proofpoint.

SOLUTION BRIEF

Managed Proofpoint Security Awareness Training—Commercial

Leverage our industry-leading expertise when setting up and managing your security awareness program

Products

- Proofpoint Security Awareness Training

Key Benefits

- Dedicated experts who will reduce user risk faster by implementing a first-class security awareness program based on best practices
- Comprehensive set of training resources, including reinforcement tools to improve user behaviour and organisational culture
- Detailed and insightful reports that provide a holistic view of your organisation's security awareness program and user readiness

Focus on your primary business activity and let us do the heavy lifting with your security awareness program. Managed Proofpoint Security Awareness Training—Commercial handles the challenge of designing, running and reporting on programs for commercial customers with up to 2,500 users. We'll provide you with dedicated experts who, with a measured, personal approach, will help you set up and run your security awareness training. Together, we'll develop a program for you that is both easy and effective and is sure to engage your end users throughout the year.

Planning

Our expert team will manage your security awareness program. Our dedicated resources will focus on implementing a predefined program based on proven best practices. From the onset of your program, you will meet monthly with your assigned team members. These experts will serve as your personal representatives and primary points of contact.

Launch

We will establish initial plans to engage key stakeholders, such as human resources, IT and security as well as how best to introduce the program to your users. Your contact will provide you with a set of guides, tools and templates for use throughout the program. These resources may include:

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

Communication

Communication is important for any endeavour. We highly recommend setting up a comprehensive communication plan to keep all key stakeholders in the loop. The plan should set expectations about program goals. It should also include a point of contact from your organisation who can address any questions or concerns. We can help notify your internal IT and help desk teams when campaigns are scheduled. This will provide the help desk 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 program, because 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. Exceptions may also 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 program. You'll need to determine whether the End-User Sync tool to pull users directly to our platform from your organisation's Active Directory (AD) or Azure 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 (up to three more). We will correlate your reporting requirements with relevant information gleaned from our discussions. 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 Components

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

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

Implementation

Proofpoint assessments will establish a realistic baseline of your organisation's vulnerability against various attack vectors.

Phishing simulations

A Proofpoint expert will be the hands-on administrator of our phishing-simulation tool. We will create, schedule and implement each campaign according to the plan over your licence term. Before we start, we will discuss with you the scope of the campaign and the users to be phished. A blind simulated phishing attack—which takes users who fall for it to a 404 error page—will be sent to your users at the beginning of the licence term to provide initial baseline data. Throughout your licence term, we will then conduct simulated phishing attacks embedded with Teachable Moments for immediate feedback. These Teachable Moments are landing pages to which any user who falls for phishing attacks is sent.

Knowledge assessment

Knowledge assessments provide an overview of your employees' knowledge and measure an effectiveness of training. We recommend conducting the assessment with broad topics at the beginning of the licence term. Additional knowledge assessments may be sent in lieu of scheduled training exercises.

Security awareness training

Proofpoint will assign training modules to any user who succumbs to phishing attacks in the scheduled Phishing Auto-enroll training exercises. We will also suggest training modules and create assignments for every user, whether or not they fall for a simulated attack. This balanced approach not only identifies and addresses specific areas of concern, it also strengthens your defences as whole by facilitating learning among all of your users. We'll remind users of the due date as the training completion deadline approaches. We'll also gauge user proficiency to plan the next assessments and training module assignments.

Note: If you are using your own learning management system (LMS) for some or all of the training assignments, then you—not your contact—will manage LMS user management, LMS assignments and LMS reporting. Training Jackets and auto-enrollment are not available for LMS-based modules.

Program Calendar

QUARTER 1	QUARTER 2	QUARTER 3	QUARTER 4
Kick-off Meeting	Phishing Exercise	Meeting—Customer Business Review	Phishing Exercise
Platform Management—Users	Training Exercise—Phishing AutoEnroll	Phishing Exercise	Training Exercise—Phishing Auto-enroll
Phishing Exercise	Training Exercise or Knowledge Assessment	Training Exercise or Knowledge Assessment	Training Exercise or Knowledge Assessment
Platform Management—Notifications			Meeting—End-of-Year Review

Reinforce

Security awareness materials are available in a wide variety of formats, including infographics, articles and videos. You can download and customise any of them. They are designed to reinforce key principles taught in our training modules. They also emphasise best practices and improve knowledge retention. Proofpoint can recommend security awareness materials based on weak areas identified in the knowledge assessment.

The PhishAlarm email add-in provides positive reinforcement to your users who report potential phish. It 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 program. The reporting of phish (reporting rate) is an important trending metric for tracking end-user behaviour as well as security awareness and engagement.

Analyse

The results from the knowledge assessment, simulated phishing campaigns, training 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 with historical performance data to derive improvement trends and 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. Your contact will provide you with industry and template benchmarking analysis, if available.

Report

Reports will be delivered for each activity as the program progresses. These reports are available to your project lead at any time. Select reports can be scheduled to run periodically. They can also be sent to you securely through email.

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**.