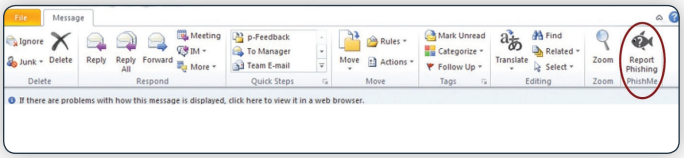
DATA SHEET

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.

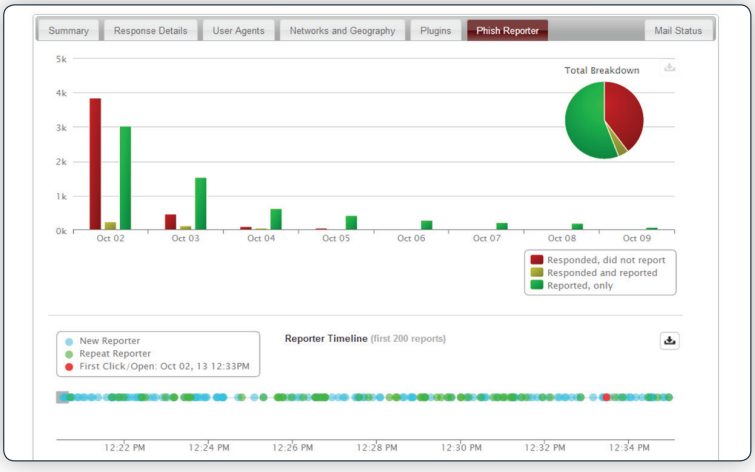
PhishMe Reporter streamlines the reporting process by installing an email add-in on users' email toolbars that, when clicked, sends a suspicious email to your security team containing the relevant information needed to analyze and respond.



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 block and remove similar emails.
- Ensuring any attachments and URLs are included.
- Supplementing Simulator campaigns, tracking user responses and organizational time to response.



KEY BENEFITS

- **Standardize and organize your user reporting process**
- **Detect and respond to email-based threats faster with user-generated reporting**
- **Analyze URL and malware attachments using third-party integrations**
- **Minimize impact of breaches with proactive response and improved visibility**
- **Customizable user feedback encourages employees to be a part of the security process**

How Does It Work?

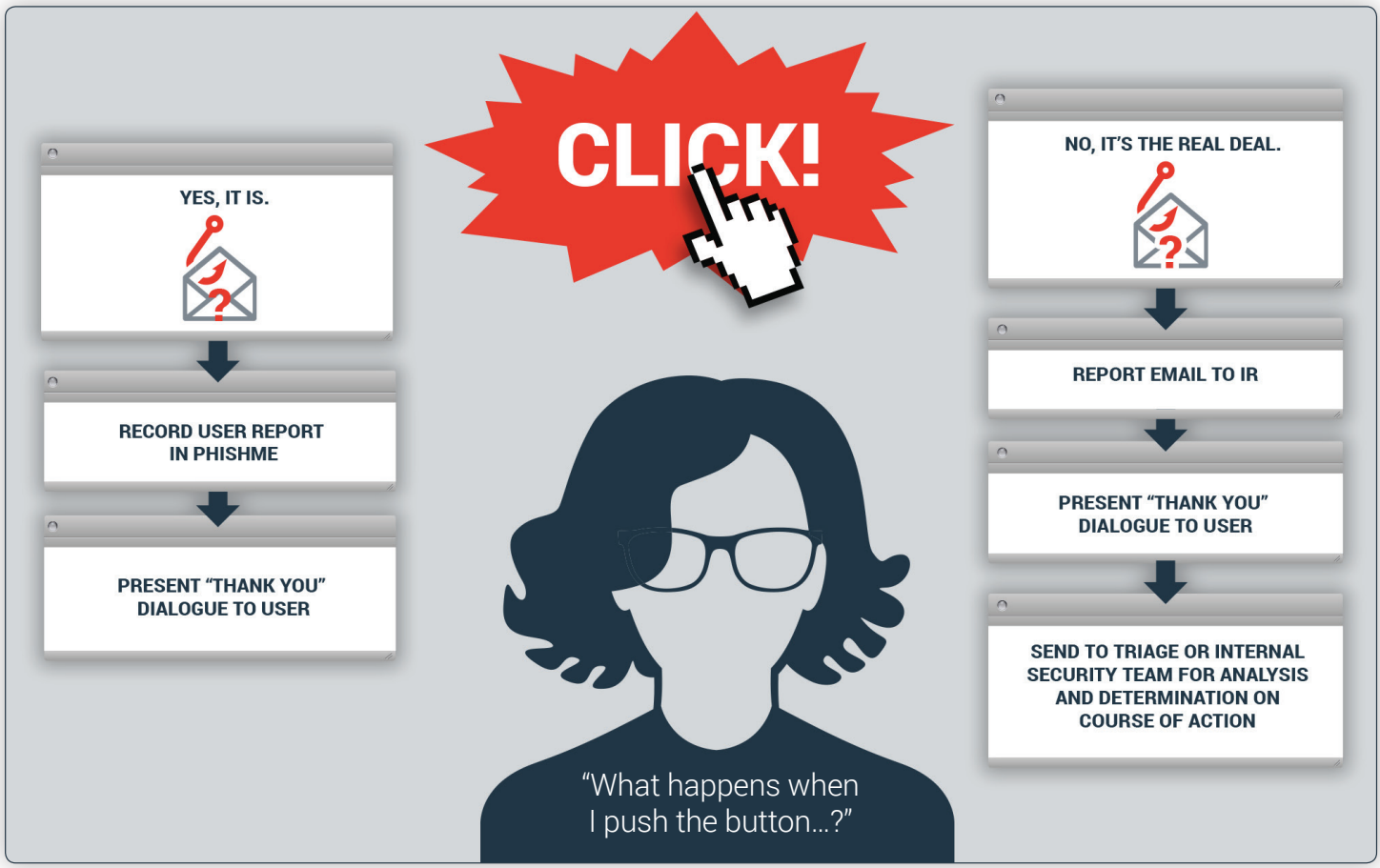
Reporter automatically discerns emails reported from PhishMe Simulator scenarios and emails reported from unknown sources, ensuring that only reports of potentially malicious emails are delivered to appropriate security staff or PhishMe Triage for analysis.

PhishMe Simulator Emails

Reporter collects reports of emails sent from Simulator, 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 the PhishMe solution's comprehensive reporting metrics.

Suspicious Unknown Emails

Reports of suspicious unknown emails are forwarded to a designated location or Triage, where they can be analyzed by an organization's internal security team. Suspicious emails are attached with the original header and contextual information for rapid analysis. Incident response and security operations teams can prioritize their analysis based on a user's reputation for accurately identifying phishing attempts among other attributes when using Triage.



Is this email a PhishMe scenario?

About PhishMe

PhishMe® is the leading provider of Human 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 while operationalizing attack intelligence and phishing incident response for the security team. 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