Managed Proofpoint Security Awareness Training

Enterprise Edition

Managed Proofpoint Security Awareness Training (mPSAT) offloads the challenge of designing, running and reporting on an assessment and training program, enabling you to focus on your primary responsibilities. Having a dedicated resource specifically focused on designing and implementing your Security Awareness Training program provides you with continuous activity and focus on cybersecurity. mPSAT uses a researched, proven educational approach that engages your end users throughout the year. With that expertise and best practice knowledge, you can rest assured you will have best-in-class programs, and you'll gain additional value as the mPSAT team uses those results to suggest security improvements.

Our goal is to make Security Awareness Training easy for you and effective for your organization. We achieve this via a disciplined, personal approach, outlined in the steps below.

PLANNING

As a mPSAT client, your security awareness program will be managed by our expert mPSAT team. At the onset of your program, you will meet weekly with your assigned mPSAT team member (a Managed PSAT administrator, or MPA). This person will serve as your personal representative and be your primary point of contact throughout your program. Your MPA will work with you to design and implement a specific security awareness program that aligns with your organization's culture and goals.

DISCOVERY

You and your MPA will meet to discuss your current cybersecurity threats and concerns, and provide details about what you liked and disliked about previous security awareness activity. This includes training programs, penetration tests, and phishing simulations. We will also discuss historical results, organizational feedback and challenges.

You will share your current and future security awareness goals, and we will use those to establish guidelines for developing a customized program. The outcome of these initial discussions will be a clearly defined set of objectives for the program. We will also discuss initial communication about the program to your users and initial plans to engage key stakeholders, such as Human Resources and IT.

Your MPA will provide you with a set of guides, tools and templates that will be used throughout the program:

- Best practices guide
- Best practices calendar
- Comprehensive reporting document
- Sample simulated phishing templates
- Notification templates for training assignments
- IT and help desk communication templates
- Whitelisting documents

COMMUNICATIONS

We strongly recommend a well-thought-out communication plan for all key stakeholders. It is also important to ensure you have a responsive plan in place to provide your key stakeholders with clarification regarding program goals. This plan should include a point of contact who can address any questions or concerns.

We can help you notify your internal IT and help desk teams when campaigns are scheduled. This will provide the help desk with detailed information on the campaigns and groups involved so they can prepare for questions and requests from users.

We can also provide sample communications to help you communicate with your users about your security awareness program. This helps you promote ownership and acceptance of an important learning experience.

TECHNICAL READINESS

Proofpoint will provide you with documents to whitelist IP addresses for your email servers and to conduct spam filter testing. In addition, exceptions may need to be created in firewall or security appliances to allow traffic to our servers.

USER MANAGEMENT

You and your MPA will discuss the user base for the program. If it is determined that End User Sync is not an option, we will request a user list with data elements such as email, first name, last name, business unit, group, location and other.

As we discuss users and associated properties, it is important to correlate this information to your reporting requirements. We will also discuss how your user information will be updated over time to accommodate new hires, individuals no longer employed, and updates on criteria such as manager and department.

SECURITY AWARENESS PROGRAM COMPONENTS

Your security awareness program will be comprised of knowledge assessments, simulated attacks, training, awareness materials, and reinforcement tools, depending on your licensed products.

PRODUCT	DESCRIPTION
CyberStrength®	• Evaluate end-user awareness with a library of 185+ questions that cover a variety of topics • Utilize as pre- and post-assessment to identify risk within the organization, identify the members at risk, and measure effectiveness of training • 11 Predefined (10-15 questions) and 3 Broad (55, 33, or 22 questions) assessments available, as well as fully customizable options • Auto-Enrollment feature automatically assigns training to employees based on results
ThreatSim®	• Simulated phishing attacks embedded with Teachable Moments • Phishing templates available in 30+ languages and 13 categories • Templates continuously updated, based on customer requests, seasonal topics, and phishing events in the wild • 3 Key Types: File Attachment, Embedded Links, and Data Entry • Teachable Moments, the “just-in-time” teaching messages to educate end users who fall for a phish • Fully customizable options: Teachable Moments, Domains, Phishing Templates • Auto-Enrollment feature to assign training to any employee who falls for a phish • Random or standard scheduling options • ThreatSim USB simulations • ThreatSim Smishing simulations
PhishAlarm®	• Email client add-in allowing employees to report phishing emails with a single click of a mouse • Positive reinforcement of reported phishing emails in the form of pop-up messages or emails
Interactive Training Modules	• Training modules with brief lessons on security and compliance topics and game- and interactive-based elements • Reinforcement of material with practice multiple-choice and true/false tests • Two formats: Standard (10-15 minutes) and Mini (5-7 minutes) • Customizable with “Training Jackets” before and after each module
Security Awareness Materials and Videos	• Educational Materials to reinforce your computer-based training modules, including images, posters, and articles • Awareness Video Campaigns: brief high-level videos, with the option to add wrapper content of tailored information such as company policy at the start and close of each video

IMPLEMENT

Proofpoint simulated attacks will establish a realistic baseline of your organization’s vulnerability against various attack vectors. Because it is just as important to learn how susceptible your users are to attack, your MPA will deliver simulated attack campaigns in parallel with the CyberStrength assessment.

Simulated Phishing Assessment

Your MPA will be the “hands-on” administrator of the simulated phishing assessment tool within the Security Education Platform.

Your MPA will work with you to choose the phishing templates and Teachable Moments for each campaign. We will create, schedule and implement each campaign according to the planned requirements over your license term. We will also discuss the scope and users to be phished with you prior to each campaign.

A blind simulated phishing attack will be sent to your users at the beginning of the license term to provide initial baseline data. Following this, we will conduct simulated phishing attacks—embedded with Teachable Moments—throughout your license term. These Teachable Moments will provide immediate and effective feedback for anyone who fell for a phishing attack.

ThreatSim USB Assessment

Your MPA will create the ThreatSim USB campaign, configuring the bait file names to be loaded on the devices and selecting/customizing the Teachable Moment. They will then deliver the zip file containing the needed files and send them to you via Secure Share. You will procure the USB devices and load the files on the devices using a supplied spreadsheet to organize their deployment. Once the devices have been deployed, your MPA will deliver activity reports on an agreed schedule.

Training Needs Assessment

CyberStrength will provide you with a Training Needs Assessment (TNA) of employee knowledge within your organization and measure the effectiveness of training. We recommend conducting a CyberStrength assessment at the beginning of the license term with broad topics, and additional assessments based on the results of the first TNA. This helps to target previously identified risk areas.

Security Awareness Training

Proofpoint will assign training modules to your users who succumbed to phishing attacks. The assignment can include the Anti-Phishing Training Suite training modules, based on your licensed products.

We will also create assignments for every user, regardless of whether they fell for a simulated attack, so that each user can benefit from training.

As the training completion deadline approaches, we remind users of the due date of their training assignment. We also gauge user proficiency to plan the next assessments and training module assignments.

Your MPA will assign training modules on security and compliance topics, including auto-enrollment assignments. Assignments will consist of multiple modules, based on identified risk areas.

Please note: If you are using your own Learning Management System (“LMS”) for some or all of the training assignments, the LMS user management, LMS assignments and LMS reporting will be managed by you, not your MPA. Training Jackets and auto-enrollment are not available for LMS-based modules.

REINFORCE

PhishAlarm provides positive reinforcement to your users who report potential phish. The PhishAlarm email add-in will alert security and incident response teams to suspected phishing emails with the click of a button. This reduces the duration and impact of active phishing attacks while reinforcing the behaviors learned in your security awareness training program.

The reporting of phish is an important trending metric for tracking end-user behavior as well as security awareness and engagement.

Security Awareness Materials are designed for reinforcement of the key principles taught within our training modules. This allows you to emphasize best practices and improve knowledge retention. Proofpoint will map Security Awareness material to weak areas within the TNA.

ANALYZE

Together, the results from the CyberStrength assessment, simulated attack campaigns, training, and PhishAlarm reporting provide a holistic view of user knowledge levels and susceptibility to attack. With this data, you can identify your greatest risk areas and create a plan for strengthening workforce knowledge.

Your MPA will review the results after each assessment and training assignment. The results will be compared to historical performance to derive improvement trends and previous or new areas of concern. The properties included in the reports (which were defined in your initial planning session) will be reviewed for correlation of risk to department, geography, role or manager. This analysis will be discussed in the ongoing planning and strategy sessions and used to determine next steps. Your MPA will provide you with industry and template benchmarking analysis, if available.

VAP FOCUS

For mPSAT customers with Proofpoint Targeted Attack Protection (TAP)

mPSAT will:

- Analyze a quarterly VAP (Very Attacked Persons) Report from the TAP Dashboard
- Identify those most targeted within your organization
- Segment your VAPs based on the targeted threat data
- Create quarterly VAP training and awareness activities based on the identified threats
- Analyze VAPs and their performance in the Security Awareness Program over time

REPORT

Reports will be delivered for each activity as the program progresses. These reports are available to your project lead in the platform at any time. Select reports can be scheduled to run periodically and be sent to you in a secure manner via email.

The following is a list of available reports and their delivery frequency:

TRAINING MODULE REPORTING	FILE TYPE	FREQUENCY
Assignment User Details	Excel, Word, CSV	Weekly during assignment
Assignment Comparison Report	Excel, Word, CSV	Upon Request
Most Missed Report	Excel, Word, CSV	Upon Request
Module Performance Report	Excel, Word, CSV	Upon Request
Module Completion Summary	Excel, Word, CSV	Upon Request
User Report Cards	Excel, Word	Upon Request

CYBERSTRENGTH REPORTING	FILE TYPE	FREQUENCY
Assessment Report	Excel, Word	Daily during assessment; final report 2 days after end date of assessment
Risk Report	Excel, Word	Daily during assessment; final report 2 days after end date of assessment

THREATSIM CAMPAIGN REPORTING	FILE TYPE	FREQUENCY
Recent Campaign Data	Excel, Word, PDF	Daily during assessment; final report 2 days after end date of assessment
All Campaigns	Excel, Word, PDF	Upon Request
Campaign History	Excel, Word, PDF	Upon Request
Campaign Overview	Excel, Word, PDF	Upon Request
Endpoints	Excel, Word, PDF	Upon Request
Geographical Distribution	Excel, Word, PDF	Upon Request
Users	Excel, Word, PDF	Upon Request

SMISH REPORTING	FILE TYPE	FREQUENCY
Smishing Campaign Report	Excel	Daily during assessment; final report 2 days after end date of assessment

USB REPORTING	FILE TYPE	FREQUENCY
USB Campaign Data	Excel	Daily during assessment; final report 2 days after end date of assessment

PHISHALARM REPORTING	FILE TYPE	FREQUENCY
PhishAlarm Reported Emails	Excel, PDF	Upon Request or Scheduled Cadence

SECURITY AWARENESS PROGRAM CALENDAR

This calendar outlines our suggested plan for implementing our Continuous Training Methodology. This schedule will be modified based upon your licensed products, term, and the specific needs and goals of your program.

QUARTER 1	MONTH 1	MONTH 2	MONTH 3
CYB	Baseline CyberStrength 1 Initial Communication		
Phishing	Blind Phish 1	Campaign 1 with Auto Enroll	
Training		Auto Enroll Training	Non-Clicker
SAM		Selected Topic	

QUARTER 2	MONTH 4	MONTH 5	MONTH 6
CYB			
Phishing	Campaign 2	Campaign 3	Campaign 4
Training		Supplemental Training*	Non-Clicker
SAM		New Topic	

QUARTER 3	MONTH 7	MONTH 8	MONTH 9
Phishing		Campaign 5	Campaign 6
Training	Non-Clicker		Supplemental Training*
SAM		New Topic	

QUARTER 4	MONTH 10	MONTH 11	MONTH 12
CYB			Repeat CyberStrength 1
Phishing	Campaign 7	Campaign 8	

QUARTER 1	MONTH 1	MONTH 2	MONTH 3
Training		Non-Clicker	Supplemental Training*
SAM		New Topic	
Smishing	Smish Campaign 1		

* Supplemental training topics are determined from CyberStrength results. ThreatSim USB drives can de dropped at any time during the license term.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.