Responsive Delivery by Cofense PhishMe™

SEND PHISHING SIMULATIONS WHEN USERS ARE ACTIVE IN THEIR EMAIL CLIENT

Flexibility, Automation, Visibility

When is the best time to send a user a phishing simulation? Clearly, it's when the user is actually using email, so he or she sees the message and is more likely to respond.

Until now, scheduling phishing scenarios for a global workforce has always been challenging. Additionally, whitelisting complications or email gateway security policy updates could affect phishing simulation delivery and skew your organizational susceptibility stats. But with the new Responsive Delivery capability offered by Cofense PhishMe, simulations are automatically delivered when users are active in their email client. You can more accurately track responses to simulated phishes to help users recognize and report malicious messages.

Key Benefits

- ✓ Eliminate time-zone and global scenario scheduling restrictions
- ✓ Eliminate technical whitelisting complications
- ✓ Ensure scenario delivery only when users are **active** in their email client
- ✓ Mobile, tablet, and desktop application compatibility
- ✓ Flexible, efficient scenario delivery

Effective and Efficient Simulation Delivery

The Responsive Delivery capability enables Cofense PhishMe Enterprise Edition operators to deliver scenario emails ONLY when recipients are actively performing tasks in their email client. Phishing simulation delivery is streamlined through automation, making your simulation program more efficient and effective. **Responsive Delivery:**

- Eliminates the need to guess when global employees are actively using email
- Ensures that scenario emails are successfully delivered, eliminating technical whitelisting challenges
- Works on mobile, tablet, and desktops!

Why does it matter?

Simple. Operators can give every user a better opportunity to receive and interact with a phishing simulation, regardless of their timezone. Moreover, operators can accurately track and measure user interactions and, ultimately, organizational resiliency to phishing. By eliminating any complications arising from whitelisting or email gateway security policy updates, operators can ensure that users receive the phishing simulations each and every time.

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175