Proofpoint Managed Security Awareness—Enterprise

Obtenga un recurso experto dedicado que se centrará en sus objetivos de ciberseguridad

Céntrese en sus actividades empresariales principales y deje que nosotros nos ocupemos de la elaboración y gestión de sus programas de formación y concienciación en materia de seguridad, así como de la generación de informes. Proofpoint Managed Security Awareness—Enterprise le proporciona un recurso dedicado que se ocupará de su programa, para una actividad continua y una atención centrada en la ciberseguridad.

Nuestros programas para concienciar en materia de seguridad son fáciles y eficaces. Utilizamos un enfoque personalizado, riguroso y de eficacia probada, que involucra a los usuarios durante todo el año. Nuestra experiencia y conocimiento de las mejores prácticas nos permiten elaborar los mejores programas.

Planificación

Nuestro equipo se encargará de gestionar su programa de concienciación en materia de seguridad. Al inicio del programa, se reunirá semanalmente con el miembro del equipo asignado. Esta persona actuará como representante personal y será su interlocutor principal. Trabajaran juntos para diseñar e implementar un programa específico que se adecúe a la cultura y objetivos de su organización.

Incorporación

El especialista en incorporación que se le haya asignado se reunirá con usted y, a partir de la información recopilada en nuestro cuestionario de incorporación, le ayudará con la implantación y configuración de:

- Lista segura
- Sincronización de usuarios
- PhishAlarm
- Inicio de sesión único

Descubrimiento

Usted y su contacto se reunirán para analizar sus inquietudes relacionadas con la seguridad y las amenazas que le afectan actualmente, y podrá informarle de los aspectos que le gustaron y que le disgustaron de la actividad de concienciación en materia de seguridad anterior. Esto incluye programas de formación, pruebas de penetración y simulaciones de phishing. También analizaremos los resultados históricos, la información y los desafíos de la organización.

Tendrá la oportunidad de compartir con nosotros sus objetivos de concienciación en materia de seguridad actuales y futuros, y utilizaremos esos datos para establecer pautas que permitan desarrollar un programa personalizado. El resultado de esas conversaciones iniciales será un conjunto claramente definido de objetivos para el programa.

A continuación abordaremos los planes iniciales para involucrar a los principales implicados, como los departamentos de Recursos Humanos y TI. Su contacto le ofrecerá un conjunto de guías, herramientas y plantillas que se utilizarán durante todo el programa. Concretamente:

- Guía de mejores prácticas
- Calendario de mejores prácticas
- Plantillas de simulación de ataques de phishing
- Plantillas de notificación para asignaciones de formación
- Plantilla de comunicación con el servicio de soporte técnico y el departamento de TI

Y puesto que es tan importante conocer la susceptibilidad de los usuarios a ataques, su contacto facilitará campañas de ataques simulados junto con evaluaciones de conocimientos.

Comunicaciones

Recomendamos encarecidamente un plan de comunicación bien estructurado para todos los principales implicados. Este plan debe definir las expectativas en cuanto a los objetivos del programa. También debería incluir un interlocutor que pueda resolver todas sus preguntas o inquietudes. El equipo de Proofpoint puede ayudarle a informar al equipo de TI y de soporte técnico del calendario de campañas de concienciación. Esta notificación les proporcionará información detallada sobre las campañas y los grupos de usuarios involucrados, para que pueda responder a las preguntas y consultas de los usuarios. También podemos ofrecer ejemplos para ayudarle a comunicarse con los usuarios sobre su programa para concienciar en materia de seguridad. Esto ayuda a promover la implicación y aceptación de los usuarios de una experiencia de aprendizaje importante.

Componentes del programa para concienciar en materia de seguridad

Su programa de concienciación sobre seguridad puede incluir los siguientes módulos, según sus productos con licencia:

- Evaluaciones del conocimiento
- Ataques simulados
- Formación
- Material de concienciación
- Herramientas de refuerzo

Encontrará más información sobre los productos para concienciar en materia de seguridad aquí: **proofpoint.com/es/product-family/security-awareness-training**.

Implementación

Los ataques simulados de Proofpoint establecerán una referencia realista del nivel de vulnerabilidad de su organización frente a varios vectores de ataque. Y puesto que es tan importante conocer la susceptibilidad de los usuarios a ataques, su contacto facilitará campañas de ataques simulados junto con evaluaciones de conocimientos.

Simulaciones de ataques de phishing

Su contacto será el administrador "sobre el terreno" de la herramienta de simulación de ataques de phishing. Elegiremos juntos las plantillas de simulación y los momentos de aprendizaje para cada campaña. Antes de cada campaña, determinaremos asimismo el ámbito de la simulación y los usuarios implicados. Se enviará a los usuarios un ataque de phishing simulado ciego al principio del período de licencia para proporcionar los datos de referencia iniciales. Después de esto, llevaremos a cabo ataques de phishing simulados, intercalados con momentos de aprendizaje, durante todo el período de licencia. Estos momentos de aprendizaje le ofrecerán información inmediata y eficaz sobre todos los usuarios que cayeron en la trampa de un ataque de phishing.

Campañas USB de simulaciones de phishing

Su contacto creará la campaña USB de simulación de ataques de phishing. Configuraremos, programaremos y lanzaremos cada campaña de acuerdo con el plan establecido con su contacto gestionado durante el periodo de vigencia de

la licencia. Configuraremos los nombres de archivos señuelo en los dispositivos y seleccionaremos/personalizaremos el momento de aprendizaje. A continuación distribuiremos el archivo zip con los archivos necesarios y se los enviarán a través de Secure Share. Usted suministrará los dispositivos USB y cargará los archivos en los dispositivos mediante una hoja de cálculo incluida para organizar el despliegue. Una que vez que los dispositivos hayan sido desplegados, su contacto proporcionará informes de actividad según un calendario convenido.

Evaluaciones del conocimiento

Las evaluaciones de conocimientos determinan el nivel de conocimiento de los empleados y permiten valorar la eficacia de la formación. Recomendamos que lleve a cabo una evaluación de conocimientos al principio del período de licencia con temas generales, y evaluaciones adicionales en base a los resultados de la primera evaluación. Esto ayuda a centrarse en áreas de riesgo previamente identificadas.

Módulos de formación

Proofpoint asignará módulos de formación a los usuarios que sucumbieron a ataques de phishing. Estas asignaciones pueden incluir módulos de formación basados en sus productos con licencia. También crearemos asignaciones para cada usuario, con independencia de si se dejaron engañar por un ataque simulado, de manera que cada usuario pueda recibir formación.

A medida que se acerque la fecha de finalización del curso, enviaremos un recordatorio a los usuarios implicados. También evaluamos el nivel de conocimientos de los usuarios para planificar las siguientes evaluaciones y asignaciones de módulos de formación.

Su contacto asignará módulos de formación sobre temas de seguridad y cumplimiento de normativas, incluidas asignaciones de inscripción automática. Las asignaciones estarán compuestas por varios módulos, en función de las áreas de riesgo identificadas.

NOTA: si utiliza un sistema de gestión de aprendizaje ("LMS") para algunas o para todas las asignaciones de formación, la gestión de usuarios, las asignaciones y la generación de informes del LMS serán su responsabilidad, no del contacto. Las cápsulas de formación (Training Jackets) y la asignación automática no están disponibles para módulos basados en sistemas de gestión de aprendizaje.

Refuerzo

PhishAlarm proporciona un refuerzo positivo a los usuarios que denuncian phishing potencial. El complemento de correo electrónico PhishAlarm alertará a los equipos de seguridad y respuesta a incidentes sobre mensajes de correo electrónico de phishing sospechosos con tan solo hacer clic en un botón. Esto reduce la duración y el impacto de los ataques de phishing activos mientras refuerza los comportamientos aprendidos en su programa para concienciar en materia de seguridad. La denuncia de phishing es un parámetro de tendencia importante para controlar el comportamiento de los usuarios, así como la concienciación y participación en la seguridad. El material para concienciar en materia de seguridad está diseñado para el refuerzo de los principios básicos impartidos en nuestros módulos de formación. Esto le permite enfatizar las mejores prácticas y mejorar la retención del conocimiento. Proofpoint asignará material para concienciar en materia de seguridad a áreas débiles dentro de la evaluación del conocimiento.

Análisis

En conjunto, los resultados de la evaluación, las campañas de ataques simulados, la formación y la denuncia de correo electrónico de PhishAlarm ofrecen una vista global de los niveles de conocimientos de los usuarios y su susceptibilidad a ataques. Gracias a estos datos, puede identificar sus áreas de mayor riesgo y crear un plan dirigido para reforzar los conocimientos de sus empleados.

Su contacto revisará los resultados después de cada evaluación y asignación de formación. Los resultados se compararán con el rendimiento histórico para obtener tendencias de mejora y áreas anteriores o nuevas de interés. Las propiedades incluidas en los informes (definidas en su sesión de planificación inicial) se revisarán para correlacionar el riesgo con el departamento, la ubicación, la función o el responsable. Este análisis se decidirá en las sesiones de planificación y estrategia en curso y se utilizarán para determinar los siguientes pasos. Su contacto le proporcionará análisis comparativos del sector y de muestra, si los hay.

Análisis de VAP

Para los clientes con Proofpoint Targeted Attack Protection (TAP), su contacto:

- Identificará las personas más atacadas dentro de su organización.
- Segmentará sus VAP en base a los datos de amenazas dirigidas.
- Creará actividades de formación y concienciación para VAP basadas en las amenazas identificadas.
- Analizará sus VAP y su rendimiento en el programa para concienciar en materia de seguridad a lo largo del tiempo.

Generación de informes

Los informes posteriores a cada actividad se entregarán de forma segura a medida que avance el programa. También puede aprovechar la API de resultados para crear paneles a través de la herramienta de inteligencia empresarial que elija.

Calendario del programa de concienciación en materia de seguridad

Este calendario describe nuestro plan sugerido para implementar nuestra metodología de formación continua. El calendario se modificará en función de sus productos con licencia, el período y las necesidades y objetivos específicos de su programa.

Mes 1 a 3

	MES 1	MES 2	MES 3
Evaluación de conocimientos	Evaluación de conocimientos de referencia 1 Comunicación inicial		
Phishing	Ataque de phishing ciego 1	Campaña 1 con inscripción automática	
Formación		Formación con inscripción automática	Usuario que no hace clic
Material de refuerzo		Tema seleccionado	

Mes 4 a 6

	MES 4	MES 5	MES 6
Evaluación de conocimientos			
Phishing	Campaña 2	Campaña 3	Campaña 4
Formación		Formación suplementaria	Usuario que no hace clic
Material de refuerzo		Nuevo tema	

Mes 7 a 9

	MES 7	MES 8	MES 9
Phishing		Campaña 5	Campaña 6
Formación	Usuario que no hace clic		Formación suplementaria*
Material de refuerzo		Nuevo tema	

Mes 10 a 12

	MES 10	MES 11	MES 12
Evaluación de conocimientos			Repetición de evaluación de conocimientos 1
Phishing	Campaña 7	Campaña 8	

* Los temas de formación vienen determinados por los resultados de las evaluaciones de conocimientos. Las unidades USB de simulación de ataques de phishing pueden entregarse en cualquier momento durante el período de licencia.

"Proofpoint Managed Security Awareness" se llamaba antes "Managed Proofpoint Security Awareness Training".

MÁS INFORMACIÓN

Para obtener más información, visite **http://proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.