Phishing is the primary method of entry in cyber-attacks worldwide and many high profile breaches emanate from a single successful phish. Since it typically takes more than 100 days to detect a breach, global organizations need to focus their efforts on prevention and response to neutralize these highly successful attack methods.

Phishing is the #1 Attack Method

Even with record investments in cyber security, the number of breaches attributed to phishing attacks continues to grow. It’s obvious that “next-gen” technology alone can’t solve the problem. That’s why Cofense solutions focus on engaging the human—your last line of defense after a phish bypasses other technology—for better prevention and response. Cofense delivers a comprehensive human phishing defense platform. It fortifies employees and enables incident response teams to quickly analyze and respond to targeted phishing attacks.

Human-Driven Phishing Solutions

What do you get when you combine best-in-class incident response technologies with employee-sourced attack intelligence? Complete, collaborative, and collective defense against email-based cyberattacks. Cofense’s solutions anticipate and disrupt the attack kill chain at delivery to stay ahead of breaches. Quickly mitigate threats such as spear phishing, ransomware, malware, and business email compromise.

OUR SOLUTIONS FOR YOUR ORGANIZATION

SPEED RESPONSE

VISION

INTELLIGENCE

TRIAGE

REPORTER

BUILD RESILIENCE

SIEM

Anti-Malware

Analysis

Threat Intelligence

Automation & Orchestration

End User

Web Browser

Mobile Device
Turn Employees into Informants

The powerful combination of Cofense PhishMe™ and Cofense Reporter™ conditions employees to resist phishing attempts and empowers them to become part of the defense by reporting potentially malicious phishing attacks in real time.

Cofense PhishMe - Reducing Employee Susceptibility to Phishing

Cofense PhishMe uses industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts—transforming your biggest liability into your strongest defense.

Available as a SaaS platform, Cofense PhishMe generates customized phishing attack scenarios recreating a variety of such real-world attack techniques as:

- Spear phishing attacks
- Social engineering attacks
- Malware and malicious attachments
- Drive-by attacks
- Advanced conversational phishing attacks
- Business Email Compromise (BEC)

Cofense PhishMe is easy to administer and provides deep metrics, benchmarking, and reporting options, including custom Board Reports. Users can get up and running quickly and automate their phishing programs by leveraging built-in playbooks—a series of prepared scenarios, landing pages, attachments, and educational pages distributed to run over the course of a year—easing the administration of your phishing program. Additionally, operators can increase the efficiency of their phishing program by ensuring simulations are only delivered when users are active in their inbox using Responsive Delivery. Cofense PhishMe is the only solution able to track Microsoft Office® attachments—the number one phishing attack type. The solution also provides pre-built and customizable phishing scenarios in an ever-expanding library of content in multiple languages, featuring HTML 5 templates, videos, and gaming modules.

Cofense Reporter - Simple Reporting for all Employees

Cofense Reporter is an easy-to-use add-in that enables users to report suspicious emails with a simple click from their email client. Cofense Reporter can be deployed on desktop mail clients and on mail clients on Apple and Android mobile devices. The user-generated reports are then forwarded to your security teams, containing the full header and attachments of reported emails for further security analysis and incident response. Cofense Reporter is included as part of any standard Cofense PhishMe license to help customers gather internal attack intelligence. It works with most popular email solutions including Outlook®, Office 365®, Gmail®, and IBM Notes®.

Cofense Mobile Reporter is the only solution removing that attack blind spot.

Cofense CBFree™ - CBTs for FREE

Cofense recognizes security awareness Computer Based Training (CBT). That’s why we developed a set of SCORM-compliant materials free for any organization that needs it. Our library of security awareness CBTs includes multiple awareness, compliance, microlearning, and game modules that have been developed using the latest eLearning techniques and trends that promote substantial engagement by the pupil. Each module takes about 3-5 minutes to complete and comes with an optional 5 minutes of interactive Q&A. CBFree works with or without an LMS so is easily added into any online learning program.
**Cofense Triage and Cofense Vision - Phishing Incident Response Platform**

Cofense Triage is the first phishing-specific incident response platform that stops attacks in progress. Cofense Triage operationalizes the collection and prioritization of employee-reported threats whether from other sources or directly from Cofense Reporter. It drives faster, more effective phishing analysis and mitigation - automating front-line analysis and orchestrating response across your security teams.

Cofense Vision stores, indexes, and enriches a moving window of email messages in a client environment, enabling security teams to take action against unreported malicious emails. Using Cofense Vision, security operations teams can extend Cofense clustering logic to find the full breadth of an attack, quickly and efficiently. From there, operators can rapidly remove threats from users’ mailboxes by quarantining emails.

**Cofense Intelligence - Phishing Threat Intelligence**

Cofense Intelligence is a phishing-specific threat intelligence solution that delivers the right information at the right time to help defend your network. Cofense Intelligence uses proprietary techniques to analyze millions of messages daily from a wide variety of sources. It automatically dissect messages to identify new and emerging phishing and malware threats. A team of analysts dive into these messages to eliminate false positives while delivering the right intelligence when it is needed. Cofense Intelligence is distributed in multiple formats including Machine-Readable Threat Intelligence (MRTI) for quick and easy integration into other security solutions.

- **TIMELY:** Real-time analysis, real-time publishing. New reports are published as they are confirmed throughout the day.
- **ACCURATE:** Our analysts provide context by connecting the indicators to malware families. We tell you that something is bad, how bad, why it is bad, and which malware is involved.
- **RELEVANT:** Our analysts dissect malware and determine which indicators are important to help determine if malware is running inside your perimeter and preemptively block it.
- **CONSUMABLE:** Delivered in the format you need. Intelligence Feed Formats include: Machine-Readable Threat Intelligence - STIX, JSON, CEF; Human-Readable Threat Intelligence - PDF, HTML; SaaS Investigation platform - Web, API.
Ensuring Success with Cofense Professional Services

If resources are limited, dedicated professional services are available for partially or fully-managed deployments of Cofense solutions. This includes a dedicated Cofense security expert assigned exclusively to each account to assist in the creation, execution, and analysis of your phishing defense programs. Programs are customized for an organization’s requirements and diverse cultural environments.

Cofense Support and Community

Each Cofense license includes access to our world-class customer support and customer community platform.

Cofense Support

Our support provides expert advice for implementing Cofense’s solutions, including:

- Reviewing scenarios against industry best practices
- Effectively leveraging Cofense solutions
- Providing assistance for new features and scenarios
- Tailoring comprehensive phishing defense programs for each organization

Cofense Community

The Cofense Community provides an easily accessible online knowledge-base where users can share and can come together to discover, develop, and connect to expert resources and peer advisors to improve and grow their Cofense programs. The Cofense Community is a place for users of Cofense solutions and products to access all the information and tools needed to improve and expand their anti-phishing programs.

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  T: 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175