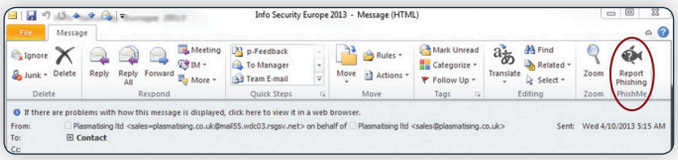
DATA SHEET

PhishMe Reporter™

Engage Your Human Sensors

When technical defenses such as proxy filtering, URL rewriting, and DLP fail, users are the last line of defense. Armed with the proper training, users can provide timely and valuable threat intelligence simply by recognizing and reporting suspicious emails. Organizations have struggled to tap into this resource and, consequently, malicious activities often operate for weeks and even months on the network.

PhishMe Reporter streamlines the reporting process by installing a button on users' Outlook toolbars that, when clicked, sends a report to your security team containing the relevant information needed to analyze and respond.



Enhanced Reporting

Whether or not you have a reporting process in place, Reporter can help you improve by:

- Preserving the full header of reported e-mails, allowing responders to see the true sending IP address to block and remove similar emails.
- Ensuring any attachments are included in report.
- Supplementing PhishMe campaigns, tracking user responses and organizational time to response.

KEY BENEFITS

- **Structure and organize your user reporting process**
- **Detect and respond to threats faster**
- **Block and remove similar emails**
- **Analyze malware attachments**
- **Minimize impact of breaches with proactive response**
- **Prioritize reports of suspicious activity from reliable users**

How Does It Work?

Reporter automatically discerns emails reported from PhishMe scenarios and emails reported from unknown sources, ensuring that only reports of potentially malicious emails are delivered to appropriate security staff.

PhishMe Scenario Emails

Reporter collects reports of emails sent from PhishMe, noting which users reported them and providing the user with customizable acknowledgement of the successful report. Positive reinforcement in the feedback loop further enhances employees' capabilities to accurately identify cyber attacks. This information is tracked and integrated into PhishMe's comprehensive reporting metrics.

Suspicious Unknown Emails

Reports of suspicious unknown emails are forwarded to a designated location where they can be analyzed by an organization's internal security team.Suspicious emails are attached with the original header information contained in the body of the reported phish. Incident response and security operations teams can prioritize their analysis based on a reporting user's reputation for accurately identifying phishing attempts.

Is this email a PhishMe scenario?

About PhishMe

PhishMe® is the leading provider of phishing mitigation and detection for organizations concerned about human susceptibility to sophisticated cyber attacks. PhishMe's immersive training platform turns employees into an active line of defense by enabling them to identify, report and mitigate spear phishing, malware, and drive-by threats. A data-driven 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, critical infrastructure, and Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise. For additional information, please visit: **www.phishme.com.**

PHISHME

25055 Riding Plaza, Suite 260 | Chantilly, VA 20152 | 703.652.0717

WWW.PHISHME.COM