COFENSE REPORTER™

Why Cofense Reporter

Would you like to effectively showcase your phishing defense program results while increasing user resilience? Do you struggle to gain visibility of threats that have evaded controls, and find it difficult to prioritize and remediate them quickly? We have the solution to these problems waiting for you – it's already part of your PhishMe program and FREE – just say the word!

Benefits to Your Simulation Program

- **Boost resiliency** – More than 50% of well-conditioned users report within the first 5 minutes. Reporter sends users immediate, customizable user feedback which boosts resiliency.
- **Reduce workload** on your helpdesk/SOC teams as reported simulations are suppressed due to full integration with PhishMe.
- **Enhanced PhishMe reporting** – measure effectiveness of your simulated phishing campaigns through increased reporting over time, and measurement of resilience.
- **Ensure behavioral change** and improved security posture. Click rates don't give the full picture. Hitting the reporter button is a deliberate action and an indicator of true behavioral change.
- **Enhanced Board of Director Reports** – PhishMe reports include Reporter and Resiliency metrics.
- **Avoid Technology Interaction Clicks** that are common with 3rd party reporting Add-Ins.
- **Increase employee engagement** with gamification.
- **Promote a positive reporting culture** by rewarding your most reliable reporters with Reporter reputation scoring.

Benefits to Your SOC or IR Teams

- **Identify threats faster** – Cofense Reporter will give your SOC near real time threat intelligence on attacks reaching the inbox.
- **Streamline SOC investigation** with standard formatting of suspicious e-mail reports preserving all information required for effective threat analysis (full header, URLs, attachment hashes and the original message attached).
- **Alleviate SOC and helpdesk workload** by suppressing reported simulations.
- **Zipping and password protection** keeps Exchange from removing header tags, and endpoint/path security devices from removing known malicious content.
- **Easy to deploy** across multiple desktop & mobile email clients.

Top 3 Reasons to Deploy Reporter

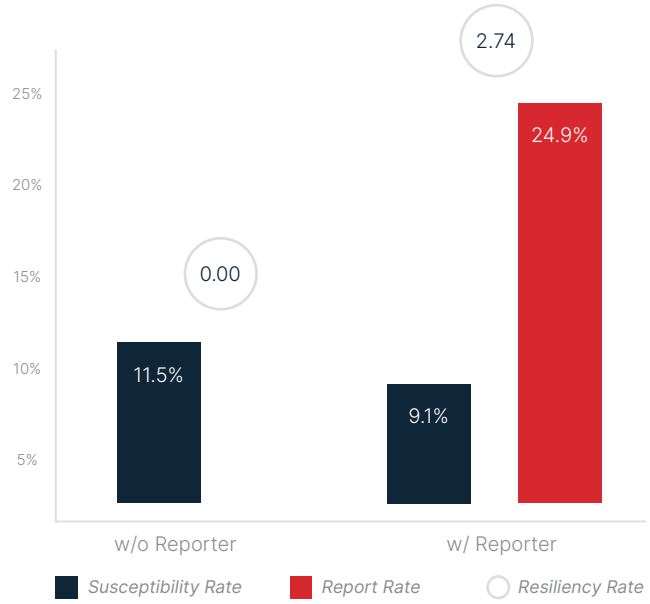
Improve your program metrics while enabling your users to easily report phishing attacks.

Immediate user feedback, including accurate metrics fed back into your PhishMe program to demonstrate program success and increased user resilience.

Near real time visibility of attacks that are reaching the inbox with all information required for effective threat analysis.

Reporter Empowers User Resiliency

Chart - 2020 Resiliency



Susceptibility Rate = [susceptible recipients ÷ emails delivered] This rate shows how many users were susceptible to the scenario versus the total number of emails delivered.

Report Rate = [users who reported ÷ emails delivered] This is a percentage of users that reported the email, without being susceptible to it, compared to the total number of users who received the email.

Resiliency Rate = [reported on rate ÷ susceptibility rate] This is the percentage of users who reported the email without being susceptible to it, compared to the percentage of users who fell susceptible.

Reporter Outpaces the Competition

- Encrypts and sends all reported body contents (zips and password protects)
- Enhanced configuration and customization options
- No limitation on message size
- Multiple options on post-reporting actions

Why Reporter vs. MSFT Button

Microsoft advocates two buttons: Report as Phish and Report as Junk. You can't expect your users to reliably and consistently differentiate between junk and a phish. If a user reports a real threat as junk, rather than as a phish, your organization is at risk. In addition, Microsoft Attack Simulator has limited reporting capabilities and is not integrated with their PhishReport Button.

The Microsoft button **DOES NOT**:

- ✗ Provide any simulation feedback to reinforce the right behavior.
- ✗ Help the SOC team expedite analysis.
- ✗ Preserve all pertinent information for threat analysis

Cofense Reporter message body preserves all pertinent information required for effective threat analysis, segregates reported simulations from real threats to save SOC time, sends users immediate feedback and helps track user resiliency. When you deploy Cofense Reporter you also benefit from the Network Effect of our 25 million plus users!

Deploy Reporter Today – it's already included in your PhishMe program! Just login to PhishMe and hit the Get Reporter button.

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of over 25 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

W: confense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175