Trellix

DATA SHEET

Trellix® Phishing Simulator

Train employees to spot advanced phishing attacks

Key Benefits

- **Create realistic simulations**
  Develop and implement effective simulations based on environment, region, and industry.
- **Provide personalized training**
  Deliver relevant training tailored to employee needs and offer automated training tips.
- **Generate actionable insights**
  Score employee performance and issue reports for executives and managers.
- **Enhance the user experience**
  Easily build custom employee landing pages with an intuitive training experience.

The median time for users to fall for phishing emails is less than 60 seconds.[1] Organizations try to counter this threat with traditional security awareness training, but such training is often ineffective due to its generic nature, infrequency, and inability to adapt to the evolving threat landscape. Employees may lack knowledge about specific phishing attacks and find training irrelevant or annoying.

Solution Overview

To overcome these hurdles, Trellix Phishing Simulator uses advanced AI—including large language models (LLMs) and generative AI (GenAI)—to create realistic phishing simulations tailored to various employee roles and risk levels. A companion to Trellix Email Security – Cloud, it addresses the challenges of ineffective traditional training by offering personalized, immediate learning opportunities and actionable feedback. The platform also provides security administrators with robust analytics and reporting to track employee performance and measure the impact of training efforts.

Ultimately, Trellix Phishing Simulator aims to reduce the risk of successful phishing breaches by fostering a more security-aware workforce through sophisticated simulations and targeted education. Key differentiators include its AI-powered automation, focus on understanding human behavior, and comprehensive integration of simulation, training, and analytics.

Key Capabilities

Simplified security administration

Trellix Phishing Simulator reduces manual effort and simplifies the administrative experience through automation, AI-powered tools, and prebuilt templates, with well-crafted workflows and wizards that enable low-touch campaign creation and launch. It streamlines the creation, customization, and deployment of phishing simulations, as well as the reporting and analysis of results.

[1] Verizon 2024 Data Breach Investigations Report, May 1, 2024.

Social engineering

80%–95% of all attacks begin with a phish.[2]

The GenAI effect

4,151% increase in malicious emails since the initial launch of ChatGPT.[3]

Spiraling costs

$4.76M is the global average cost of a phishing breach.[4]

The human element

68% of breaches involve a nonmalicious human action.[5]

Extensive reporting and analytics

The simulator provides in-depth, actionable data and metrics through automated reporting, including customizable reports for executives and departments. By tracking phishing click rates and repeat offenders, this data enables organizations to understand their vulnerabilities, measure training effectiveness, and make data-driven security decisions.

Comprehensive training strategy

The training strategy is based on understanding different audience needs, delivering relevant content, and incorporating feedback mechanisms.

Advanced Phishing Training

Trellix Phishing Simulator moves beyond basic phishing awareness and provides a more advanced, personalized, and effective training experience designed to change employee behavior and strengthen an organization's security posture. It does so by integrating the following features:

- **Advanced Phishing Tests:** These include simulations for business email compromise, whaling, quishing (QR code phishing), spear phishing, collaboration platform attacks, and account compromise.
- **Customized Simulations:** The simulator utilizes LLMs and the Trellix Advanced Research Center to understand phishing training needs and simplify the creation of relevant simulations, including customized simulations based on customer-identified phishing attacks.
- **Personalized and Adaptive Training:** The simulator focuses on understanding how employees learn and the challenges they encounter to tailor training to fit their needs. It offers GenAI-driven prebuilt templates with relevant content to design role-based, rank-based, and risk-based attacks.
- **Interactive Remediation Training:** Following a failed simulation, employees receive immediate learning opportunities with interactive remediation training to reinforce messaging and measure comprehension.
- **Cue Training:** Appearing on landing pages, this helps individuals identify what they missed during the simulation and provides specific guidance on recognizing phishing indicators.

[2] Comcast Business Cybersecurity Threat Report, July 21, 2023.
[3] The last six months shows a 341% increase in malicious emails, Security, May 22, 2024.
[4] Cost of a Data Breach Report, IBM, July 30, 2024.
[5] Verizon 2024 Data Breach Investigations Report, May 1, 2024.