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.
- Medida de los cambios del comportamiento de los usuarios con panel de CISO e informes con informes en tiempo real.

Con más del 85 % de las fugas de datos provocadas por algún error humano[1], la seguridad de su organización pasa inevitablemente por enseñar a sus empleados cómo frustrar los ciberataques. Después de todo, 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 frente a intentos de ataques de phishing, ransomware y estafas Business Email Compromise (BEC).

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 que protege proactivamente su organización.

Le ayudamos a distintos niveles:

- Evaluar
- Modificar comportamientos
- Valorar

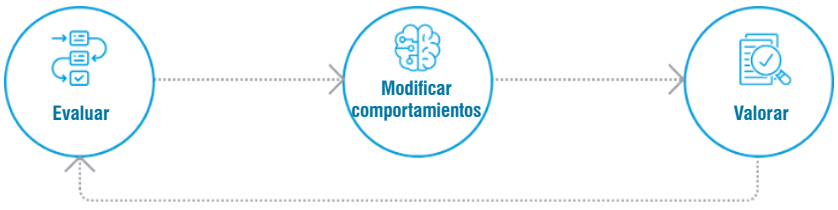

Figura 1: Proceso continuo para una modificación duradera de los comportamientos.

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

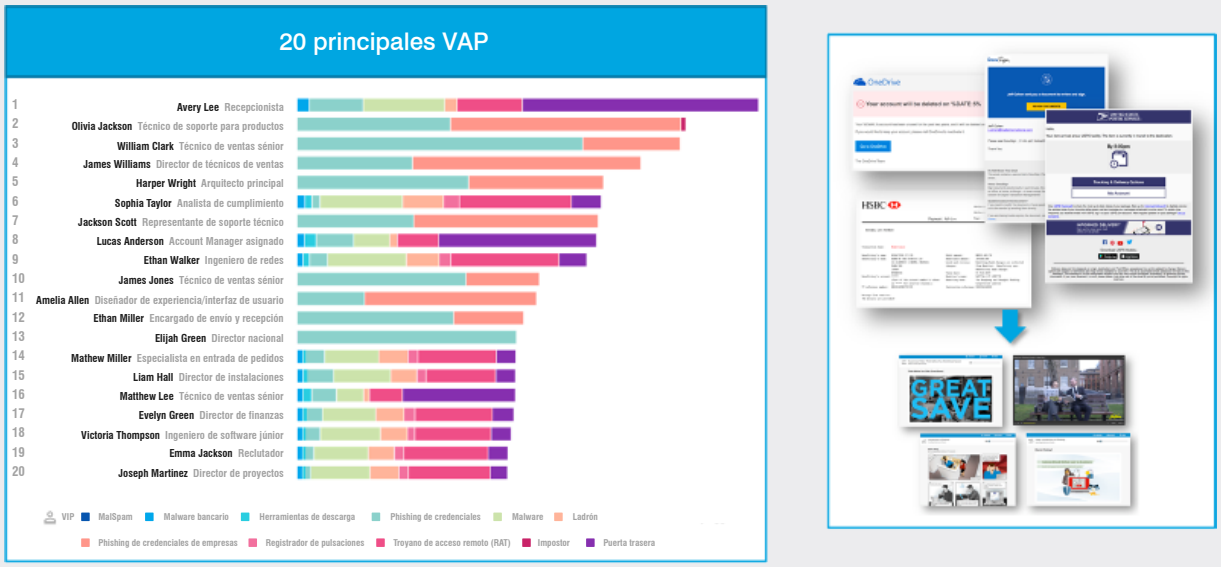

Figura 2: Ejemplo de informe de VAP. Los clientes pueden utilizar phishing simulado con las últimas tendencias de ataque para estos usuarios de alto riesgo e inscribir automáticamente en el curso de formación a los que no superan una simulación.

Evaluar

Identifique quién está siendo atacado y evalúe su capacidad para protegerse

No todos los empleados sufren ataques de la misma frecuencia o intensidad. Muchos factores convierten a empleados distintos en objetivos más atractivos que otros para los ciberdelincuentes. La integración con Targeted Attack Protection (TAP) permite a sus administradores identificar las áreas y personas que representan los mayores riesgos. Con toda esta información, pueden preparar e implementar medidas preventivas más eficazmente. Serán capaces de desarrollar y ejecutar programas de concienciación sobre seguridad de más eficaces basados en riesgos reales.

Esta potente integración permite identificar a sus VAP (Very Attacked People™, o personas muy atacadas) y a los empleados más incautos de su organización. Le facilita información detallada 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 determinar los riesgos. También es posible asignar formación para estimular los cambios de comportamiento.

Las simulaciones de phishing de ThreatSim® le ayudan a conocer el nivel de susceptibilidad de su empresa a los 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, concretamente:

- Basadas en adjuntos (DOC, HTML, PDF, DOCX, XLSX)
- Basadas en enlaces
- Phishing de introducción de datos/credenciales

La actualización continua garantiza que siempre estén representadas las últimas tendencias de ataques. Nuestras simulaciones de ataques de phishing incluyen plantillas dinámicas basadas en la inteligencia sobre amenazas de phishing de simulación de Proofpoint. Las plantillas están diseñadas para responder a las 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 a las personas que caen en la trampa del phishing simulado.

Además, puede conocer el nivel de conocimiento que tienen sus empleados sobre los problemas asociados a los dispositivos de memoria extraíbles infectados. Las simulaciones de ataques con dispositivos USB les enseñan los peligros de los dispositivos USB infectados. Esta función incluye contenido educativo "just in time" para los usuarios que no superan el ejercicio de simulación. Puede acceder a las simulaciones de ataques con dispositivos USB en cualquier momento y para un número ilimitado de campañas.

No obstante, las simulaciones solo pueden reproducir los riesgos de determinados vectores de amenazas. Nuestras evaluaciones de conocimientos le ayudan a determinar el nivel de conocimientos de sus usuarios sobre una amplia variedad de dominios, como las apps cloud, las amenazas internas, los dispositivos móviles, las contraseñas, etc.

También puede:

- Utilizar evaluaciones completas que cubren todos los dominios de control.
- Seleccionar evaluaciones predefinidas en una biblioteca de cientos de preguntas en más de 40 idiomas.
- Inscribir automáticamente a los usuarios en los módulos de formación apropiados si obtienen una puntuación inferior al umbral establecido.

Figura 3: Gran diversidad de contenido que permite estimular la participación de los usuarios.

También puede crear preguntas personalizadas. Utilice esta función para calibrar el conocimiento de las políticas y los procedimientos de su empresa. Una vez que establezca una línea básica de referencia para sus empleados, puede seguir las recomendaciones para cubrir las lagunas de conocimientos y reducir los riesgos.

Modificar comportamientos

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

El objetivo último es modificar los comportamientos, por lo que nuestra formación está diseñada para ofrecer una experiencia personalizada e interesante. Podemos centrar nuestros programas en los recursos más vulnerables, concretamente los VAP o los empleados que más se dejan engañar identificados por Proofpoint TAP. Además, la formación puede centrarse en los usuarios que no superan las simulaciones o que obtienen una puntuación por debajo de un determinado umbral en una evaluación de conocimientos.

Hemos ayudado a millones de usuarios vulnerables a convertirse en una sólida línea de defensa frente a los ciberataques.

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.
- Texto e imágenes inclusivas y diversas.

Preparación para nuevas amenazas

- 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.

Nuestras mejores prácticas, campañas y planes de estudio le ayudarán a preparar atractivas experiencias de formación en múltiples canales. La diversidad de contenidos es esencial. La biblioteca de Proofpoint contiene más de 300 módulos formativos y se incorporan nuevos contenidos permanentemente. Incluye centenares de archivos PDF, infografías, vídeos, memes y mucho más. Ofrecemos distintos estilos y tipos de materiales para responder a la cultura de cualquier organización y preferencias de usuarios. Además, nuestra alianza con TeachPrivacy garantiza una cobertura todavía más completa del cumplimiento.

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

Figura 4: Resultados con clientes reales entre las organizaciones con mejor rendimiento del informe "State of the Phish 2020" de Proofpoint.

Distribución de contenido

Mejore la relevancia del contenido para adaptarlo a sus empleados. Nuestro Customization Center, con funciones de autoservicio, le permite:

- Adaptar la formación con la ayuda de texto, imágenes y preguntas pertinentes para sus usuarios.
- Clonar y modificar 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 de su contenido con el Learning Science Evaluator. Por ejemplo, si la longitud, contenido en pantalla o número de preguntas de una prueba es demasiado importante, se lo advertiremos.

Si posee su propio sistema de gestión de aprendizaje (LMS) que utiliza archivos SCORM, los administradores pueden fácilmente personalizar y exportar los módulos de formación a su LMS.

Pueden combinar varios módulos, y también definir el orden en el que los usuarios deben realizarlos.

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

Permita a sus empleados denunciar los mensajes sospechosos con un solo clic. Utilice nuestro complemento (add-in) de cliente de correo electrónico PhishAlarm®. Tras denunciar el correo electrónico sospechoso, los usuarios reciben inmediatamente un mensaje emergente de agradecimiento, con objeto de reforzar 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. En general, el porcentaje de usuarios que denuncian las simulaciones de ataques de phishing varía entre el 10 y el 20 %. Gracias a la formación de sus empleados, algunos de nuestros clientes han alcanzado tasas superiores al 70 %.

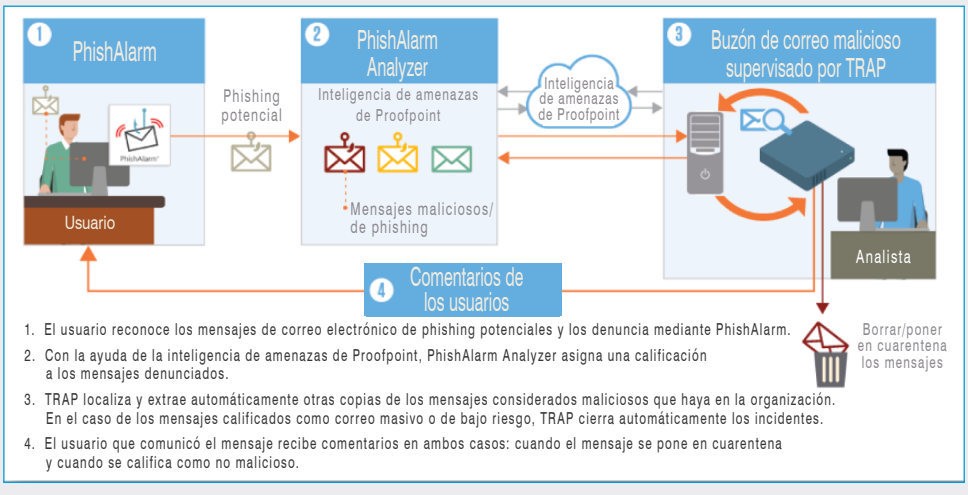

Figura 5: Flujo de trabajo de CLEAR.

Pero los ataques simulados no son un riesgo comparable a las amenazas reales. Nuestra inteligencia sobre amenazas permite la mejor agregación y correlación de datos de amenazas en el correo electrónico, los usuarios la nube, los dominios, las redes y las redes sociales. Contamos con inteligencia sobre amenazas de talla mundial, análisis en entorno aislado (sandbox) y motores de detección para identificar los mensajes maliciosos. Estas funciones pueden proporcionar automáticamente información a los equipos de seguridad sobre los mensajes denunciados gracias al informe sobre amenazas. Además, este informe especifica exactamente qué elemento convierte en maliciosos a los mensajes. 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.

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

Valorar

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

Nuestro panel de CISO ofrece información valiosa para los miembros del equipo directivo. Si quiere compartir los resultados sobre concienciación en materia de seguridad con su CISO/CIO u otras partes interesadas clave, no busque más.

En el panel de CISO encontrará:

- La calificación general de su programa.
- El rendimiento de los diferentes componentes de su programa.
- Una comparación de sus resultados con los de otras organizaciones de su sector.
- Las áreas a las que dar prioridad en su programa.
- Tendencias de datos de rendimiento.
- Datos de vulnerabilidad de los usuarios. Esto incluye los usuarios que menos participan, lo que tienen peor rendimiento y los VAP, si tiene Proofpoint TAP.

Gracias a nuestros nuevos informes en tiempo real, sus administradores ya no tienen que esperar los resultados para presentar el estado de las formaciones asignadas a los usuarios.

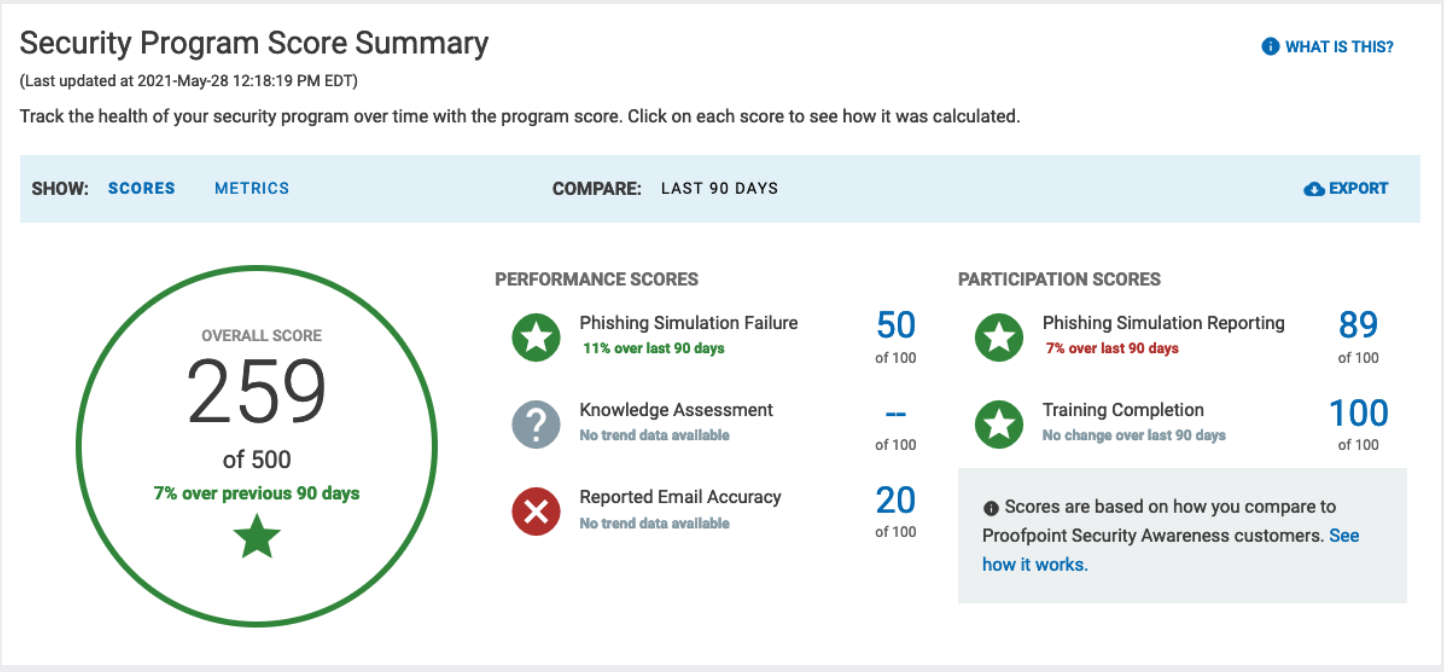

Figura 6: El resumen de calificaciones del panel de CISO ofrece información pertinente en tiempo real sobre el estado actual del programa y compara sus calificaciones con las de otros clientes de Proofpoint.

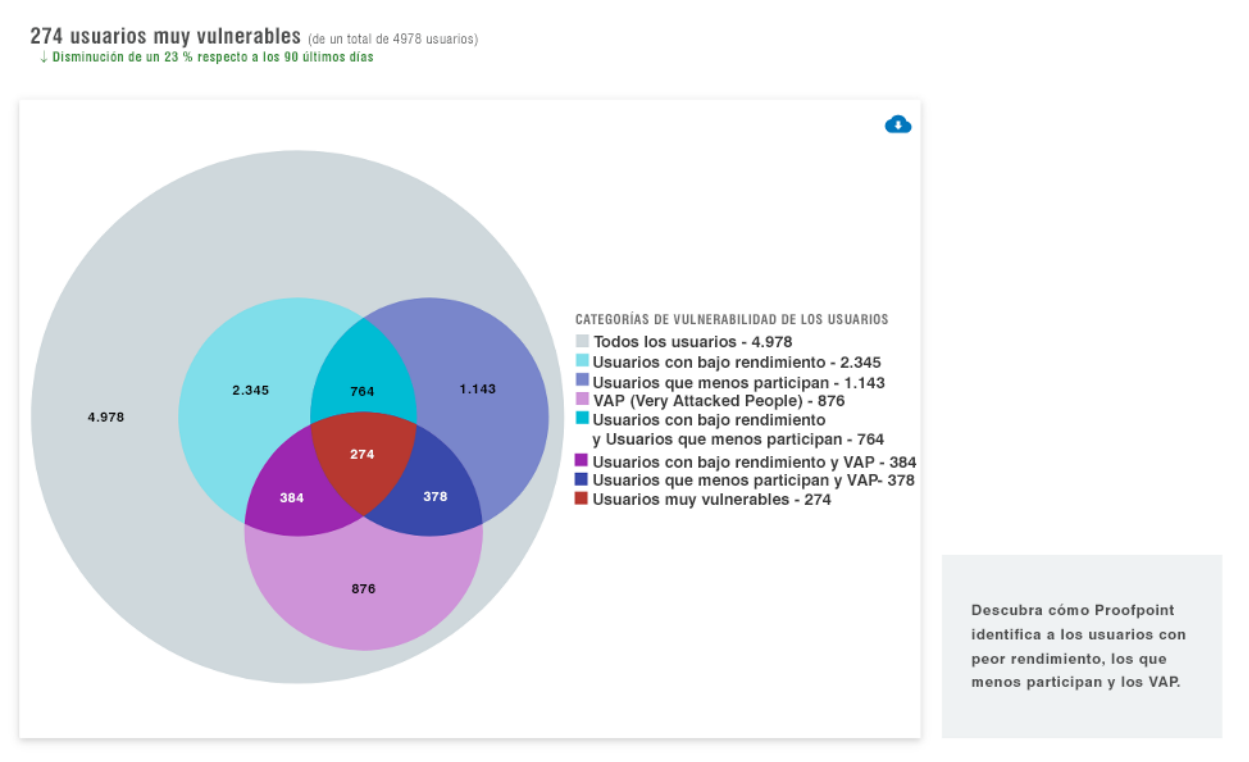

Figura 7: Nuestra sección Vulnerabilidad de los usuarios del panel de CISO le ayuda a elaborar un programa más dirigido y eficaz organizando las actividades para los usuarios vulnerables.

Obtienen comentarios rápidos para mejorar el programa. Nuestros informes en tiempo real ofrecen información muy completa, de simulaciones de phishing a tareas asignadas.

Utilícelos para:

- Obtener rápidamente una visión global del progreso conseguido para una evaluación o formación específica.
- Demostrar la formación realizada con fines de cumplimiento o auditoría.
- Exportar rápidamente un informe para una reunión de último minuto o una solicitud de una parte interesada.
- Adoptar medidas respecto a los usuarios que no cumplen los plazos de la formación que tienen asignada.

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**.