FÜRTINET

Extend Your Defense Perimeter With the Fortinet Security Awareness and Training Service

Protect Your Organization by Building a Cyber-aware Workforce

Executive Summary

The prevalence of ransomware continues to grow. According to the 2021 1H Global Threat Landscape report from FortiGuard Labs, ransomware grew 1070% between July 2020 and June 2021. While numerous high-profile incidents have grabbed international headlines, the real impact is felt by tens of thousands of organizations, from enterprises to small businesses and from federal agencies to local governments.

Employees have become high-target, high-value assets for cyber criminals—the human factor of cybersecurity cannot be forgotten. Most organizations today continue to face a skills shortage. Although awareness and training are critical, some organizations may struggle with defining, deploying, and managing an effective program.
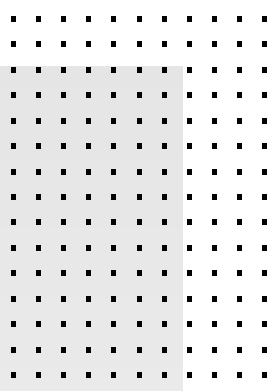
Protecting an organization from the growing volume of nation-state actors, cyber-criminal organizations, cyber terrorists, and lone hackers is increasingly difficult. Employees are now high-risk targets. An ongoing training engagement effort is needed to drive effective awareness and behavioral change.

Developed by top cybersecurity training experts, the Fortinet Security Awareness and Training Service provides a turnkey solution that brings timely and current awareness to today's cybersecurity threats and helps build a cyber-aware culture that is knowledgeable and empowered to help protect the organization.

Market-driven and Responsive

Because the threat landscape changes quickly and is becoming more malicious, security awareness and training programs need to evolve in step to ensure they are keeping pace with today's threats. The expanded attack surface driven by digital transformation, the work-from-anywhere hybrid workforce, and the global pandemic have placed employees as high targets for cyber criminals.

A security awareness and training solution must contribute to an overall security culture. To do that, applying a checkbox to a compliance approach to training will not foster a culture of awareness, nor will it be responsive to the ever-changing threat landscape.

"In fact, people directly affect security outcomes more than technology, policies, or processes. In the last 12 months, the 'human element' has been involved in 85% of breaches, and in nearly half of them (36%), phishing was the primary mode of attack. Accordingly, a security awareness program must be considered a critical element in delivering a defense-in-depth, or multilayered, enterprise security program."

– Gartner®, Market Guide for Security Awareness Computer-Based Training, Richard Addiscott, Claude Mandy, William Candrick, 26 July 2021

In the Fortinet Cybersecurity Insiders: 2021 APPLICATION SECURITY REPORT, 344 cybersecurity professionals were asked, "Which of the following barriers inhibit your organization from adequately defending against cyberthreats?" Forty-three percent chose low security awareness among employees as a key issue.

Elements of a robust security awareness training program include:

- Context- and content-relative training

- Engaging content that is not overwhelming to the learner

- Ability to reengage learners to ensure that information is reinforced

- Role-based training to deliver the right training to the right personas

- Bite-sized, digestible learning to hold the attention of the learner

- Measurement and analytics for testing and improvements

Deploying an effective awareness and training service, and fostering a culture of awareness of cyber threats help organizations meet compliance requirements and protect their technology investments, brand reputation, and financials.

The Fortinet Security Awareness and Training Service is a Software-as-a-Service (SaaS) offering that can be integrated with FortiPhish to provide a solution. Training delivered in multiple formats, including video, text, audio, imagery, and animation, appeals to different learning styles to ensure that training is understood and applied. Smaller, more easily consumed lengths such as micro-learning and nano-learning coupled with communications resources allow organizations to augment their training to help reinforce key lessons.

High-quality Training	Communication & Reinforcement Resources	Easy-to-use Administration & Management
Courses are designed for optimal learning, with introductory modules averaging approximately 8 minutes and reengagement micro modules averaging approximately 2 minutes. Role-based training for end-users, managers, and executives. Throughout the training, interactive quizzes and knowledge checks keep learners engaged and interested, allowing managers to assess knowledge levels.	Reinforce key teachings from the course modules with videos and other assets. Mix and match assets with different courses and use them to run targeted campaigns on key timely threats. - Nano videos - Posters - Screensavers - Banners - Tip sheets	The service provides several resources to help administrators deploy and manage the service, including: - Planning and deployment videos - Security Awareness Campaign Roll-out Guide - Quarterly Top Threat Signals Report for Admins (Powered by FortiGuard Labs) In addition, single sign-on, two-factor authentication, and LDAP integration ease user provisioning and management.
Active Monitoring & Reporting	**Custom Brand and Co-brand**	**Phishing Simulation**
The admin portal provides an up-to-date dashboard of user activity. Out-of-box reports available in pdf format: - Individual campaign report - Report weekly, monthly, or at campaign completion - Campaign report for executives - Summary of all campaigns - Overall completion rate - Progress of all campaigns	Partners can custom brand and offer a complete Security Awareness and Training Service to their customers. With multi-tenancy and role-based hierarchical support, partners can manage the entire experience from user provisioning to reporting for their customers and packaging and selling additional consulting services with the solution.	Integrate the Security Awareness and Training Service with FortiPhish and test awareness and vigilance across your users through real-world simulated phishing attacks while reinforcing proper practices at the point of click. Admins can create dynamic rules with training actions based on phishing simulation results to provide remediation training where needed.

The training educates the workforce about today's cyber threats, such as phishing, social engineering, and ransomware attacks, and how to protect against them. The awareness and training service is suitable for any workforce, from technical to nontechnical employees and contractors.

When completed, they will understand:

- The bad actors behind the attacks and what motivates them

- The methods used for attacks

- How to protect themselves and the information they have access to

- Key cybersecurity terms

Compliance and Protection

Fortinet training course materials address user-awareness training outlined in GDPR, PCI DSS, SOC 2, PIPEDA, CCPA, and ISO. Purpose-built to address the requirements for Security Awareness and Training as outlined in NIST 800-50 and NIST 800-16, Fortinet's focused and market-responsive training modules address the needs of today's organizations. Unlike other solutions that provide an overwhelming volume of content with no clear roadmap to deployment, the Fortinet Security Awareness and Training Service provides the right training that can be delivered at any time.

Extending Protection

The cybersecurity mesh architecture of the Fortinet Security Fabric, working together with Security Awareness and Training, gives organizations the ability to respond to threats anywhere and everywhere. The Fortinet Security Awareness and Training Service extends the protection provided by the Fortinet Security Fabric technologies to empower employees to become aware and engaged in the protection of the organization, thereby fortifying and extending the defense perimeter.

F⊞RTINET

www.fortinet.com