Stay Connected® Security Awareness Training

Powered by Webroot

Cybercriminals target end users.
Ongoing cybersecurity education and training
for end users is a must for businesses to stay secure.

Ongoing defense

Proven efficacy

Regulatory compliance

A fully featured phishing stimulator

Trackable, customizable campaigns

Campaign and contact management

Reporting Center

What is security awareness training?

Security awareness training is an education process that teaches employees about cybersecurity, IT best practices, and even regulatory compliance. A comprehensive security awareness program should train employees about a variety of IT, security, and other business-related topics. These may include how to avoid phishing and other types of social engineering cyberattacks, spot potential malware behaviors, report possible security threats, follow company IT policies and best practices, and adhere to any applicable data privacy and compliance regulations (GDPR, PCI DSS, HIPAA, etc.)

Studies have shown that quick, relevant, and continuous training throughout employee's tenure with a company are the best way to arm end users to become an organization's first line of cyber-defense.

Why businesses need security awareness training.

Although businesses may feel their employees wouldn't be fooled by something like a phishing scam, cybercriminals still use this attack method because it continues to be successful. In fact, the 2018 Verizon Data Breach Investigations report revealed that 93% of successful security breaches start with phishing.

With regular training that includes phishing simulations, courses on IT and security best practices, and data protection and compliance training, businesses can significantly reduce risk, decrease infections and related help desk costs, protect their reputation by experiencing fewer breaches, and secure their overall cybersecurity investment.

Our courses are specifically designed to help you address unwitting user error to enhance your Business security posture and meet compliance regulations.

Some course outlines:

Understanding Cybersecurity

Length: 10 min
Course Information:
Description: Best practices every end-user and employee should know to help reduce risk of malware infection and company breach.
Usage: Annual and new-hire security awareness training.
Topics:
Internet and email best practices, Keeping a clean machine, Password management, Phishing & social engineering
Signs of a cybersecurity breach
Interactive quiz (8 questions)

Understanding Phishing

Length: 8min
Course Information:
Description: Comprehensive phishing course with an overview of different types of phishing attacks, the risks phishing poses to users and companies, as well as best practices to avoid falling for a phishing attack. Includes real-world scenarios and examples.
Topics:
Categories of phishing, Risks associated with phishing, Best practices to stay safe, Full and abbreviated versions
Varying knowledge check questions

GDPR: General Data Protection Regulation

Length: 20 min
Course Information:
Description: Privacy awareness for the workforce of global organizations. Focuses on key concepts around privacy that are common across international jurisdictions including GDPR.
Topics:
What counts as personal data, Why we protect personal data, Data collection, handling, and processing, Updated for GDPR
10 knowledge check questions

PCI DSS

Length: 20 min
Course Information:
Description: This course will help you understand the basics of the PCI security standards and how to put the knowledge into practice while at work.
Topics:
What is PCI DSS and who needs to comply? Terminology, responsibilities and standards, Vulnerabilities and risks to payment card data, Security best practices when taking payments
Interactive quiz (8 questions)

Other available courses:

Social Media Awareness, Introduction to Ransomware, Freedom of Information Act, Email Security, Password Security, Remote Worker & Business Traveler