

Phishing Awareness

Solution Brief



Improving Phishing Awareness

Cymulate's Phishing Awareness vector enables you to evaluate employees' security awareness. It simulates phishing campaigns and detects easy clickers that can place your organization at risk. Increasing their awareness and vigilance will reduce your cyber exposure and help you to prevent data breaches, minimize malware-related downtime, and avoid incident costs.

Attack Vector Overview

Phishing attacks use social engineering to mimic trusted entities and increase the likelihood of the recipient to act, such as clicking on a malicious attachment or link and unwittingly enter sensitive information such as a password or bank account details. A successful phishing attack enables the adversary to infiltrate and compromise corporate and production environments.

That's why it is important to raise awareness among employees regarding cyber-attacks using social engineering methods since they are constantly evolving and becoming increasingly harder to detect.

Continuous Testing

The Cymulate Phishing Awareness vector simulates real-life phishing campaigns in which employees might click on and fall victim to within your organization. The continuous feedback given from the simulated tests will help focus on employees that require more education and monitoring than others.

How It Works

Campaign Setup – Campaigns are created in four simple steps or less. The platform provides all the resources required for the campaign:

- 01.** Create the target list of contacts that will participate in the phishing campaign.
- 02.** Select the email which will be sent during the campaign. Cymulate provides a wide selection of templates based on social platforms, system messages, attachments or links. You may also create custom campaigns.
- 03.** Optionally, select to add a login page for your campaign.
- 04.** Create a landing page that informs your employees of the campaign. In stealth mode, the landing page will only be visible at the end of the campaign.

Campaign Execution – Campaigns can be executed on-demand or scheduled. The phishing simulation utilizes ready-made out-of-the-box templates or custom-built templates assigned to a corresponding landing page with simulated malicious links.

Campaign Results – At the end of the simulation, a report is generated summarizing statistics and details of employees who have opened the email, and those who have clicked on the links or entered credentials, enabling organizations to assess their employees' readiness to identify phishing emails.

Key Features



Phishing emails are sent from Cymulate's cloud to a list of emails the customer chooses.



Events are tracked and updated by Cymulate throughout the campaign.



None of the emails contain real malicious content (ransomware, URLs, worms, etc.).



You have full control of email templates, attachments, and login pages, and can create your own using an easy-to-use composer.

Actionable Insights

Cymulate offers a suite of tools to create and launch a customized phishing campaign within the organization. Each step in the campaign is tracked (e.g. when an email is opened, and a link is clicked) to provide the security manager with the full picture of employees' security awareness levels and focus on employees that require more education and monitoring than others.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company—and every company—will be.

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

[Start Your Free Trial](#)