User Security
Managed Security Awareness Training

Empower your employees to be part of your security solution

TPx

Considering that 90% of successful breaches are caused by human error[1], it's no surprise that the right Security Awareness Training program can greatly enhance any organization's security. By implementing regular Security Awareness Training that includes phishing simulations and teaches employees about cybersecurity, IT best practices, and regulatory compliance, organizations can experience fewer breaches and significantly reduce their risk from cyberattacks.

[1] Gartner   [2] Infosec Institute   [3] IBM

Why should I implement Security Awareness Training?

Expand awareness to reduce threats Proactive training that helps your users learn how to recognize and avoid cyberattacks can significantly reduce the threat.

Minimize successful phishing attacks Phishing is the number one attack method used by cybercriminals. The right Security Awareness Training program can reduce phishing email click rates by 75%[2].

Reduce costs Cyberattacks are expensive. A recent study showed an average cost per data breach of $3.86 million[3]. Outsourcing your Security Awareness Training program can reduce this risk.

Why should I choose TPx?

Leading content TPx delivers best-in-class learning content that is effective and designed to engage the user so you can maximize your training program's success.

NIST recommended curriculum TPx's training curriculum follows the guidelines developed by the National Institute of Standards and Technology (NIST), which recommends specific topics to train on and strengthens overall security.

Fully managed TPx delivers a turn-key solution that leaves you free to run your business. Users receive training materials automatically, and you get weekly reports to track progress toward reaching your security goals.

How It Works

Phishing Simulations Enrolled learners will receive phishing simulation emails each month. Email templates and delivery times are randomized to improve effectiveness.

Scheduled Training Courses Each month, existing learners will automatically be enrolled and invited via email to participate in that month's class. Monthly classes are online and self-paced. Courses follow the national Institute of Standards and Technology (NIST) curriculum guidelines.

Automated Reporting Weekly reports are provided to help you track your progress toward meeting your security goals.

What's Included?

Onboarding and Support Services TPx's professional onboarding process allows you to quickly achieve value for your investment. TPx configures the learning platform, adds your learners, sets up all campaigns, schedules reports, and manages the entire implementation project. Once service is launched, our support team is available 24/7/365 to address your questions.

Phishing Simulations Three random phishing templates will be sent automatically to every enrolled learner every month. Delivery is randomized. Learner activity such as clicking a link or entering data in a form is tracked for status reporting, and if phished, learners are directed to a landing page with a brief point-in-time training message to reinforce correct behavior.

Training Courses Monthly training classes cover specific NIST recommended topics and are designed to be engaging and informative. Typical course length is less than 5 minutes to encourage participation, and learners receive email reminders to complete courses. Additional customer-specific courses can also be selected from TPx's predefined list to cover training on content such as regulatory compliance. TPx refreshes contact annually to enhance learning.

TPx managed Security Awareness Training is powered by INFOSEC IQ

Exceptional learner experience

Proven training methodology

Scheduled reports

Need to Know: Mobile Security

Completed!

🕐 4 minutes

About this course

Join Anthony and Ivana as they explore the ups and downs of phone security. What is encryption? What kind of damage could a stolen phone do? Learn how to take security with you wherever you go.

Certificate of completion

Congratulations on completing your course! A record of completion was sent to Infosec. You can download your course completion certificate here.
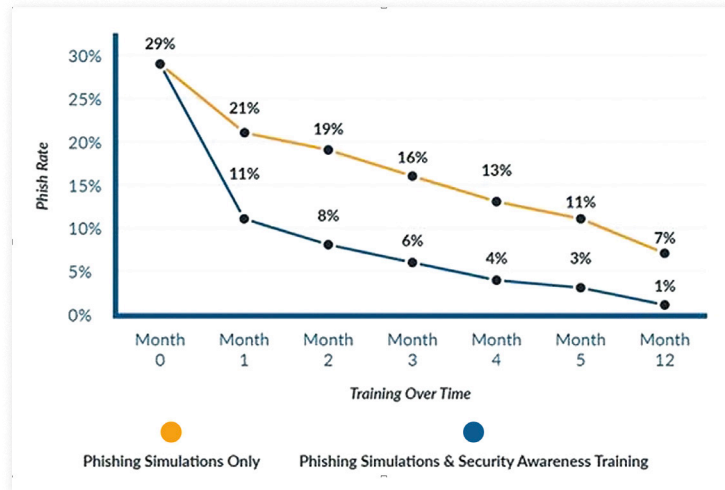
Course contents

LEARN

▶ Need to Know: Mobile Security *Complete*	03:32

ASSESS

✏ Need to Know: Mobile Security Assessment (2018) *Passed*	

INFOSEC IQ

Report Active Learners is available for download. Click the following link to view a csv file:

View Your Report

Note: Infosec IQ csv reports are available for download for up to 30 days. All data is preserved within Infosec IQ.

Sincerely,
The Infosec IQ Team

Training Over Time chart (Phish Rate vs Month):

Phishing Simulations Only (orange): Month 0: 29%, Month 1: 21%, Month 2: 19%, Month 3: 16%, Month 4: 13%, Month 5: 11%, Month 12: 7%

Phishing Simulations & Security Awareness Training (blue): Month 0: 29%, Month 1: 11%, Month 2: 8%, Month 3: 6%, Month 4: 4%, Month 5: 3%, Month 12: 1%

Security Awareness Training is an integral part of TPx's security services portfolio for protecting endpoints and users from ransomware and other cyberattacks. Bundling multiple services can increase your overall value and improve your organization's security. Below is our current portfolio of Endpoint and User Security and Management services.

Service Features	Description	Endpoint Management	Endpoint Security	User Security
Monitoring, Alerting, and Reporting	TPx provides automated monitoring and alerting and scheduled reports for device availability, health and performance, and inventory. Monitoring and alerting are per TPx's recommended practices. Alerts are received and actionable by either TPx or the customer, based on service level.	■		
System Patching	TPx provides managed, automated patching of operating systems and select third-party applications. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting are also included.	■		
Remote System Support	TPx provides 24/7 troubleshooting and repair of covered devices. Service includes proactive support based on TPx recommended practice and responsive support for customer requests or identified alerts. Remote Systems support features may be included in the fixed monthly charge or billable based on the chosen service level.	■		
Lifecycle Management	TPx provides proactive reporting and communication of end-of-life status on covered servers. Service includes hardware warranty expiration as well as manufacturer end-of-support status for operating systems and select applications. Post-warranty hardware support packages are available at additional cost.	■		
Managed NGAV	TPx provides managed Next-Generation Antivirus support. Service includes the use and management of the NGAV software as well as monitoring, alerting, and reporting on NGAV status. Virus remediation is available as a billable service.		■	
Endpoint Managed Detection and Response	TPx provides MDR services to identify and prevent advanced security attacks. The service includes the use and management of leading EDR software, SaaS platform hosting, SOC threat hunting, alert response, and event mitigation with an industry-leading 15-minute response time.		■	
DNS Protection	TPx provides DNS Protection for covered devices to combat Internet-born threats and enforce Internet usage policy. Service includes the use and management of the DNS Agent software, configuration of security policies, and monitoring and reporting on browsing activity and security events.		■	
Security Awareness Training	TPx provides automated Security Awareness Training campaigns. Service includes campaign setup, ongoing phishing simulations, and monthly training courses delivered automatically to enrolled users. Scheduled reporting of campaign status and activity is also included.			■
Inbox Detection and Response	TPx Inbox Detection and Response service allows users to easily report potential phishing emails. Reported emails are quarantined then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inbox and all instances of malicious emails are automatically removed from all other users' mailboxes.			■

All service features are available in pre-packaged solution bundles to meet a variety of use cases. Endpoint Security and User Security service features are also available as stand-alone offerings.