Phishing is the primary method of entry in 91% of cyber-attacks world-wide and many high profile breaches emanate from a single, successful phish. Since it typically takes more than 200 days to detect a breach, global organizations need to focus their efforts on prevention and response to neutralize these highly successful attack methods.

Cofense helps to significantly speed the collection, analysis and response to real phishing threats. Even with record investments, the number of breaches attributed to phishing attacks, continues to grow. It’s obvious that 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 focused on fortifying employees and enabling incident response teams to quickly analyze and respond to targeted phishing attacks.

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, triggering enterprise-wide security automation and orchestration. Now you can disrupt attacks in progress to stay ahead of breaches. Quickly mitigate threats such as spear phishing, ransomware, malware and business email compromise.

Phishing is the #1 Attack Method
Phishing is the primary method of entry in 91% of cyber-attacks world-wide and many high profile breaches emanate from a single, successful phish. Since it typically takes more than 200 days to detect a breach, global organizations need to focus their efforts on prevention and response to neutralize these highly successful attack methods.

Human-Driven Phishing Solutions
Even with record investments, the number of breaches attributed to phishing attacks, continues to grow. It’s obvious that 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 focused on fortifying employees and enabling incident response teams to quickly analyze and respond to targeted phishing attacks.

OUR SOLUTIONS FOR YOUR ORGANIZATION

RECOGNIZE
When a phish gets through your technology, your employees need to be able to recognize the attempt.

REPORT
Engaging employees to report attacks in progress can significantly decrease time to respond to developing threats and attacks in progress.

RESPOND
Cofense helps to significantly speed the collection, analysis and response to real phishing threats.

RESEARCH
Cofense focuses on phishing-specific threats and provides human-vetted analysis of phishing and ransomware campaigns and the malware they contain.

CONDITION EMPLOYEES
To Recognize and Report Threats

Cofense PhishMe  Cofense Reporter  Cofense Triage  Cofense Intelligence

SPEED INCIDENT RESPONSE
Collect, Analyze, and Respond to Verified Active Threats
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.

Provided as a SaaS-based conditioning 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

Cofense PhishMe is easy to administer and provides deep metrics, benchmarking and reporting options. The solution provides pre-built and customizable phishing scenarios in an ever-expanding library of content in 19 languages, featuring HTML 5 templates, videos and gaming modules.

Topics cover a multitude of security concerns, including:

- Phishing
- Security awareness
- Risk and compliance
- Social media in various formats

Cofense Reporter™ - Simple Reporting for all Employees

Cofense Reporter is an easy-to-use email client add-in that enables users to report suspicious emails with a simple click. 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 CBFree™ - CBTs for FREE

Cofense recognizes security awareness Computer Based Training (CBT) helps check-a-box to satisfy compliance needs. 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 12 modules that have been developed using the latest eLearning techniques and trends that promote substantial engagement by the pupil. Each module takes about 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 Intelligence™ strengthen your organization’s ability to quickly identify and respond to phishing attacks in progress. With the entire employee-base now reporting malicious emails, the SOC and IR teams must collect, prioritize, analyze and respond efficiently to keep up with the volume of reported threats.

Cofense Triage is the first phishing-specific incident response platform that allows security operation (SOC) and incident responders to automate the prioritization, analysis and response to phishing threats that bypass your email security technologies.

Cofense Triage gives incident responders the visibility and analytics needed to speed processing and response to employee-reported phishing threats and decrease your risk of breach. Cofense Triage operationalizes the collection and prioritization of employee-reported threats whether from other sources or directly from Cofense Reporter.

Available on-premises, hosted or as a managed service, Cofense Triage provides real-time visibility and fast verification of attacks in progress. Cofense Triage seamlessly integrates with your existing security solutions including SIEM, Anti-malware, Analysis and Threat Intelligence solutions.

Sender Name(s)

<table>
<thead>
<tr>
<th>Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bashar Bagdadi</td>
<td>1</td>
</tr>
</tbody>
</table>

Malware description

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keylogger</td>
<td>Malware capable of collecting victim...</td>
</tr>
</tbody>
</table>

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, including 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 knowledgebase 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.