Security Awareness Training

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Mitigate Your Human Error

Most cybersecurity breaches are the result of human error, which means employees tend to be the biggest threat to cybersecurity in any organization. As such, it's more important than ever to create a security-focused culture within your organization to maximize your chances of avoiding a breach. In order to have security-conscious employees, security awareness training must be provided by the organization. However, most organizations don't have the time, resources, or expertise to create and administer a comprehensive security awareness training program. With our Security Awareness Training service, you can have an effective training program that covers topics relevant to your organization's unique security policies, procedures, and processes with little to no time or resources required on your end.

Our Security Awareness Training can be offered in one of two forms: remotely (through electronic presentations or web-based live sessions), or on-site (through in-person training sessions in the comfort of your own office or at an off-site location of your choosing). By providing Security Awareness Training lead by a cybersecurity expert, your employees have the opportunity to ask questions, discuss the latest cybersecurity threats, and learn about the most up-to-date strategies to identify and avoid cybersecurity incidents before they occur.

Training That Actually Works

We know that effective security awareness training must be specific to your particular organization and employees, and will work with you to ensure our content is specifically tailored to your needs. You need the best training available to truly mitigate the threats presented by human error, and ensure your employees are completely knowledgeable on the types of attacks they could be facing. Let us work with you, and we'll be sure to develop a security awareness training that really works FOR YOU.

When we perform security awareness training, we focus on the major threats to your organization, including (but not limited to) phishing, vishing (voice phishing), smishing (SMS text message phishing), in-person social engineering, visitor policy training, proper reporting procedures for cybersecurity incidents, and much more. Additionally, our training can be as interactive as you want! We can provide quizzes, tests, or periodic question-and-answer sessions to assess employee knowledge on the presented materials. Attackers are getting smarter and smarter every day, so it's imperative that your employees are up to date on the latest threats "out there". Attacks can be avoided - and educating employees on how to recognize bad actors, even when they seem legitimate, is the most effective way to prevent these kinds of issues. If you already have a security awareness program in place, we can help to fill in any gaps you may have, or to improve upon the training you're already offering.

Security Awareness Training Includes:

- **Onsite or remote training from our experts**
- **Content specifically tailored to your organization**
- **Training on the biggest and latest threats**
- **Optional quizzes or tests to validate training efficacy**

Frequently Asked Questions

What's the difference between remote and onsite security awareness training?
For onsite security awareness training engagements, a TraceSecurity Information Security Analyst (ISA) will travel to your office(s) to preform in-person security awareness training sessions. For remote security awareness training, a TraceSecurity ISA will work with you and your team to curate the content of your security awareness training program and will provide it in your organization's preferred format (i.e. slide shows, electronic presentations, or as a web-based training session with the ISA).

Will there be a pass/fail test for employees at the end?
This is completely up to you and what is best for your program! TraceSecurity can build quizzes or tests to assess employee knowledge of the concepts presented during the training sessions.

How often should we provide security awareness training to our employees?
The NIST Cybersecurity Framework (PR.AT-1) calls for organizations to inform and train users on cybersecurity and information security-related duties and responsibilities. Depending upon your industry and its relevant regulations, you may be required to perform such trainings at least annually. In general, TraceSecurity recommends conducting quarterly security awareness training in order to reinforce security best practices as they constantly change and evolve.

Will the training include information on recent attacks to keep my employees up to date?
Because the training content is customized to your organization's specific needs at the time, the security awareness training content will include information on recent attacks and updated security regulations in the event they are relevant to the topics being covered.

tracesecurity
Compliance, simplified.