

Proofpoint Security Awareness Training Enterprise

PRODUCTOS

- Proofpoint Security Awareness Training Enterprise
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull

VENTAJAS PRINCIPALES

- Reducción de hasta un 90 % de los ataques de phishing y las infecciones de malware.
- Reducción del riesgo que plantean el phishing y otros ciberataques, gracias a la modificación del comportamiento de los usuarios.
- Optimización de la eficacia de las iniciativas mediante una formación dirigida y adecuada de los usuarios.
- Reducción de la exposición y la carga de trabajo para el personal de TI gracias a la formación de los usuarios y a la automatización de la respuesta a incidentes.
- Seguimiento del progreso alcanzado mediante la generación de informes dinámicos y la comparación con datos de referencia.

Más del 90 % de los ciberataques se dirigen contra los usuarios¹, por lo que la formación de los empleados es fundamental para la seguridad de su organización. Las tecnologías que detectan y bloquean las amenazas antes de que lleguen a los usuarios no pueden neutralizar todos los ataques. Sus empleados deben ser conscientes de esta realidad y ser capaces de reaccionar adecuadamente a intentos de ataques de phishing y estafas Business Email Compromise (BEC). La solución le ayuda a formar a sus empleados a reaccionar correctamente a los ciberataques de este tipo.

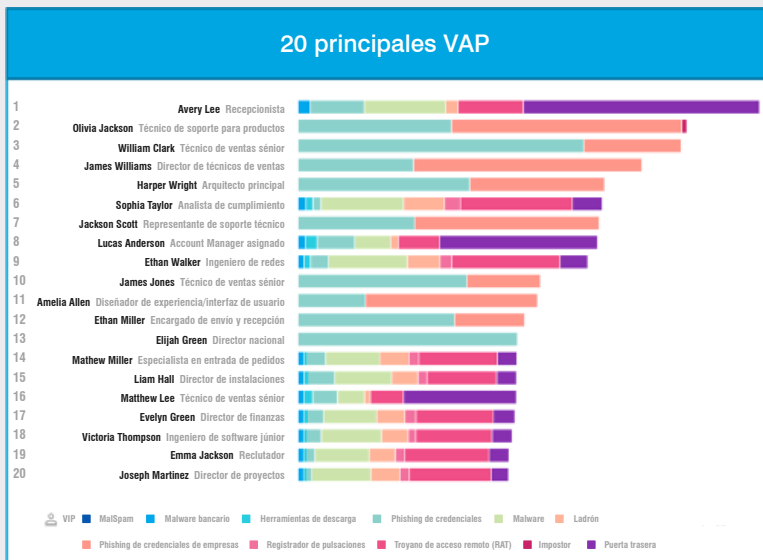
Proofpoint Security Awareness Training Enterprise le permite ofrecer la formación adecuada a las personas apropiadas para que reaccionen de manera eficaz a los ataques peligrosos actuales. Esta solución transforma a sus empleados en una sólida línea de defensa para proteger proactivamente a su organización.

Le ayudamos a distintos niveles:

- Identificación de los riesgos asociados a los usuarios
- Modificación del comportamiento de los empleados
- Reducción de la exposición a riesgos de su organización



¹ Verizon. "2019 Data Breach Investigations Report" (Informe de investigaciones de fugas de datos de 2019). Julio de 2019.



Ejemplo de informe de VAP. Los clientes pueden utilizar phishing simulado con las últimas tendencias de ataque para estos usuarios de alto riesgo e inscribir automáticamente en el curso de formación a los que no superan una simulación.

Identificación de los riesgos

Identifique quién está siendo atacado y evalúe su capacidad para protegerse

No todos los empleados sufren ataques de la misma intensidad. Hay muchos factores que convierten a un empleado en un objetivo deseable para un ciberataque. Gracias a la integración de Proofpoint con Targeted Attack Protection (TAP), sus administradores pueden centrarse en los recursos más vulnerables y garantizar una eficacia máxima. Esto se consigue con un programa de concienciación en materia de seguridad más normativo y atractivo, basado en los riesgos reales de su entorno de correo electrónico.

Esta potente integración facilita información sobre sus VAP (Very Attacked People, o personas muy atacadas) y sobre los empleados más incautos de su organización, así como sobre los tipos de amenazas que reciben o por las que se dejan engañar. Puede utilizar esta información para inscribir a los usuarios en simulaciones y evaluaciones de conocimientos que permitan valorar el riesgo o para asignarles tareas formativas que induzcan un cambio de comportamiento.

Las simulaciones de phishing de ThreatSim® le ayudan a conocer el nivel de vulnerabilidad de su empresa ante distintos ataques de phishing. Puede elegir entre miles de plantillas de phishing diferentes de 13 categorías distintas para evaluar la respuesta de los usuarios ante muchos tipos de amenazas, como:

- Adjuntos maliciosos
- Enlaces incrustados
- Solicitudes de datos personales

Cada semana añadimos nuevas plantillas para asegurarnos de que siempre estén representadas las últimas tendencias de ataques. Nuestras plantillas de phishing de simulación dinámica de amenazas se crean a partir de la inteligencia de amenazas

de Proofpoint, junto con peticiones recibidas de los clientes o temas que dependen de la época del año. La inteligencia sobre amenazas de Proofpoint compartida en tiempo real es la solución más desplegada por las empresas de los índices Fortune 100, Fortune 1000 y Global 2000. Esto significa que las plantillas reflejan lo que los usuarios pueden ver en un ataque real.

Cuando un usuario cae en la trampa de un ataque simulado, recibe formación que denominamos "enseñanza a tiempo" (o "just-in-time teaching"), que le permite comprender:

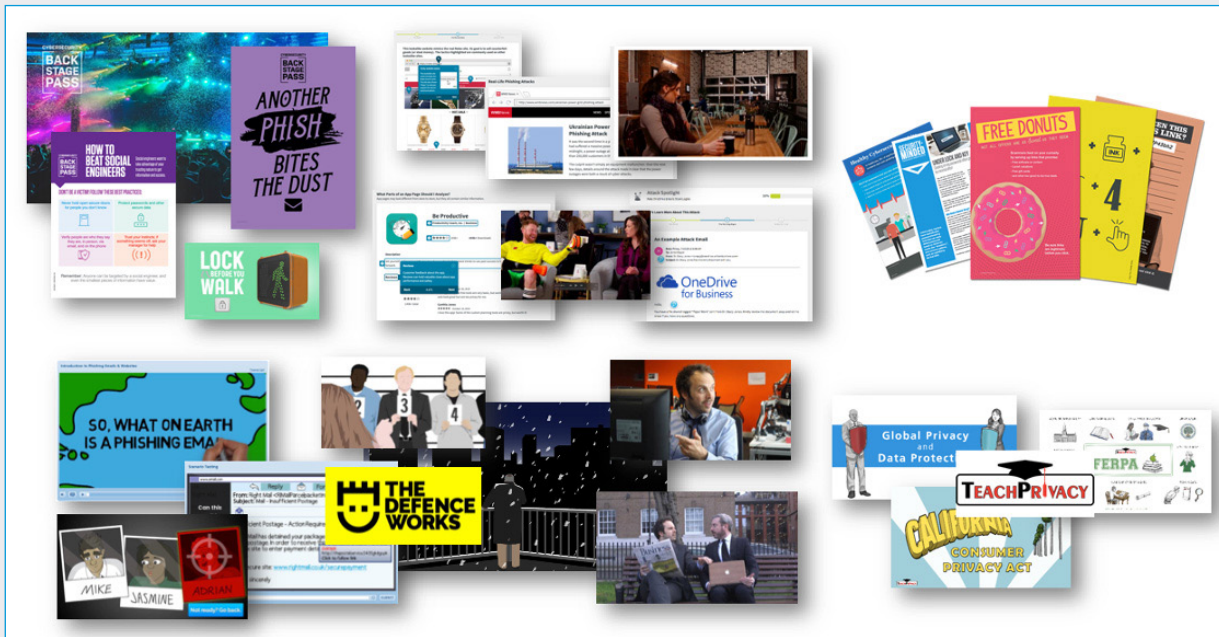
- El objetivo del ejercicio
- Los peligros de los ataques reales
- Cómo evitar dejarse engañar en el futuro

También es posible asignar automáticamente formación adicional a las personas que caen en la trampa durante una simulación de ataque de phishing.

Además, puede averiguar el nivel de concienciación de sus empleados sobre los problemas asociados a los dispositivos de memoria extraíbles infectados. Las simulaciones USB de ThreatSim muestran a sus empleados los peligros de los dispositivos USB infectados. Puede acceder a las simulaciones para USB en cualquier momento y realizar todas las que desee. Esta función incluye contenido educativo "just in time" y está pensada para los usuarios que no superan el ejercicio de simulación.

No obstante, las simulaciones solo pueden transmitir el riesgo específico de esos vectores de amenaza. CyberStrength® es una potente herramienta de evaluaciones de conocimientos. Le permite:

- Evaluar las vulnerabilidades de los usuarios en una gran variedad de temas fundamentales relacionados con la seguridad, como el uso de dispositivos móviles, los timos de ingeniería social, las contraseñas y la navegación web, además del correo electrónico y las unidades USB.



- Seleccionar evaluaciones predefinidas en una biblioteca de cientos de preguntas en más de 40 idiomas e inscribir automáticamente a los usuarios en el curso apropiado.
- Crear preguntas personalizadas para calibrar su conocimiento de las políticas y los procedimientos de su empresa.
- Seguir las recomendaciones para reducir los riesgos asociados a los usuarios en las áreas temáticas evaluadas una vez establecida una base de referencia.

Modificación de comportamientos

Ofrezca formación basada en las amenazas reales, el comportamiento de los usuarios y las lagunas de conocimiento

Con el objetivo último de cambiar comportamientos, nuestra formación está diseñada para ofrecer a los usuarios experiencias educativas personalizadas y atractivas. Nos aseguramos de que nuestro programa se centre en primer lugar en las áreas de mayor riesgo. Una vez identificadas con Proofpoint Targeted Attack Protection (TAP), pueden impartirse cursos de formación a las personas muy atacadas (VAP) o a las más incautas. Además, la formación puede centrarse en los usuarios que no superan las simulaciones o las que obtienen una puntuación por debajo de un determinado umbral en una evaluación de conocimientos.

El liderazgo del contenido de Proofpoint ha conseguido transformar a millones de usuarios vulnerables en una sólida línea de defensa para la organización. Para asegurarnos de que nuestro contenido induce cambios de comportamiento, utilizamos lo siguiente:

Metodología

- Uso de las mejores prácticas demostradas para modificar comportamientos en adultos.
- Accesibilidad y posibilidad de búsqueda del contenido en nuestra biblioteca.

- Acceso a una gran diversidad de contenidos con cientos de módulos de formación y materiales relacionados con el programa.
- Planes de estudio dirigidos por CISO para desarrollar las competencias necesarias según el tipo de usuario (basadas en privilegios, funciones, etc.).

Soporte mundial y multicultural

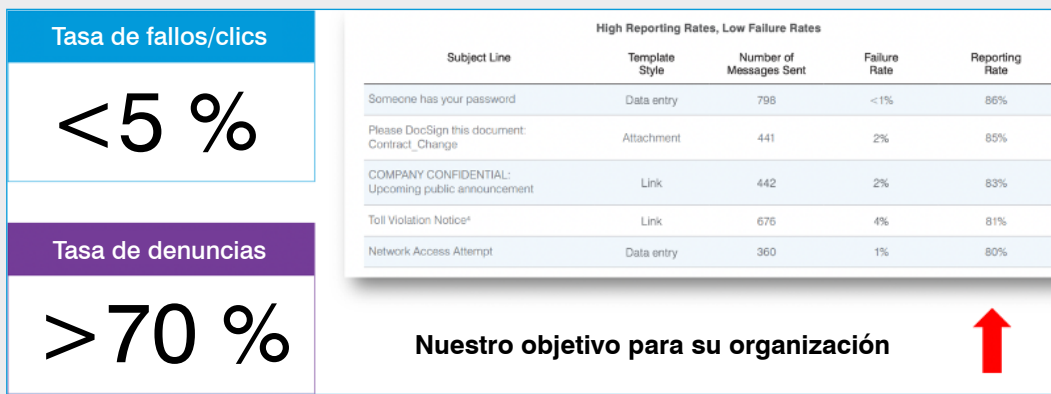
- Contenido traducido a más de 40 idiomas y referencias regionales (dominios, nombres, etc.) en todos los planes de estudios principales.
- Inclusión y diversidad de texto e imágenes.

Preparación para nuevas amenazas

- Aprovechamiento de la mejor inteligencia sobre amenazas del mercado para ir un paso por delante de los ciberdelincuentes.
- Miles de millones de muestras de amenazas recopiladas diariamente del correo electrónico, la nube y las redes sociales.
- Contenido basado en amenazas, como nuestras alertas de amenazas, los módulos Attack Spotlight y las plantillas de simulación.

La diversidad de contenidos es fundamental para que los usuarios puedan ver su utilidad. La biblioteca de Proofpoint contiene más de 200 módulos formativos y se incorporan nuevos contenidos permanentemente. Los centenares de materiales de nuestro programa incluyen PDF, infografías, vídeos, memes y mucho más. Nuestra adquisición en mayo de 2020 de The Defence Works y nuestra alianza con TeachPrivacy aseguran una variedad de contenido aún mayor. Toda esta diversidad de estilos formativos permite adaptarlos a la cultura de cualquier organización. Nuestras mejores prácticas, campañas y planes de estudio le ayudarán a preparar atractivas experiencias de formación en múltiples canales.

[Para ver el contenido disponible, descargue el [resumen de la solución Proofpoint Security Awareness Training](#)]



Resultados con clientes reales entre las organizaciones con mejor rendimiento del informe "State of the Phish 2020" de Proofpoint.

Distribución de contenido

Con nuestro Customization Center con funciones de autoservicio, puede mejorar la relevancia del contenido para adaptarlo a sus empleados. Puede:

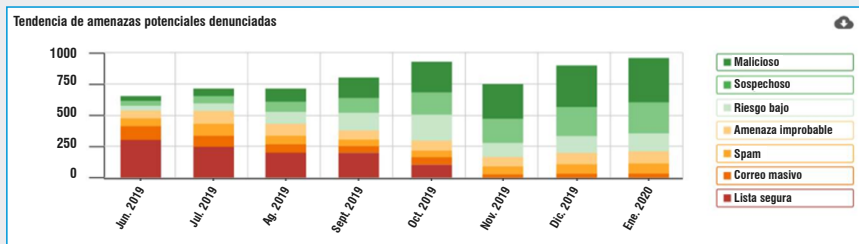
- Adaptar fácilmente la formación con la ayuda de texto, imágenes y preguntas pertinentes para sus usuarios.
- Clonar y modificar rápidamente módulos, lecciones y páginas para realizar los cambios necesarios, todo en tiempo real.
- Transformar los módulos de formación (con preguntas) en módulos de concienciación con un clic.
- Garantizar la eficacia del contenido con nuestro Learning Science Evaluator, que le advierte si la longitud, la cantidad de contenido en pantalla o el número de preguntas de un ejercicio se desvían de lo indicado.

En las empresas que poseen su propio sistema LMS que utiliza archivos SCORM, los administradores pueden fácilmente personalizar y exportar los módulos de formación a su LMS. Pueden combinar varios módulos en uno, y también definir el orden en el que los usuarios deben realizarlos.

Reducción de la exposición a riesgos

Los usuarios bien informados denuncian las amenazas potenciales, lo que reduce la superficie de ataque

Haga posible que sus empleados denuncien los mensajes sospechosos con un solo clic utilizando nuestro add-on para cliente de correo electrónico PhishAlarm®. Tras denunciar un correo electrónico sospechoso, los usuarios reciben un mensaje emergente de agradecimiento para reforzar inmediatamente los comportamientos positivos. Este complemento elimina la necesidad de obtener los encabezados y archivos adjuntos de los usuarios, que de otra manera reenviarían los mensajes a un buzón de correo malicioso. La tasa de denuncias habitual de una organización varía entre el 10 y el 20 %. Gracias a la formación de sus empleados, algunos de nuestros clientes han conseguido que más de un 70 % y a veces incluso más de un 80 % de los usuarios denuncien los ataques simulados.



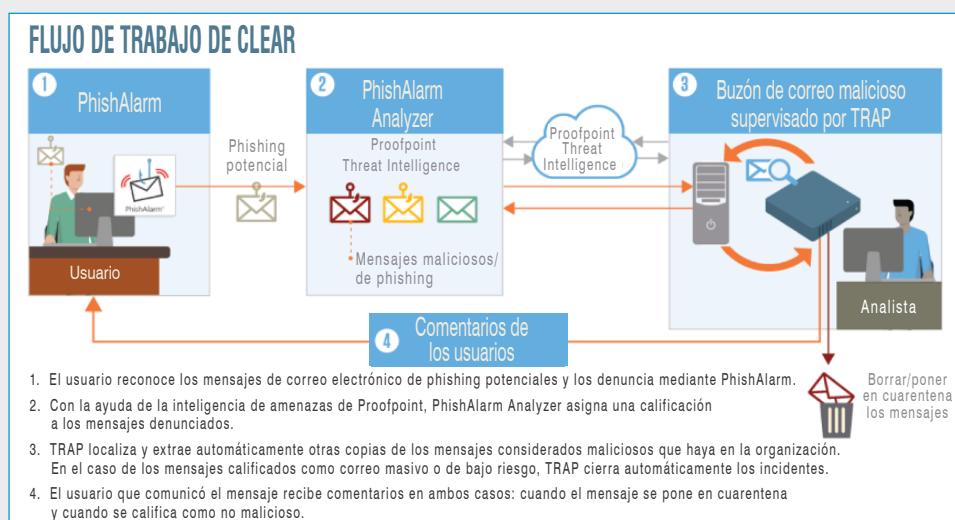
Los tipos de mensajes denunciados permiten evaluar mejor los progresos de los usuarios.



Proporcione información práctica al equipo de respuesta a incidentes.

Pero los ataques simulados no son un riesgo comparable a las amenazas reales del entorno. Contamos con inteligencia sobre amenazas de talla mundial, junto con análisis en entornos aislados (sandbox). Le informaremos automáticamente si los mensajes denunciados por los usuarios son maliciosos o no a través de un informe descriptivo de las amenazas, que incluye información detallada sobre qué elementos del mensaje son maliciosos. Esto permite a su equipo de respuesta a incidentes ganar tiempo y ofrece información sobre cómo su programa de concienciación en materia de seguridad reduce los riesgos asociados al correo electrónico. Nuestra inteligencia sobre amenazas procede de la solución más desplegada por las empresas de los índices Fortune 100, Fortune 1000 y Global 2000. Permite la mejor agregación y correlación de datos de amenazas en el correo electrónico, la nube, la red y las redes sociales.

Con nuestra solución automática CLEAR (Closed-Loop Email Analysis and Response), los mensajes denunciados se envían a Threat Response Auto-Pull (TRAP). En TRAP, estos mensajes pueden ponerse automáticamente en cuarentena, cerrarse o bien enviarse al equipo de respuesta a incidentes para profundizar en el análisis, si así se desea. Los administradores pueden definir mensajes de respuesta personalizados para los usuarios en función de la clasificación del mensaje. Estos mensajes personalizados se envían a los usuarios para reforzar su comportamiento y ayudar a crear una cultura de concienciación en el tema de la seguridad.



Evaluación y adaptación

Comprenda cómo afecta el cambio de comportamiento de los usuarios a los principales resultados

Nuestros completos informes le ayudan a entender cómo cambia el comportamiento de los usuarios y le indican cuál es la posición de su organización con respecto a empresas como la suya.

Puede conocer las interacciones de los empleados mediante:

- Evaluaciones
- Ataques simulados
- Tareas de formación
- Informes y análisis del correo electrónico (incluida su eliminación)

Los informes le permiten filtrar los datos con facilidad, comparar las evaluaciones, cambiar los métodos de evaluación y configurar vistas personalizadas.

Le ayudan a responder a preguntas fundamentales como:

- ¿Qué personas son las más vulnerables al phishing simulado en la organización?
- ¿Cuáles son las lagunas de los usuarios en materia de seguridad y cumplimiento de normativas?
- ¿Qué resultados obtienen los usuarios en la formación?
- ¿Cuántos mensajes y de qué tipo denuncian los usuarios (maliciosos, correo masivo, spam, etc.)?

Puede descargar, exportar y configurar la distribución automatizada de informes a otras personas. De esta forma, a su organización le será más fácil estar al día de la información y podrá comunicar automáticamente los resultados a los principales implicados en su programa.

También se incluye nuestra API de resultados. Es una interfaz que ofrece acceso a los informes y análisis sobre formación, phishing, evaluación de conocimientos, usuarios y correo electrónico. Esta información puede integrarse después en herramientas de inteligencia empresarial o en un sistema de gestión del aprendizaje.

MÁS INFORMACIÓN

Para obtener más información, visite proofpoint.com/es.

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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 encuentran más de la mitad del Fortune 1000, 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.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.