense is consistenly named a leader in the Gartner Magic Quadrant for Security Awareness Computer-Based Training. Go with a trusted innovator.

HOW **COFENSE PHISHME** WORKS.

Cofense PhishMe is a SaaS platform that immerses users in a real-world phishing experience. The solution's customizable scenarios simulate the most relevant threats 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 customization. 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.

Save effort as you maintain your phishing awareness program. Cofense PhishMe Playbooks provide a series of prepared phishing scenarios, landing pages, attachments, and educational content to run throughout the year.
Our Smart Suggest capability uses machine learning to recommend 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. There is no greater combined source on phishing attacker tricks and techniques.
With our Active Threat templates, you can find phishing scenarios matching attacks against your company or industry, helping users more effectively spot and report real-world attacks. You can even search for scenarios based on phish observed to bypass secure email gateways, such as 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 phishing awareness program aligned to the ever-changing landscape.

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 users to report potential phishing emails, you'll turn employees into active defenders. 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 phishing 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 phishing attacks.

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.

COFENSE

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