Managed Services for Proofpoint Security Awareness Training

Enterprise Edition

Managed Services for Proofpoint Security Awareness Training offloads the challenge of designing, running and reporting on a security awareness training programme, enabling you to focus on your primary responsibilities. Having a dedicated resource specifically focused on designing and implementing your programme provides you with continuous activity and focus on cybersecurity. The solution 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 programmes, and you’ll gain additional value as the Managed Services team uses those results to suggest security improvements.

Our goal is to make security awareness training easy for you and effective for your organisation. We achieve this via a disciplined, personal approach, outlined in the steps below.

**PLANNING**

As a client, your security awareness programme will be managed by our expert team. At the onset of your programme, you will meet weekly with your assigned team member. This person will serve as your personal representative and be your primary point of contact throughout your programme. Your Managed Services contact will work with you to design and implement a specific security awareness programme that aligns with your organisation’s culture and goals.

**DISCOVERY**

You and your contact 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 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, and we will use those to establish guidelines for developing a customised programme. The outcome of these initial discussions will be a clearly defined set of objectives for the programme. We will also discuss initial communication about the programme to your users and 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:

- 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 programme 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 programme. 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 contact will discuss the user base for the programme. 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 PROGRAMME COMPONENTS
Your security awareness programme will be comprised of knowledge assessments, simulated attacks, training, awareness materials and reinforcement tools, depending on your licensed products.


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

ThreatSim Phishing Assessment
Your contact will be the “hands-on” administrator of the simulated phishing assessment tool within the Security Education Platform. Your contact 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 licence term. These Teachable Moments will provide immediate and effective feedback for anyone who fell for a phishing attack.

ThreatSim USB Assessment
Your contact will create the ThreatSim USB campaign, configuring the bait file names to be loaded on the devices and selecting/customising 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 organise their deployment. Once the devices have been deployed, your contact will deliver activity reports on an agreed schedule.

CyberStrength Knowledge Assessment
CyberStrength will provide you with an employee knowledge assessment within your organisation and measure the effectiveness of training. We recommend conducting a CyberStrength assessment at the beginning of the licence term with broad topics, and additional assessments 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. The assignment can include 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 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.

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 contact. 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 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.

ANALYSE

Together, the results from the CyberStrength assessment, ThreatSim simulated attack 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 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 licensed products, term, and the specific needs and goals of your programme.

<table>
<thead>
<tr>
<th>QUARTER 1</th>
<th>MONTH 1</th>
<th>MONTH 2</th>
<th>MONTH 3</th>
</tr>
</thead>
</table>
| CYB       | Baseline CyberStrength 1  
Initial Communication |
| Phishing  | Blind Phish 1  
Campaign 1 with Auto Enroll |
| Training  | Auto Enroll Training  
Non-Clicker |
| SAM       | Selected Topic |

<table>
<thead>
<tr>
<th>QUARTER 2</th>
<th>MONTH 4</th>
<th>MONTH 5</th>
<th>MONTH 6</th>
</tr>
</thead>
</table>
| CYB       | Campaign 2  
Campagne 3  
Campaign 4 |
| Phishing  | Supplemental Training*  
Non-Clicker |
| Training  | New Topic |
| SAM       | |

<table>
<thead>
<tr>
<th>QUARTER 3</th>
<th>MONTH 7</th>
<th>MONTH 8</th>
<th>MONTH 9</th>
</tr>
</thead>
</table>
| Phishing  | Campaign 5  
Campaign 6  
Supplemental Training* |
| Training  | Non-Clicker  
New Topic |
| SAM       | |

<table>
<thead>
<tr>
<th>QUARTER 4</th>
<th>MONTH 10</th>
<th>MONTH 11</th>
<th>MONTH 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB</td>
<td>Repeat CyberStrength 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Phishing  | Campaign 7  
Campaign 8 |

<table>
<thead>
<tr>
<th>QUARTER 1</th>
<th>MONTH 1</th>
<th>MONTH 2</th>
<th>MONTH 3</th>
</tr>
</thead>
</table>
| Training  | Non-Clicker  
Supplemental Training* |
| SAM       | New Topic |
| Smishing  | Smish Campaign 1 |

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

LEARN MORE

For more information, visit proofpoint.com.