NINE THINGS
BUSINESSES NEED TO KNOW ABOUT
SECURITY AWARENESS TRAINING

Instances of cybercrime are exploding. Since the onset of the COVID-19 pandemic, the FBI has reported a **300 percent increase** in reported cybercrimes. Learn why security awareness training (SAT) is a must for every business today.

1 Most Cyberattacks Are Caused by Human Error

90% **of breaches are caused by employee mistakes according to IBM.**

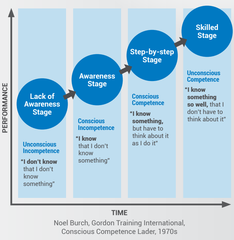
Your employees are your most significant liability in avoiding cyberattacks. Giving them the tools to protect your business is imperative.

2 Reduce Successful Phishing Attacks

Security awareness training programs can reduce phishing email click rates by 75 PERCENT, according to Infosec Institute.

3 Training Changes How You React to Threats

By changing the way your employees see threats, through regular ongoing training, they move from the "lack of awareness" stage and progress to the "skilled" stage – where they can recognize and avoid cyberattacks without thinking about it. Without ongoing training, according to USENIX employees forget SAT program best practices after six months on average, so constant training is critical.



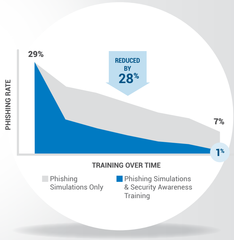
Noel Burch, Gordon Training International, Conscious Competence Ladder, 1970s

4 SAT is a Regulatory Requirement

Most major industry and federal regulations such as PCI-DSS, HIPAA, the FTC Safeguards Rule, etc. require security awareness training.

5 Combine Phishing Simulations & SAT

Research from InfoSec Institute shows the combination not only results in a lower phishing rate over time but leads to faster success – with lower rates happening sooner in the process.

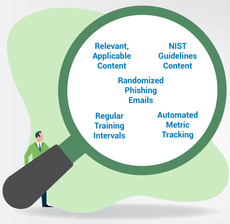


6 Use a Multi-Pronged Protection Strategy

High-quality security awareness training programs include multiple components, such as a wide range of topics, regular ongoing education, ongoing communication reinforcement, phishing simulations and is supported by the company culture and cybersecurity program.

7 Consider Outsourcing

In-house security awareness training programs can be costly, time-consuming and challenging. Outsourcing the management of your security awareness training to an MSP can be more effective and affordable, without placing a burden on your IT team.

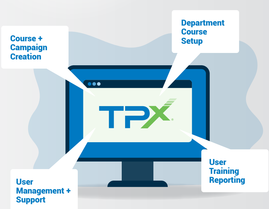


8 All Training is not Created Equally

Program quality is critical in rolling out an effective initiative at your company. Look for the components referenced in the graphic on the left as part of your security awareness training solution.

9 TPx is Your Trusted Partner

Running a business is challenging enough, you don't need to worry about data breaches and the impacts of cyberattacks. Our security awareness training looks at four key elements referenced in the graphic on the right.



TPx leverages InfoSec IQ platform and configures its implementation to be 100 percent in accordance with the National Institute of Standards and Technology's (NIST) 800-50 recommendations. InfoSec IQ was awarded Cyber Defense Magazine's 2021 InfoSec award as Security Awareness Training Market Leader and has received many other awards.

The bottom line is your organization's security is at stake, so it's crucial to choose an MSP with the technical know-how and resources to deliver consistent, regulatory-adhering security awareness training.

Learn More About Security Awareness Training in TPx's Guide

DOWNLOAD NOW

TPX
www.tpx.com