Simulator Small Business Edition

EMPLOYEE CONDITIONING FOR RESILIENCY AGAINST PHISHING

PHISHME

Phishing attacks are a problem for organizations of all sizes. In fact, 38% of spear phishing attacks target companies with under 250 employees because attackers often assume smaller organizations lack the advanced technology of large enterprises. However, the frequent breaches indicate that technology alone is not adequately protecting organizations against phishing incidents.

Key Benefits

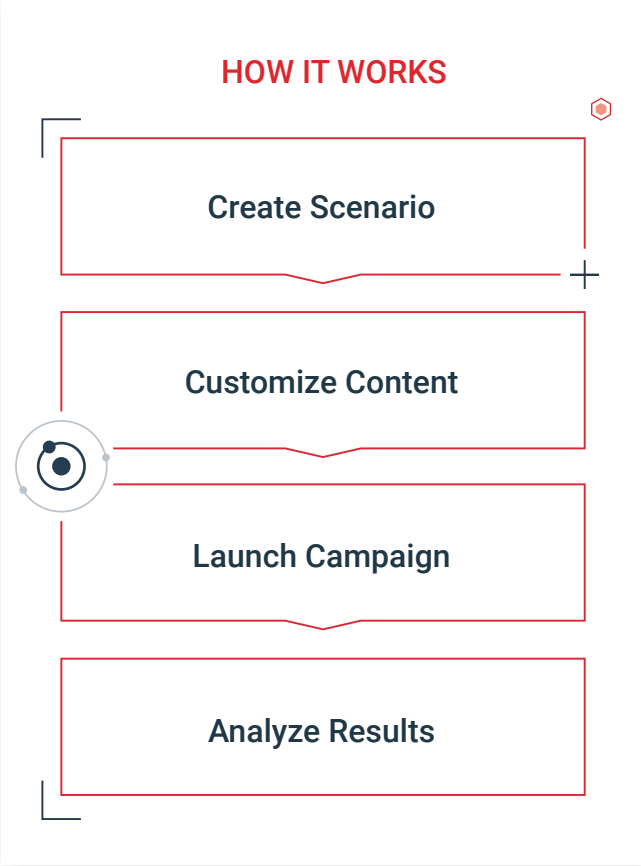
- ✓ Provides real results through a simplified enterprise-grade solution
- ✓ Reduces organizational susceptibility to phishing attacks by more than 95%
- ✓ Deploys quickly, and includes easy to manage SaaS application
- ✓ Mimics real-life attack tactics with threat-based scenario content and training templates
- ✓ Incorporates free Computer-Based Training (CBT) modules
- ✓ Delivers detailed reporting to identify risk and validate program efficacy
- ✓ Based on our award-winning enterprise platform that recently won the 2016 SC Magazine Award for Best IT Security-Related Training Program

Human Phishing Defenses

The human element behind attacks is the reason the technology approach to security is failing. The attacker, a human, is constantly inventing new ways to penetrate your existing security stack. To launch an effective defense, you have to fight fire with fire. Or in this case, human with human, and engage your entire employee base in the war against phishing attacks.

Turn Employees Into Informants

Built specifically for smaller organizations, PhishMe® Simulator™ Small Business Edition (SBE) conditions employee security behavior to identify and deflect phishing attacks through proven, immersive education processes. Simulator SBE accurately mimics real-life spear phishing scenarios and provides instant learning opportunities for recipients who fall for the exercises. The solution provides IT teams with the tools to effectively educate employees while providing employees with the knowledge to thwart phishing attacks aimed at them and your organization.



Pre-Built Learning Scenarios

PhishMe Simulator SBE includes a number of pre-built templates that emulate the latest strategies and techniques used by attackers. These templates are updated continuously based on threat intelligence feeds that PhishMe subscribes to, feedback from our customer base, and information collated by our internal research team. The scenario types include Click-only, Data Entry and Attachment–based.

Learning Content

PhishMe understands that effectively changing user behavior is not accomplished with lengthy, time-consuming training modules, and our content is designed with this in mind. We make our experiential content fun and interactive; addressing the immediate issues with the phishing email they reacted to while still underscoring the seriousness of the issue. The conditioning experience focuses on providing approximately 90 seconds of targeted messaging that matches the context of each scenario. This practice increases efficacy and memory retention and helps you reach your objectives faster.

Reporting

Our reporting dashboard demonstrates real-time results of these immersive exercises, trends data over time, and automatically identifies repeat victims that may need additional assistance.

The PhishMe reporting dashboard provides company performance metrics as well as details about each employee's review and response. These reports can be used to emphasize the ROI from user security behavior management training, tracking the effectiveness of the training over time, identifying the types of employees that are most susceptible to attacks, and pinpointing departments or locations that may be more susceptible than others.

Internal Communication Tools

PhishMe provides you with announcement templates that can be used to gain employee and stakeholder buy-in and communicate important compliance and security-related awareness concerns without having to spend additional budget for the content.

FREE Computer-Based Training Modules

PhishMe also provides you with free compliance mandated computer-based training. This program—CBFree, is a complimentary library of short, security-awareness CBTs that include modules that have been developed using the latest eLearning techniques and trends that promote substantial engagement by the pupil.

World-Class Support via the PhishMe Community

PhishMe Community is an online portal where users can discuss product issues with PhishMe and other users, get product support, access PhishMe's exhaustive knowledge base, exchange ideas with other users, and learn more about the exciting things happening in the world of PhishMe. Access to the community is included with your license.

For more information on Simulator SBE, please email us at contact@phishme.com

PhishMe is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today's top attack vector — spear phishing. 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.

PHISHME

For more information contact:

W: phishme.com/contact T: 703.652.0717
A: 1608 Village Market Blvd, SE #200 Leesburg, VA 20175