Cymulate

Phishing Awareness Assessment

Solution Brief

Challenges

The ever-present phishing threat continues to be a major breach entry point, even with significant investments in email security. Employees are the first line of defense against such attacks, making it crucial to regularly test their alertness and awareness of emerging phishing techniques through efficient pre-emptive measures.

However, running phishing awareness campaigns is resource intensive. It requires creating production-safe inactive payloads to gauge the potential reach of successfully luring an employee, tracking phishing email success rates and attribution, crafting a variety of high-quality, well-designed phishing emails , and, when necessary, fake landing pages.

Due to limited resources, many organizations opt to rely on annual phishing awareness training instead of addressing these challenges head-on.

Overview

Cymulate's Phishing Awareness campaigns evaluate employees' security awareness levels by simulating phishing attacks and identifying potential target opportunities.

Creating a customized phishing simulation with the user-friendly drag-and-drop menu is quick and easy. Options include the selection of email text, attachments with production-safe payloads, fake landing pages, and more.

Employees' interactions with the mock phishing emails are automatically recorded, logging hazardous behaviors such as clicking links or entering credentials. This identifies employees in need of additional phishing awareness training.

Benefits

- Customization wizard
- Scalable
- Repeatable
- Schedulable
- Automated report generation

Phishing Awareness with Cymulate

Cymulate

Main Features

Drag-and-drop phishing element repository with customizable hundreds email templates, landing pages, and office templates to create attack phishing awareness campaigns.

Automated phishing campaign simulations with real production-safe payload, links to fake malicious websites identify employees who need additional phishing awareness training.

Automatically generated reports including every action taken by employees interacting with the campaign email phish.

Case Study

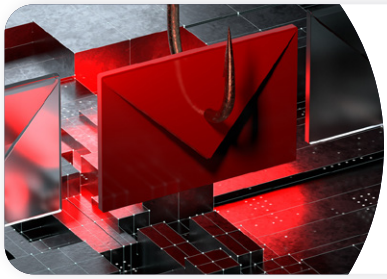
Persistent Systems

A digital engineering and enterprise modernization partner, with over 22,000 employees located across 18 countries.

Use Case: Breach Feasibility Assessment
Persistent checks breach feasibility through testing employees' phishing awareness. The Risk and Governance team are responsible for security awareness training, and with Cymulate they can continuously run phishing assessments to measure the success and return on investment of their program. Over time, the assessments have shown a significant decrease in the number of employees falling for phish as well as a significant increase in the number of people who report phish.

Read more

Additional Resources



Cymulate

Blog Post -The GoDaddy Phishing Awareness Test

Read more

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com