

Home / Solutions / Security Awareness Training:

Security Awareness Training: The Definitive Guide

Security awareness training helps organizations worldwide reduce risks related to cyber security, building vital threat resilience, and create a strong security-aware culture.

GET YOUR FREE DEFINITIVE GUIDE



OVERVIEW

HOW TO IMPLEMENT

FAQS

GET STARTED

What is Security Awareness Training?

Security awareness training is the practice of educating employees, contractors, partners, and other stakeholders on how they can safeguard sensitive information from cyber threats. Additionally, this process also informs training participants on how they can keep various systems, networks, online accounts, and other digital assets safe from hackers.

Why is Security Awareness Training Important?

Security awareness training helps organizations reduce risk related to the human side of cyber security and build a strong security-aware culture across all business units. To achieve this, CISOs and other security leaders construct risk-based awareness training programs that targets unsafe behaviors like clicking on a phishing email link or downloading a malicious attachment.

With a security awareness program in place, organizations strengthen information security and keep sensitive data like personally identifiable information (PII), intellectual property (IP), and accesses to confidential accounts, such as bank accounts. Awareness training can also ensure employees comply with industry or regional data privacy regulations, such as GDPR.

As organizations improve their security awareness maturity model, they often see a sharp decrease in cyber security-related costs, as well as a positive impact on their productivity, revenue generation, and brand reputation.

Does Security Awareness Training Work?

Because all cyber attacks are rooted in human behavior manipulation, security awareness training is the most effective tool to safeguard sensitive information from hackers. By giving employees the knowledge needed to detect and report common threats, organizations minimize the possibility of data breaches compromising their data.

That said, effective training is grounded in effective security awareness planning. An organization's security awareness professionals must establish clear cyber security goals, the metrics they'll use to measure performance, and actionable strategies to attain or exceed their aspirations. Boosting employees training participation and completion rates must also be considered.

According to the 2021 Gone Phishing Tournament results, one in every five end users click on suspicious phishing message links. Of those who clicked, three-quarters compromised their data. By implementing dynamic security awareness training options, organizations can avoid extended downtime, revenue loss, and other inevitable data breach consequences.

What Should a Security Awareness Program Include?

The best security awareness solutions combine a variety of different learning activities to deliver an engaging, informative, and fun (yes, work-based training can and **should** be fun!). Common training program components include (but are not limited to): online courses, quizzes, interactive modules like Serious Games, phishing simulations, and ongoing communication campaigns.

Security awareness program topics will vary based on an organization's goals and maturity level. However, it's important to cover a solid spectrum of security awareness fundamentals, such as phishing, social engineering, ransomware, malware, email security, and password best practices. A solid knowledge foundation will improve knowledge retention and [phishing simulation](#) performance.



Building a security-aware culture shouldn't be complicated (or pricey). Share cyber security best practices with your employees instantly with content kits from the Cyber Security Hub.

[ACCESS THE HUB](#)

FORTRA

**GONE
PHISHING
TOURNAMENT®**

Join the Gone Phishing Tournament

The biggest phishing benchmarking event

[REGISTER FOR THE EVENT](#)

[VIEW LAST YEAR'S RESULTS](#)



How Do You Implement Security Awareness Training?

The goal of security awareness training is about more than meeting compliance standards or ticking corporate mandates off a checklist. Organizations must strive to build vital cyber threat resilience, based on real-world intel, and, using that momentum, foster an internal culture that prioritizes continuous security awareness education.

To get the most out of your training program, you must implement each element carefully and connect it to you an overarching information security vision. For most security awareness teams, a successful implementation will resemble the following process:

Baseline phishing test

To accurately gauge initial end user security awareness, perform an initial baseline phishing simulation test. The results of this exercise will infuse the result security awareness report with the intel needed to craft a focused, risk-based training strategy.

Expert planning and executive support

Before launching any awareness training initiatives, it's vital to get executive support. This process can be made much easier by leveraging informed opinions based on your baseline security awareness report and industry expertise, such as in-house Terranova Security CISO resources.

Engaging, multilingual training content

To maximize your training program's ROI, your security awareness content must be engaging, informative, and, above all else, provide a fun learning experience for all participants. Be sure to offer training content in various modules, formats, and languages, which will enable you to benefit from increased participation, reduced risk, and changed behaviors.

Phishing training modules

Every organization needs a safe way to train employees about real-world threats and put their cyber security knowledge into practice. Because of this, phishing simulations are a key ingredient for security awareness success. They can also allow your organization to assess training content effectiveness and ensure you're always targeting the right behavior change.

Reinforcement tools

To support your awareness training initiatives with consistent, impactful messaging and learning opportunities, reinforcement and communication tools are essential. From newsletters and infographics to videos, web banners, and more, these assets help keep participation and engagement rates high while also emphasizing key cyber security topics.

Dynamic, real-time reporting

With the proper analytics and reporting infrastructure in place, making data-driven decisions via an in-depth security awareness report or dashboard is easy. By customizing a reporting experience to your organization's unique needs and goals, you'll be able to instantly see and synthesize course and simulation results, as well as optimize your program for the long term.

FAQs

- ▶ How Much Does Security Awareness Training Cost?
- ▶ How Long Does Security Awareness Training Take?
- ▶ How Often is Security Awareness Training?
- ▶ What is the Difference Between Security Awareness and Security Training?
- ▶ How Do You Promote Security Awareness?
- ▶ What are the Benefits of Security Awareness?
- ▶ Why is Security Important in the Workplace?
- ▶ Who is Responsible for Security Awareness Training?
- ▶ What is the Most Important Security Awareness Training?

Get Started

Get the highest-quality cyber security awareness training that provides an engaging, informative eLearning experience. Terranova Security offers customizable courses, quizzes, game-style activities, and communication tools that are perfect for any industry, organization size, and security awareness budget.

[SCHEDULE A DEMO](#)

FORTRA[™]



TRAINING

- Cyber Security Training for Employees
- Privacy Awareness
- Phishing Simulation
- Compliance & Governance
- Cyber Games

GET STARTED

- Platform Overview
- Free Demo
- Request a Quote
- Phishing Simulation Trial
- Guide to Security Awareness Training

COMPANY

- About Terranova Security
- Join Our Team
- Customer Support