

Human Phishing Defense

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 PhishMe solutions focus on engaging the human—your last line of defense after a phish bypasses other technology—for better prevention and response. PhishMe 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.

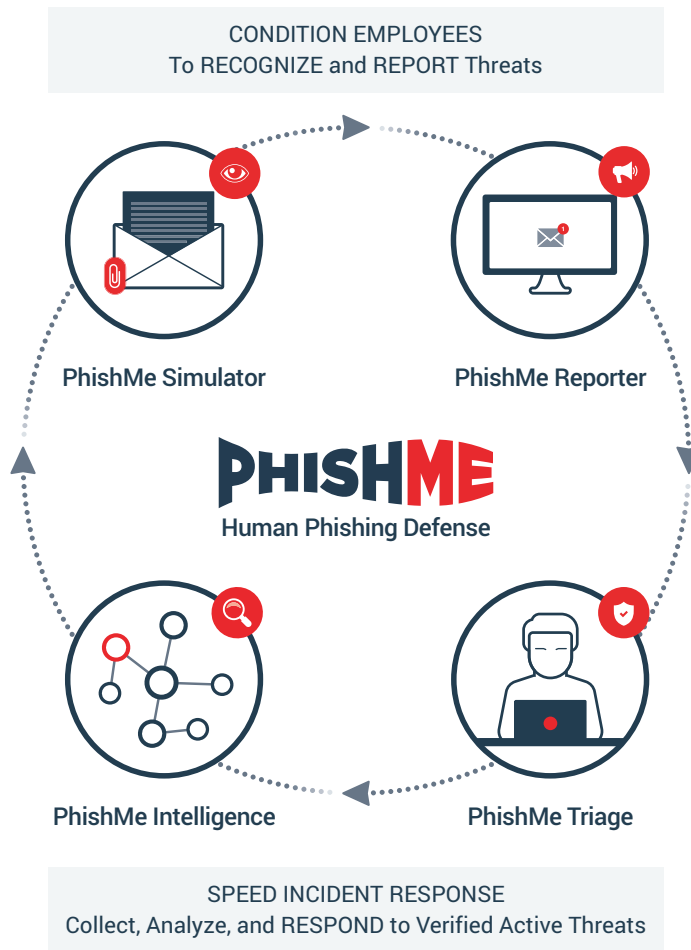
TURN EMPLOYEES INTO INFORMANTS

The powerful combination of PhishMe Simulator™ and PhishMe 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.

PhishMe Simulator - Reducing Employee Susceptibility to Phishing

PhishMe Simulator 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, PhishMe Simulator 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



PhishMe Simulator 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

PhishMe Reporter - Simple Reporting for all Employees

PhishMe 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.

PhishMe Reporter is included as part of any standard PhishMe Simulator license to help customers gather internal attack intelligence. It works with most popular email solutions including Outlook, Office 365, Gmail and IBM Notes.

PhishMe CBFree - CBTs for FREE

PhishMe 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.

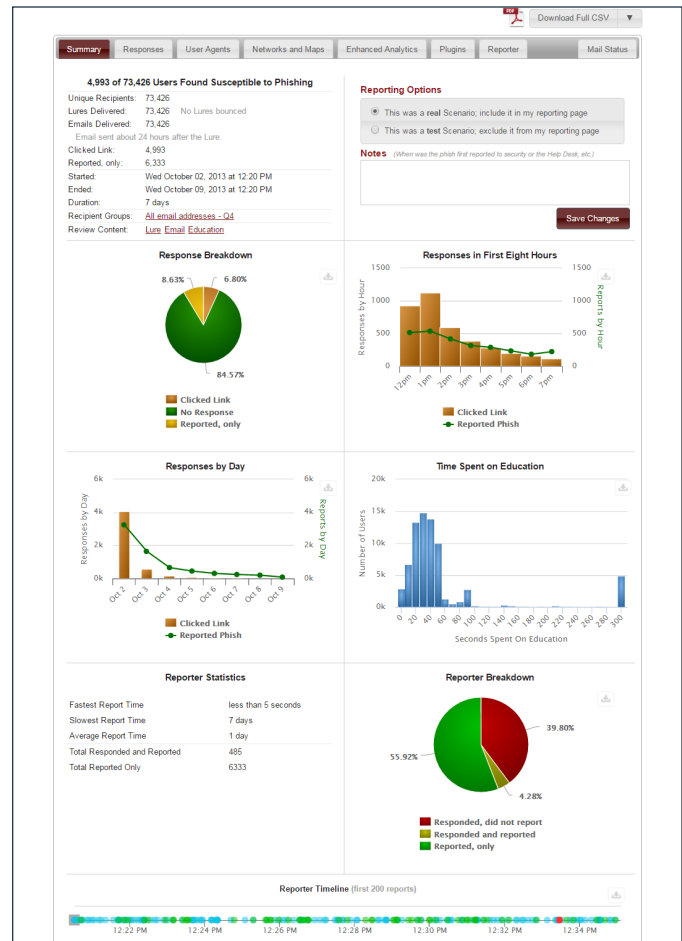


Figure 1 - PhishMe Simulator Dashboard

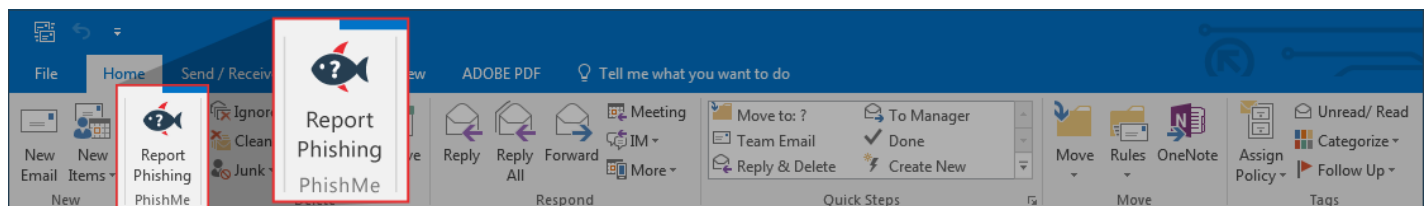


Figure 2 - Outlook Ribbon Bar with PhishMe Reporter installed

SPEED INCIDENT RESPONSE

PhishMe Triage™ and PhishMe 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.

PhishMe Triage - Phishing Incident Response

PhishMe Triage is the first phishing-specific incident response platform that allows security operation and incident responders to automate the identification, prioritization and response to threats delivered via phishing emails.

PhishMe Triage gives incident responders the visibility and analytics needed for email-based attacks occurring against their organization in near real time. PhishMe Triage operationalizes the collection and prioritization of employee-reported threats whether from other sources or directly from PhishMe Reporter. Available as hardware or virtual appliance, PhishMe Triage seamlessly integrates with your existing SIEM, malware and domain analysis and threat intelligence solutions across a variety of infrastructure environments.

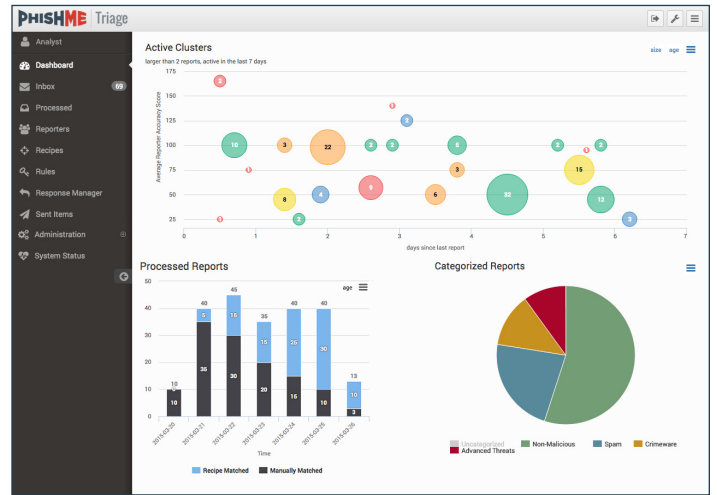


Figure 3 - PhishMe Triage Dashboard

PhishMe Intelligence - Phishing Threat Intelligence

Available as a stand-alone product or integrated with the PhishMe solution suite, PhishMe Intelligence is a high-fidelity, human-verified intelligence service to enable security teams to identify, block and investigate ongoing and evolving threats. Threat data is delivered in multiple forms to effectively prepare and respond to attacks:

- Human-readable threat intelligence reports provide deep-dive analysis of your biggest threats.
- Machine-readable threat intelligence (MRTI) feed directly into security devices and threat repositories.
- SaaS investigation applications research phishing and malware attacks.
- Expert guidance from our global security team to implement industry leading best practices, improve phishing defense outcomes and reduce threats.

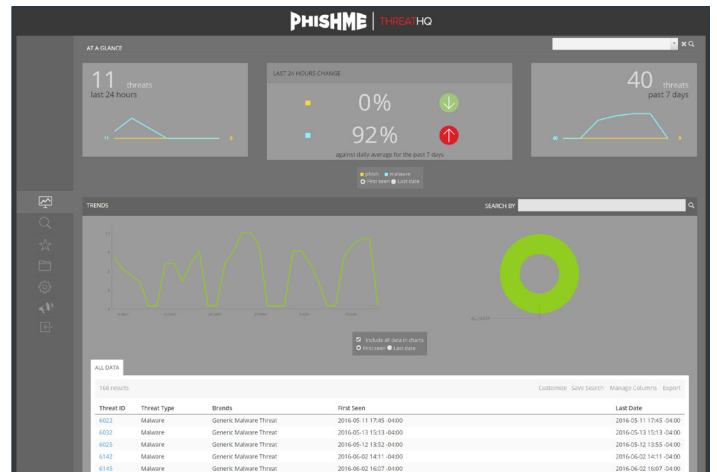


Figure 4 - PhishMe Intelligence Dashboard

PhishMe Intelligence is used by global Fortune 100 organizations and hailed as a trusted, high-fidelity source of phishing-specific threat information.

ENSURING CUSTOMER SUCCESS WITH PHISHME SERVICES

If resources are limited, dedicated professional services are available for partially or fully-managed deployments of PhishMe solutions, including a dedicated PhishMe 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.

PHISHME SUPPORT AND COMMUNITY

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

PhishMe Support provides expert advice for implementing PhishMe's solutions, including:

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

The PhishMe 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 PhishMe programs. The PhishMe Community is a place for users of PhishMe solutions and products to access all the information and tools needed to improve and expand their anti-phishing programs.

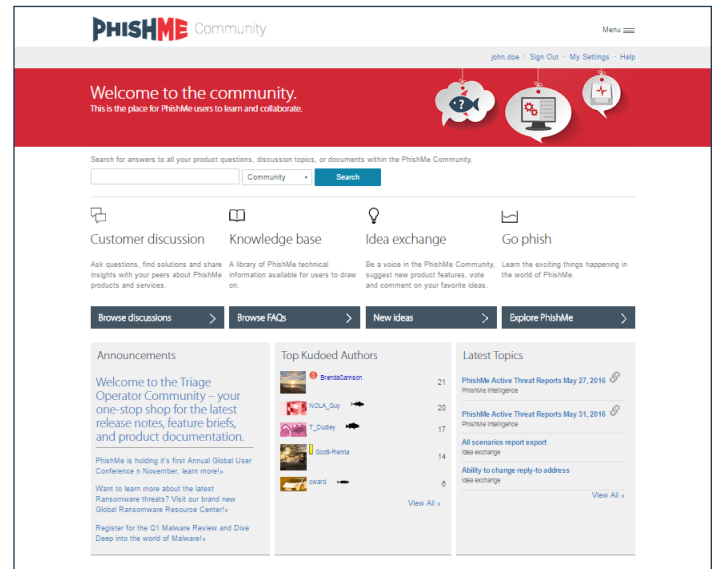


Figure 5 - PhishMe Community Home Page



1608 Village Market Blvd.
Suite #200
Leesburg, VA 20175
Tel: 703.652.0717

WWW.PHISHME.COM

About PhishMe

PhishMe® is the leading provider of threat management for organizations concerned about human susceptibility to advanced targeted attacks. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process. PhishMe's customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

© Copyright 2016 PhishMe, Inc. All rights reserved.