

TECHGUARD SERVICES

Security Awareness Training



TechGuard Services

Security Awareness Training

CONTENTS

2 What is Security Awareness Training?

3 Why Security Awareness Training?

4 How does TechGuard Approach Security Awareness Training?

5 What is the TechGuard Difference?

WHAT IS SECURITY AWARENESS TRAINING?

Security Awareness Training is a formal, educational process that trains employees to recognize and respond to sophisticated cyberattacks.

An effective security awareness program should be holistic in nature and based on best practices for adult learners. A comprehensive program will educate employees about cyber risk, their role in preventing a cyber incident, your corporate

policies and procedures for working with information technology (IT), how to adhere to any applicable data privacy/compliance regulations and how to spot phishing attacks.

Studies show that proper, relevant and on-going security awareness training is the best way to arm end users to become an organization's first line of cyber-defense.



WHY SECURITY AWARENESS TRAINING?

A well-educated workforce is a **critical** component that impacts the overall security posture of a company.



Ninety-five percent of cyberattacks are caused by **human error**

Whether your business is large or small, empowering your workforce to recognize and respond to sophisticated threats can be the difference between your employees being your weakest point of vulnerability or your greatest asset in cyber-defense.

The most effective way to lower your risk is to engage in routine, ongoing training for all employees - including key executives.

HOW DOES TECHGUARD APPROACH SECURITY AWARENESS TRAINING?

We make training your employees as easy as 1, 2, 3. Train, phish, track. Our role-based, high production quality content covers the needs of all users.

Real-world scenarios and simulation ensure adaptive learning experiences and maximum opportunity for retention of information. Our content is delivered in a way that supports best practices for driving awareness and actual behavior change for adult learners.

We include unlimited use of our phishing simulator to deliver customizable, sophisticated attacks to reinforce learning, remediate behaviors and prevent internal cyberattacks. We also include our world-class analytics suite to track your entire team's progress and course completion rate. In addition, our analytics measure the performance of your employees to identify susceptible users, compare performance over time and determine the direct ROI from your training.

With the ability to expose each employee's strengths and weaknesses, our approach provides insight to adjust curricula and increase employee training depth and intensity to address vulnerabilities and reduce cybersecurity risks. Ongoing supplemental materials deployed to you monthly aids the creation of a security-minded culture among your workforce.





WHAT IS THE TECHGUARD DIFFERENCE?

When it comes to changing the security behaviors of your employees, there is no one size fits all solution. We customize our approach to meet the needs of every one of our clients. We understand that a training platform is only as good as what is deployed and managed, therefore your deployment lead will assist you as much (or as little) as you need at no additional charge.

We ensure you get the most out of your investment. From your first contact with our sales team to the deployment of your training, we guarantee you will not only be satisfied, but you will see results. Over 9 million users have been impressed by our proven training content, unlimited phishing engagements, managed services and analytics suite. We pride ourselves in building and maintaining long-term relationships with our clients.

TechGuard has been dedicated to delivering high-end, professional cybersecurity solutions since 2000 - making us a trusted partner in both the government and private sectors.

TechGuard Security is an ISO 9001:2015-registered, certified SDB, DBE and Woman-Owned Business Enterprise. TechGuard Security was founded to address national cyber defense initiatives and US critical infrastructure security. We provide a comprehensive suite of cybersecurity solutions to help reduce your risk of cybersecurity-related incidents.