proofpoint.

SOLUTION BRIEF

Managed Proofpoint Security Awareness Training—Enterprise

Security awareness training for customers with more than 2,500 users

Focus on your primary business activity and let us handle the design, running and reporting for your security awareness training programmes. Managed Proofpoint Security Awareness Training—Enterprise is intended for customers with more than 2,500 users. The service provides you with a dedicated resource who will take care of your programme with continuous activity and an expert focus on cybersecurity.

We make security awareness training easy and effective. We use a proven disciplined, personal approach that engages your end users throughout the year. With our expertise and knowledge of best practices, you will have best-in-class programmes.

Planning

Our Managed Services team will manage your security awareness programme. From the onset, you will meet weekly with your assigned team member. This person will serve as your personal representative and your primary point of contact. Together you will work to design and implement a specific programme that aligns with your culture and goals.

Discovery

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

You will share your current and future security awareness goals. We will use those goals to establish guidelines for developing a customised programme. These initial discussions will lead to a clearly defined set of objectives for the programme.

Then we will discuss initial plans to engage key stakeholders, such as Human Resources and IT. Your contact will provide you with a set of guides, tools and templates that will be used throughout the programme. These include:

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

Communications

We strongly recommend a well-thought-out communications plan to keep all key stakeholders in the loop. The plan should set expectations about a programme's goals. It should also include a point of contact who can address any of your questions or concerns. We can help notify your internal IT and help desk teams when campaigns are scheduled. This will provide them with detailed information about the campaigns and any groups involved so they can field questions and requests from users. We can also provide sample communications to help you keep users informed about your security awareness programme. Effective communication can promote ownership and acceptance of important learning experiences.

Technical Readiness

We will provide you with documents to safelist 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 contact will discuss the user base for the programme. You'll need to determine whether the End-User Sync tool is an option. If it is not, then we will request a user list with data elements such as email, first name, last name, business unit, group, location and other properties. As we discuss users and associated properties, we will correlate this information with your reporting requirements. We will also discuss how your user information will be updated over time to accommodate new hires, people no longer employed and updates on criteria such as manager and department.

Security Awareness Programme Components

Your security awareness programme may include the following (depending on your licenced products):

- Knowledge assessments
- Simulated attacks
- Training
- Awareness materials
- Reinforcement tools

Learn more about the products in Proofpoint Security Awareness Training here: proofpoint.com/us/product-family/security-awareness-training.

Implementation

Proofpoint simulated attacks will establish a realistic baseline of your organisation's vulnerability against various attack vectors. Because you need to know how susceptible your users are to attack, your contact will deliver Phishing Simulation attack campaigns in parallel with Knowledge Assessments.

Phishing Simulation assessments

Your contact will be the hands-on administrator of the simulated phishing assessment tool. We 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 licence term. Prior to each campaign, will also discuss the scope of the campaign and the users to be phished. A blind simulated phishing attack will be sent to your users at the beginning of the licence term to provide initial baseline data. Following this, we will conduct simulated phishing attacks—embedded with Teachable Moments—throughout your licence term. These Teachable Moments will provide immediate and effective feedback for anyone who falls for a phishing attack.

Phishing Simulation USB assessments

Your contact will create the Phishing Simulation USB campaign. We will configure the bait file names to be loaded on the devices and select/customise the Teachable Moment. We 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 organise their deployment. Once the devices have been deployed, your contact will deliver activity reports on an agreed schedule.

Knowledge assessments

Knowledge assessments provide an overview of your employees' knowledge and measure the effectiveness of training. We recommend conducting a knowledge assessment at the beginning of the licence term with broad topics. Additional assessments can be based on the results of the first assessment. This helps to target previously identified risk areas.

Training modules

Proofpoint will assign training modules to your users who succumbed to phishing attacks. These assignments can include training modules based on your licenced products. We will also create assignments for every user, regardless of whether they fell for a simulated attack, so everyone can benefit from training.

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

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

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 contact. Training Jackets and auto-enrollment are not available for LMS-based modules.

Reinforcement

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 behaviours learned in your security awareness training programme. The reporting of phish is an important trending metric for tracking end-user behaviour 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 emphasise best practices and improve knowledge retention. Proofpoint will map security awareness material to weak areas within the knowledge assessment.

Analysis

Together, the results from the knowledge assessment, Phishing Simulation attack campaigns and PhishAlarm email 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 contact 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 contact will provide you with industry and template benchmarking analysis, if available.

VAP Focus

For customers with Proofpoint Targeted Attack Protection (TAP) your contact will:

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

Report

Reports will be delivered for each activity as the programme 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 securely via email.

Security Awareness Programme Calendar

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

QUARTER 1	MONTH 1	MONTH 2	MONTH 3
CYB	Baseline Knowledge Assessment 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 Knowledge Assessment 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 Knowledge Assessment results. Phishing Simulation USB drives can de dropped at any time during the licence term.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations 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**.