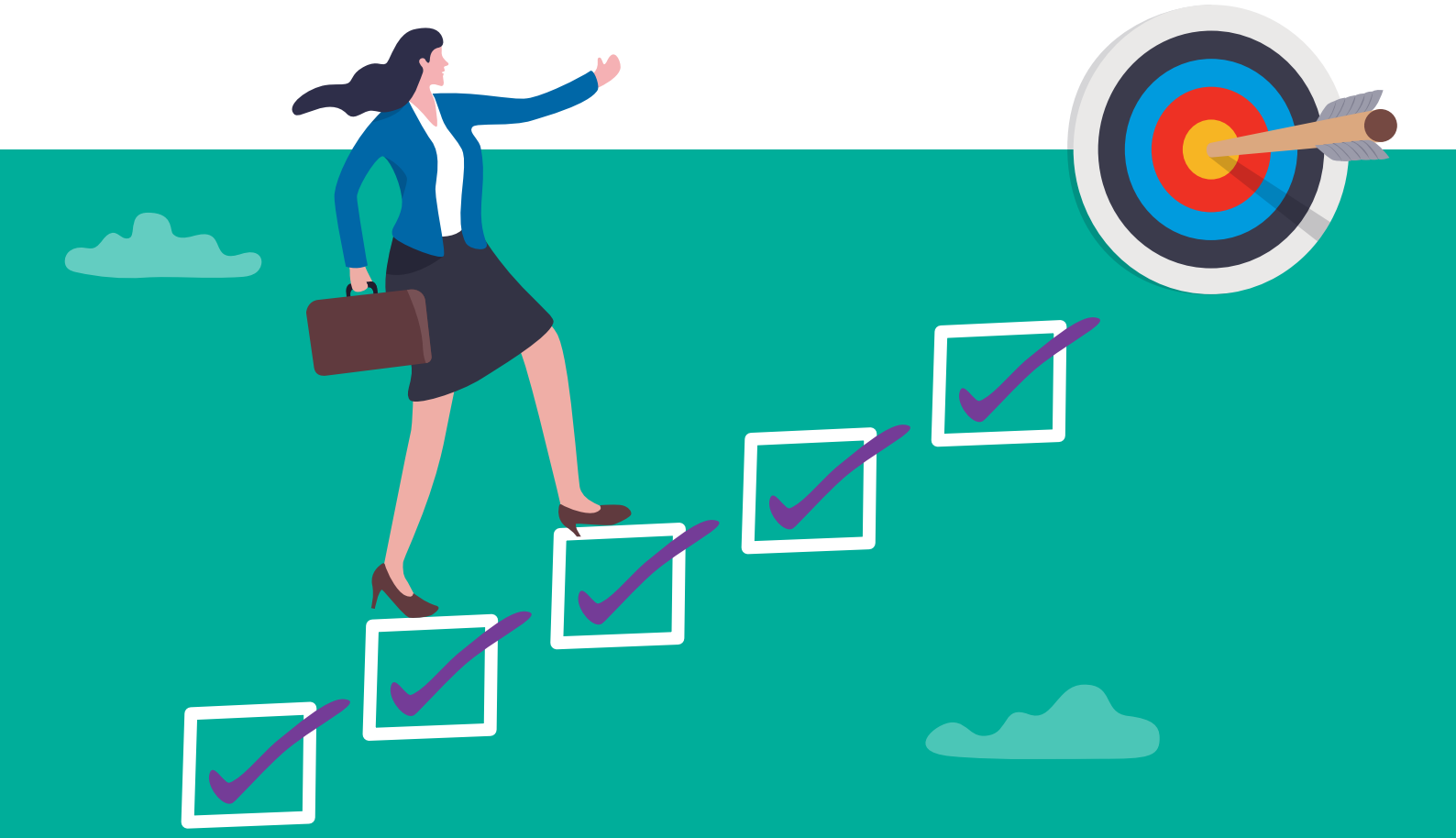
proofpoint.

LIBRO ELECTRÓNICO

EDICIÓN 2023

Impulsando un verdadero cambio de comportamiento

La guía completa para crear un programa de concienciación en materia de seguridad que funcione



Las personas en el centro de sus iniciativas de ciberseguridad

En la actualidad la ciberamenaza más importante no es una vulnerabilidad desconocida, un nuevo malware o el último kit de exploits; son sus propios empleados.

El motivo es que ahora el objetivo de los ataques no son las infraestructuras tecnológicas, sino las personas. Todo ciberataque, sea cual sea su forma, requiere la intervención humana para activarse. Los ciberdelincuentes engañan a las personas para que abran archivos adjuntos maliciosos, hagan clic en URL no seguras, les entreguen las credenciales de sus cuentas e incluso directamente lleven a cabo acciones, como transferir dinero o enviar datos confidenciales.

Por qué es fundamental la formación

Según el informe de sobre las investigaciones de fugas de datos de 2022, en el 82 % de los incidentes intervino el factor humano. Tal y como indica el informe: "el malware y las credenciales robadas entran en juego en un segundo paso, una vez que el ataque de ingeniería social ha abierto la puerta a los ciberdelincuentes, lo que subraya la importancia de disponer de un programa robusto de concienciación en materia de seguridad"[1].

La formación para concienciar a sus empleados en materia de seguridad es una de las medidas más importantes que puede aplicar para proteger a su empresa. Cuando los usuarios sepan reconocer, rechazar y comunicar los intentos de phishing, habrá creado una última línea de defensa contra las mayores ciberamenazas actuales.

Qué aprenderá en esta guía

Poner en marcha un nuevo programa de formación puede parecer una tarea abrumadora. Si además quiere un programa que capte el interés de sus empleados, cambie sus comportamientos y reduzca el nivel de exposición de su organización ante las amenazas, el reto es aún mayor.

Nosotros estamos a su disposición para ayudarle.

Esta guía le muestra cómo crear y mantener un programa de formación en materia de ciberseguridad eficaz, con independencia de la madurez de su programa, el proveedor o los obstáculos a los que se enfrente. Proporciona datos clave, estrategias eficaces, recursos de gran valor y consejos prácticos para los responsables de la seguridad en cada fase del proceso de concienciación en seguridad.

Estas son algunas de las preguntas para las que encontrará respuesta:

- ¿Cómo consigo que mis empleados acepten el programa? ¿Con quién debo trabajar internamente?
- ¿Qué debo hacer? ¿Con qué frecuencia?
- ¿Cómo captar el interés de mis empleados?
- ¿Cómo medir y compartir el éxito?

En el 82 %

de las fugas de datos interviene el factor humano[1].

1 Verizon. "2022 Data Breach Investigations Report" (Informe sobre las investigaciones de fugas de datos de 2022), junio de 2022.

Un modelo centrado en las personas para medir y mitigar los riesgos asociados a los usuarios

Si cada persona es única, el valor para los ciberdelincuentes y los riesgos que presentan para la organización también lo son. En Proofpoint, hemos creado el modelo (VAP)™ (Very Attacked People, o personas muy atacadas) para medir y mitigar tres aspectos distintos del riesgo asociado al usuario.

La formación para concienciar en materia de seguridad está principalmente ligada a la vulnerabilidad del usuario. Sin embargo, su programa también debe tener en cuenta el perfil de ataque y los privilegios de sus empleados. Esta información le ayuda a adoptar un enfoque de la concienciación centrado las personas que incluye formación de seguimiento adaptada, proactiva y dirigida.

V

Vulnerabilidad

Mide con qué frecuencia su empleado es víctima de un ataque debido a su susceptibilidad ante las tácticas que utilizan los atacantes o a que tiene hábitos digitales poco seguros. Se puede medir mediante evaluaciones de conocimientos, cuestionarios de formación para concienciar en seguridad y ataques de phishing simulados.

A

Perfil de ataque

Cuantifica el volumen y el nivel de sofisticación de los ciberdelincuentes y de los ataques que se dirigen contra el usuario. También puede tener en cuenta a usuarios relacionados o parecidos dentro o fuera de la organización.

P

Privilegios

Mide el valor y la confidencialidad de los datos, sistemas y recursos a los que el usuario tiene acceso. Se puede considerar también como una forma de calcular el daño que podría provocar un ataque contra ese usuario si tuviera éxito.

Índice

SECCIÓN 1

Lo que debe saber antes de empezar

Ya lo tiene. Por fin ha concluido el proceso de adquisición. Solo falta que su nuevo proveedor de concienciación en seguridad le envíe un enlace a su software, y todo listo para comenzar. Puede empezar a lanzar ataques de phishing simulados, recopilar datos, asignar sesiones de formación y utilizar todas las fantásticas funcionalidades y el contenido que ha visto en las demostraciones del producto.

Así que, envía el mensaje que anuncia su nuevo programa de concienciación en materia de seguridad. Pero, de repente, su bandeja de entrada recibe multitud de respuestas:

- ¿Quién aprobó este ejercicio?
- Voy a hablar con mi VP sobre este tema.
- ¿Realmente tengo que hacer esto?

Estos suelen ser los primeros obstáculos que encuentran nuestros clientes. Sin embargo, también nos ofrecen una idea de lo primero que se puede hacer para garantizar el éxito de un programa de concienciación en seguridad: conseguir la aceptación del empleado.

Una impresión que comparten muchos clientes es que algunos empleados simplemente no desean participar en cursos de formación para concienciar en seguridad.

Poner a los empleados de su parte

Una impresión que comparten muchos clientes es que algunos empleados simplemente no desean participar en cursos de formación para concienciar en seguridad. Es posible que los ataques simulados les hagan sentirse vulnerables. O quizás consideren la formación como otro ejercicio corporativo más y una distracción de su "trabajo real".

A continuación se indican algunas formas de solucionar este habitual inconveniente:

Hable siempre destacando las ventajas que la formación tiene para el empleado. Cuando diseñe las comunicaciones que presentará a los empleados, tenga en cuenta la pregunta que le van a formular: "¿Y esto qué tiene que ver conmigo?". Saque a colación ejemplos del mundo real, como los robos de identidad o de tarjetas de crédito, la usurpación de cuentas y otros casos similares. Muéstreles cómo la formación ayuda también a los usuarios en su vida personal. De esta forma apreciarán la utilidad del programa para su propio caso particular y mejorará la participación.

Consiga un equilibrio entre las evaluaciones y la formación. Los programas suelen incluir evaluaciones de phishing simulado. Sin embargo, en ocasiones se abusa de ellas. Muchos clientes nos hablan de la necesidad de conseguir un equilibrio entre las actividades de evaluación, y las de formación y concienciación. Uno de ellos nos comentó: "Cuando únicamente envío simulaciones de phishing, los usuarios piensan que intentamos engañarlos". Es conveniente incluir la dosis adecuada de estos dos tipos de actividades, junto con otras de concienciación o de otra clase, como concursos.

Muestre un rostro amable y sonriente en los eventos de la empresa. Las evaluaciones y las sesiones de formación por ordenador pueden acabar siendo muy impersonales. Con un estand en grandes eventos de la empresa o con sesiones virtuales, como los webinars, ofrecerá a los usuarios la posibilidad de tener un contacto más personal. Empiece por una presentación para empleados, organice los eventos de aprendizaje y proporcione recursos de utilidad. Piense en la posibilidad de ofrecer premios o incluso simplemente un café. Todo esto ayuda a humanizar el programa y le pone una cara amiga y un nombre.

Vencer la resistencia

A juzgar por las conversaciones con clientes, los usuarios que no están interesados en el programa se clasifican en dos tipos:

- **Reincidentes:** usuarios que suspenden sistemáticamente las simulaciones de phishing y otras evaluaciones.
- **Reticentes:** usuarios que se niegan a realizar el curso de formación.

Es posible que ya haya intentado todo lo posible para cambiar este comportamiento: mensajes de correo electrónico, conversaciones en persona, charlas con un superior o incluso desconectarles el acceso a la red. Si no lo ha conseguido, sepa que no ha agotado todas las vías.

La estrategia de un cliente era reservar 15 minutos en los calendarios de estos empleados para hablar con el CISO u otro responsable acerca de:

- La importancia del comportamiento del empleado y de estar concienciado sobre la seguridad.
- Cómo el departamento está intentando ayudar con la protección de la empresa y los usuarios en situaciones personales.
- Por qué los empleados deben comprometerse a estar más atentos y a participar en formación para ayudar.

Este tipo de interacción surte efecto, ya que recalca de manera personal y tangible la importancia que tienen un buen comportamiento y una mayor participación.

Las denuncias de phishing son un arma de doble filo

Durante una de nuestras conferencias anuales, un cliente realizó el siguiente comentario después de la presentación.

"Mis empleados no denuncian los mensajes de phishing en nuestro buzón de correo malicioso", dijo. "Solamente hay spam o mensajes legítimos. Nuestro equipo no da abasto. ¿Cómo podemos solucionarlo?".

Los buzones de correo malicioso son una forma excelente de reducir el riesgo. Sin embargo, no es un secreto que su administración lleva mucho tiempo. Nosotros hemos encontrado dos soluciones a este obstáculo habitual:

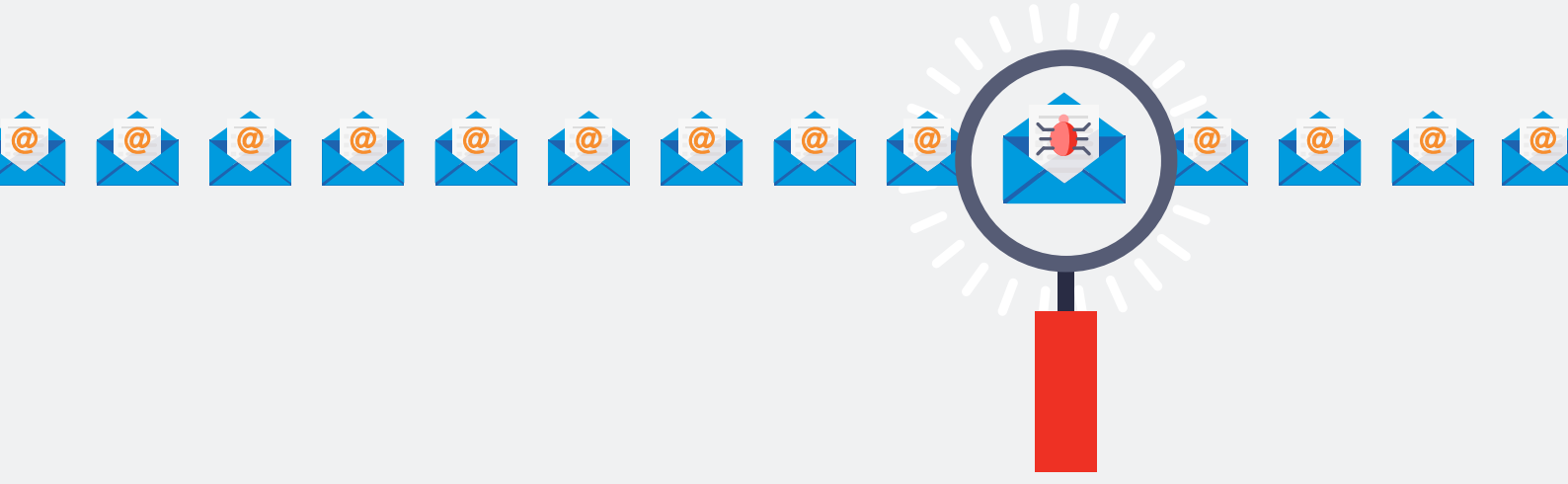
- Ayude a sus empleados a detectar mejor los mensajes de phishing verdaderos.
- Automatice el proceso de análisis y respuesta a mensajes de phishing denunciados.

El resultado natural de un programa de concienciación en seguridad eficaz será una mejora de las denuncias. Muchos clientes observan una mejora en las denuncias, con más mensajes verdaderamente maliciosos y menos falsos positivos, en un plazo de seis a doce meses tras implementar un programa eficaz para formar a los usuarios de manera que identifiquen los mensajes de phishing.

La automatización del análisis del correo electrónico y la respuesta puede facilitar las cargas de trabajo mediante el empleo de entornos aislados (sandbox) e inteligencia sobre amenazas para el análisis y enriquecimiento de la información. De esta forma, se elimina el contenido malicioso de las bandejas de entrada de los usuarios o se cierran los falsos positivos automáticamente, lo que reduce la carga de trabajo para el personal de TI.

Otra ventaja de la respuesta automatizada es que los usuarios pueden recibir comentarios personalizados que les permiten saber si el mensaje que han denunciado era realmente malicioso. De esta forma, los usuarios aprenden y se mejora la seguridad, reforzando el comportamiento positivo con un simple agradecimiento por denunciar mensajes maliciosos.

El resultado natural de un programa de concienciación en seguridad eficaz será una mejora de las denuncias.



SECCIÓN 2

Planificación de su programa

La planificación no es un detalle aislado de su programa de formación para concienciar en materia de seguridad; es la suma de todos sus esfuerzos. Para que el programa llegue "en el momento preciso" se requiere que la formación sea la adecuada, para las personas apropiadas y con la suma de muchos otros componentes tácticos, organizativos y estratégicos.

Cada organización es diferente y no habrá dos programas de formación iguales, pero el suyo debe incluir los siguientes elementos:

- Definición de las necesidades de formación
- Identificación de los usuarios que tienen necesidades de formación concretas
- Definición de actividades
- Creación y administración de calendarios
- Comunicación y prueba de los primeros pasos
- Definición de la frecuencia y la programación de las actividades del programa

Orden recomendado de las actividades: lista de verificación

Un principio fundamental de la ciberseguridad centrada en las personas es que cada usuario es diferente.

El éxito de su programa depende en gran medida de su planificación y diligencia. Estos pasos clave han sido de utilidad para nuestros clientes.

1. **Definición de las necesidades de formación.**

   La ciberseguridad centrada en las personas comienza por medir el riesgo para los usuarios. Las evaluaciones de los usuarios proporcionan información sobre dónde son más vulnerables sus empleados y qué sesiones de formación debe asignarles para mejorar su conocimiento de tema fundamentales, como el phishing, la protección de datos o la seguridad para dispositivos móviles, etc.

   El riesgo no es un factor aislado. Una parte esencial de la identificación de las necesidades de formación es entender el panorama de amenazas actual. Ahí es donde la inteligencia sobre amenazas juega un papel clave. La inteligencia sobre amenazas del mundo real obtenida de forma puntual le ayuda a conocer las amenazas actuales y emergentes a las que pueden enfrentarse los usuarios.

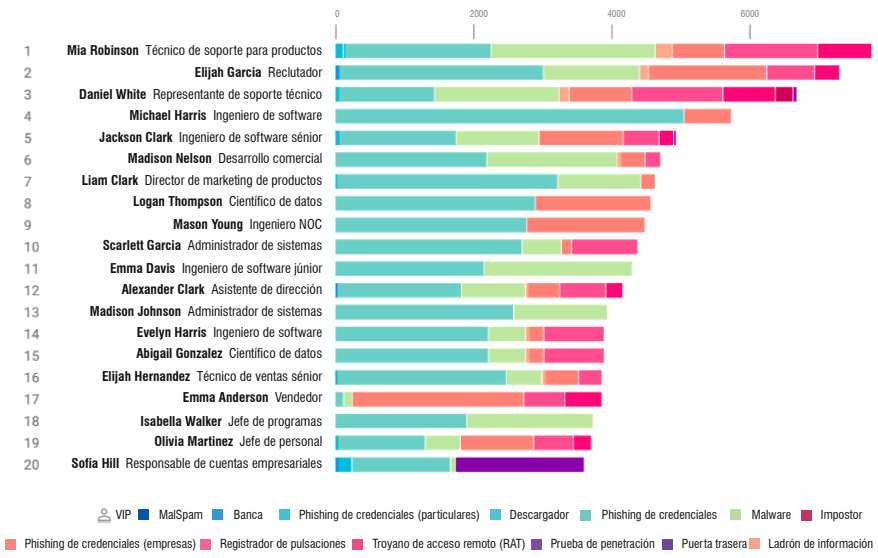
2. **Identificación de usuarios y grupos que pueden necesitar otro plan de estudio o formación, adaptado a sus necesidades.**

   Un principio fundamental de la ciberseguridad centrada en las personas es que cada usuario es diferente. En el entorno actual no funciona aplicar un mismo modelo a todo el mundo, y esto incluye los programas para concienciar en materia de seguridad.

   Los siguientes grupos pueden necesitar formación adaptada o especializada:

   - VAP**:** usuarios que plantean un riesgo elevado debido a que son particularmente vulnerables a las tácticas de los ciberdelincuentes, reciben numerosos ataques o bien tienen acceso a datos, sistemas o recursos valiosos.

Informe de VAP generado por Proofpoint Targeted Attack Protection



- VIP: altos ejecutivos, miembros de la junta directiva, gerentes y miembros destacados del personal que pueden necesitar una formación específica debido a su importancia en la organización. Muchos VIP también son VAP.
- Determinados cargos y departamentos: los empleados de los departamentos de recursos humanos, finanzas, servicios jurídicos, cumplimiento normativo, desarrollo u otros pueden necesitar formación obligatoria por ley u otra específica. A medida que avance su programa debe prever distintas evaluaciones de conocimientos y simulaciones para estos grupos.

3. **Definición de las actividades esenciales que va a incluir en su programa.**

   Un programa de formación que funcione debe tener la combinación adecuada de evaluaciones, formación, material de apoyo, comunicaciones y actividades virtuales o presenciales. A continuación se citan algunos elementos que puede considerar para su programa:

   - Evaluaciones de usuarios para medir sus conocimientos y detectar sus vulnerabilidades. Incluyen evaluaciones de conocimientos y simulaciones de ataques de phishing, USB y smishing (phishing mediante mensajes SMS/de texto).
   - Formación por ordenador diseñadas en torno a las necesidades de los usuarios y el panorama de amenazas actual.
   - Actividades de concienciación (pósteres, webinars, boletines de noticias, vídeos) para presentar los conceptos y reforzar los mensajes clave.
   - Actividades virtuales y presenciales, como cursos con almuerzo y webinars. Sea creativo. Por ejemplo, algunos de nuestros clientes han creado *escape rooms* de ciberseguridad, que dan muy buenos resultados.

4. **Pruebas y comunicación de los primeros pasos.**

   Para muchas organizaciones, un programa de formación de usuarios integral puede implicar un cambio importante. Empiece por un grupo pequeño para ir resolviendo los posibles problemas. Comunique los primeros pasos con antelación y con frecuencia a todos los participantes. Limite al máximo las sorpresas.

   Dos meses antes del comienzo

   Envíe una simulación de phishing de prueba a un pequeño grupo que esté al corriente, con el fin de descubrir cualquier problema técnico oculto. A continuación, envíe una prueba de phishing de dificultad moderada a todos los empleados para utilizarla como base de referencia.

   Por el momento, dirija a los usuarios que caigan en la trampa del phishing que ha enviado a un sitio de tipo 404 "página no encontrada". (Más adelante, dirigirá a los usuarios que hagan clic a una página de un sitio de formación).

   Un mes antes del comienzo

   Anuncie el programa a los usuarios. Si va a desplegar un add-on de denuncia de mensajes de correo electrónico, explique su finalidad y cómo utilizarlo. Y si tiene acceso a contenido, como pósteres, imágenes u otro material de concienciación sobre seguridad, colóquelo en la oficina o publíquelo en un wiki sobre su programa.

5. **Definición de la frecuencia y la programación de las actividades del programa.**

   De nuevo, la programación es crucial. Recomendamos el siguiente orden para sus actividades de concienciación en seguridad:

   - Envíe una prueba de phishing cada cuatro a seis semanas, con una combinación de distintos tipos de temas y señuelos utilizados.
   - Utilice la inscripción automática en pruebas de phishing al menos una vez cada trimestre. Utilice un módulo de formación de seguimiento dirigido, según el tipo de ataque enviado.
   - Revise los informes sobre los VAP una vez al mes o cada dos meses. Según la información que aporten, decida quién debe recibir formación dirigida y qué contenido de formación va a utilizar.
   - Asigne formación en toda la empresa al menos una vez al trimestre.
   - Repita las evaluaciones de conocimientos amplias y las pruebas de phishing al menos una vez al año para comparar los resultados con la base de referencia.
   - Para reforzar lo aprendido, programe, como mínimo dos veces al año, actividades destinadas a concienciar en seguridad, como webinars, concursos o (si es posible) actividades presenciales.

Cree un marco anual para planificar los componentes y las actividades de formación. Sea flexible para poder ajustar su planificación según cambie el panorama general de las amenazas.

Nuestro informe State of the Phish 2020 descubrió que los programas de formación para concienciar en materia de seguridad han pasado de ser anuales o trimestrales a llevar a cabo actividades todos los meses o cada dos meses. Nosotros recomendamos una sesión de formación al mes o con más frecuencia, con formación dirigida, campañas de concienciación y evaluaciones de conocimientos.

Frecuencia de la formación para concienciar en materia de seguridad

Fuente: State of the Phish 2020

Cuándo realizar un cambio

El panorama de amenazas evoluciona constantemente. Por eso nuestro programa de concienciación en seguridad necesita aplicarse de forma continua. Partiendo de la base de referencia de la evaluación inicial, las evaluaciones posteriores permiten llevar un control del nivel de conocimientos del usuario y ayudarle a planificar cómo reducir el riesgo.

El panorama de amenazas evoluciona constantemente. Por eso nuestro programa de concienciación en seguridad necesita aplicarse de forma continua.

Estas son situaciones que requieren un cambio de la frecuencia o el orden de sus actividades de formación:

- **Cuando se intensifican las amenazas específicas para un usuario o los ciberdelincuentes utilizan una marca o señuelo específico.** Modifique el contenido de la evaluación, como las plantillas de las campañas de phishing simulado, o utilice contenido de formación adaptado a las amenazas, para gestionar mejor el riesgo.
- **Si su organización sufre un incidente, como una fuga de datos.** Plantéese actualizar sus actividades planificadas y la frecuencia de la comunicación, las evaluaciones y la formación relacionadas con dicho incidente.
- **Si hay nuevas leyes o normativas que requieren más formación.** Consulte las evaluaciones de conocimientos personalizadas para ver cómo retienen los usuarios el contenido del curso.
- **Cuando su organización publica una nueva directiva o actualiza una existente y tiene dudas sobre si los usuarios la conocen.** Una evaluación de conocimientos personalizada le puede ayudar a localizar las carencias de los usuarios y a orientar sus esfuerzos de formación.
- **Si un programa de concienciación en materia de seguridad se ha interrumpido durante más de seis meses.** En este caso, tiene sentido volver a lanzar el programa para asegurarse de que los usuarios entienden su contexto y su importancia.

Nosotros no recomendamos extremar la frecuencia de las actividades de formación, ni siquiera con los empleados que suspenden sistemáticamente las evaluaciones. Una solución dirigida y razonable es realizar evaluaciones de phishing mensuales e inscribir concretamente a los usuarios que "suspenden" en una sola actividad de formación Asignarles hasta cuatro sesiones de formación les puede parecer un castigo y provocar que rechacen el programa.

Sobre todo, no intente hacerlo todo de forma inmediata. Empiece por un análisis adecuado, basado en inteligencia y en evaluaciones. A partir de ahí, extienda el programa a toda la organización para crear un plan realista que todo el personal pueda aprovechar.

SECCIÓN 3

Por qué captar el interés es fundamental

Parece evidente que la formación para concienciar en materia de seguridad es en esencia un esfuerzo centrado en las personas. Su objetivo es dotar al personal de lo necesario para reconocer los ataques que les afectan y cambiar el comportamiento de los empleados.

Por eso mantener el interés de los usuarios es clave para que el programa funcione. Pero hasta el programa mejor intencionado puede resultar tedioso si los participantes no tienen experiencias positivas y gratificantes.

Mantener el interés de los usuarios es fundamental para que el programa funcione.

Los programas que mejor funcionan:

- Emplean su marca para que los usuarios adviertan claramente su relevancia.
- Utilizan principios de aprendizaje demostrados científicamente para cambiar el comportamiento.
- Refuerzan la formación con una combinación de distinto contenido y material multimedia.
- Reclutan a los mejores profesionales en toda la organización para conseguir su apoyo y mejorar.
- Orientan a los usuarios con las dosis adecuadas de incentivos y consecuencias.

Considere estos cinco principios como la base de un marco para un programa eficaz y valorado por sus empleados. Clientes de una amplia variedad de sectores han utilizado estos conceptos para crear programas de formación que reduzcan el riesgo, recorten gastos y faciliten el cumplimiento de normativas de privacidad de los datos.

Use su marca en el programa

El nombre adecuado puede ayudar a los usuarios a entender de qué trata su programa de formación para concienciar en materia de seguridad y por qué es importante para ellos.

Por ejemplo, es posible que su organización necesite que sus empleados traten los datos de clientes de la Unión Europea conforme dicta el Reglamento general de protección de datos (RGPD). Puede que un título soso y fácil de olvidar, como "Formación para RGPD", no despierte en los usuarios el interés que necesita para inspirar cambios en el comportamiento.

Un tema más apropiado sería "Conviértase en defensor de la privacidad de los datos". Este título destaca claramente el objetivo del programa (la privacidad de los datos) y el papel del usuario (contribuyente activo al esfuerzo de privacidad).

Es posible que la cultura de su organización exija un enfoque más directo, con temas más prácticos. Incluso en estos casos, utilizar para sus programas nombres relacionados con temas concretos, como el phishing, la ingeniería social, el correo electrónico o el teletrabajo, mejora sus posibilidades.

Uso de principios de la ciencia del aprendizaje

Su programa debe aprovechar las décadas de existencia de la ciencia del aprendizaje para que la enseñanza, la retención de conocimientos y el cambio de comportamientos sean más eficaces. Un programa perfecto proporciona conocimiento conceptual, así como de procedimientos, ofreciendo a los usuarios una idea general y además, lecciones específicas. Estas técnicas tienen demostrada eficacia:

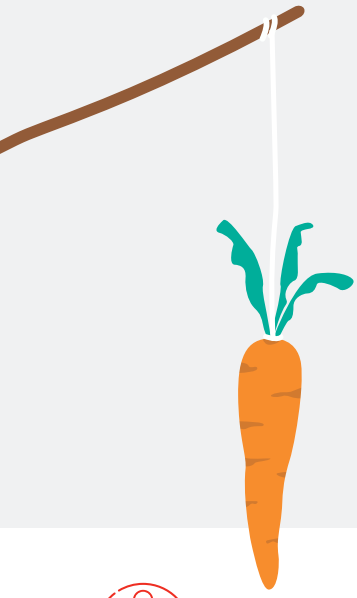
- **Ofrezca sesiones pequeñas.** Las sesiones deben durar minutos (y no horas) y centrarse en temas concretos siempre que sea posible.
- **Afiance lo aprendido.** Proporcione comentarios, y ofrezca formación y concienciación continuas.
- **Ofrezca contexto para la formación.** Asigne formación relevante para los distintos cargos y amenazas.
- **Comunique los comentarios inmediatamente.** Comunique directamente los resultados de la formación o los ejercicios de phishing.
- **Respete el ritmo de los usuarios.** Cada persona es diferente y aprende a una velocidad distinta.
- **Ilustre el contenido con casos prácticos.** Ofrezca ejemplos del mundo real.
- **Varíe los mensajes.** Los temas deben tener distintos grupos de contenido que empleen una expresión y estilo diferentes.
- **Consiga la implicación de los estudiantes.** El contenido interactivo y los ejercicios mejoran la retención.
- **Oblíguelos a reflexionar.** Los ejercicios deben poner a prueba cómo los estudiantes aplican los conocimientos.
- **Califique los resultados.** Evalúe a los estudiantes al principio y haga un seguimiento continuo de su progreso.

Ofrezca formación interesante, con contenido diverso y material multimedia

Según la "Regla de los siete", los publicistas deben presentar el mensaje al menos siete veces al cliente potencial para que cause efecto. El proceso de aprendizaje es similar.

Independientemente de la solución de formación empleada, debe ofrecer sesiones a través de varios canales y actividades. A continuación se incluyen algunos ejemplos de actividades y canales que puede utilizar.

ACTIVIDADES	CANALES
Simulaciones de ataque (phishing, USB, SMS, etc.)	Herramientas de formación para concienciar en seguridad
Evaluaciones del conocimiento	Herramientas de formación de concienciación sobre seguridad o herramienta de encuesta
Identificación y control de las personas muy atacadas (VAP)	Inteligencia sobre amenazas/puerta de enlace del correo electrónico
Formación asistida por ordenador	Módulos de formación para concienciar en materia de seguridad a través de una plataforma online u otro sistema de gestión del aprendizaje
Campañas de concienciación	Pósteres, vídeos, podcasts, webinars, oradores invitados, infografías
Ejercicios de concienciación y formación presenciales o virtuales	Almuerzos de formación, webinars, estands en eventos empresariales, turnos de palabra en eventos de empresas, formación presencial, escape rooms
Concursos/juegos	Reconocimiento del cambio de comportamiento positivo a través de un canal de la empresa, como un boletín de noticias o un wiki
Información para concienciar en materia de seguridad	Wiki, intranet o calendario de empresa compartidor
Novedades de concienciación en seguridad	Boletines de noticias de la empresa, canal de app de chat (como Microsoft Teams y Slack) o integrado en las comunicaciones de otros departamentos
Comentarios para el usuario acerca del programa de formación para concienciar en materia de seguridad	Herramienta de encuesta o buzón compartido
Informe sobre phishing de los usuarios	Solución add-on en el cliente para denuncias de mensajes de correo electrónico o buzón de correo malicioso



Si los usuarios no tienen una buena opinión de la formación para concienciar en materia de seguridad de su empresa, pueden mostrarse indiferentes o incluso negarse a realizar el curso.

Involucre a otros departamentos y empleados de puestos clave para ayudarle

El personal de seguridad de TI, marketing y recursos humanos, y los ejecutivos clave pueden desempeñar un papel importante en su programa. Aproveche su experiencia para reforzar y mejorar el enfoque, contenido y ejecución de la formación.

Otros departamentos pueden ayudar en lo siguiente:

- **Seguridad de TI** puede recomendar contenido relevante para la política corporativa (por ejemplo, sobre contraseñas). Además, los profesionales de este departamento pueden averiguar qué usuarios necesitan más formación porque reciben un mayor número de ciberataques o bien porque gestionan datos confidenciales.
- **Marketing** puede ayudar a diseñar el material de concienciación en seguridad, así como otro contenido, según los elementos de la marca de la empresa.
- **Recursos humanos** puede asesorar sobre dinámicas organizativas y proporcionar información sobre cómo trabajar con ejecutivos y jefes de las líneas de negocio.
- **Los CISO** (u otros altos ejecutivos o directivos clave) pueden comunicar y recalcar la importancia del programa.

El palo o la zanahoria: cómo orientar a los usuarios hacia un cambio de comportamiento

Si los usuarios no tienen una buena opinión de la formación para concienciar en materia de seguridad de su empresa, pueden mostrarse indiferentes o incluso negarse a realizar el curso. Hasta ahora, hemos descrito pasos que pueden ayudar a preparar el terreno para que el programa tenga buena acogida y ofrezca un valor real. Cuando se trata de elegir entre el palo o la zanahoria, la mayoría de nuestros clientes se decantan por la zanahoria.

Sin embargo, de vez en cuando, la resistencia de los usuarios exige que se utilice el palo. En estas raras ocasiones, un modelo basado en consecuencias puede ayudar a garantizar que se cumplan las normas de la formación. Aunque como último recurso, nuestros clientes han usado los siguientes modelos de consecuencias:

- Un programa de "tres errores" en el que los usuarios que hacen clic en tres mensajes de phishing simulado sufrirán una consecuencia, a una amonestación de un superior o una limitación temporal del acceso a la red o la pérdida de privilegios de acceso.
- Consecuencias como: críticas de recursos humanos, recortes del sueldo, las primas o las bonificaciones y, en casos extremos, cese laboral

Es más recomendable centrarse en los incentivos positivos y utilizar los modelos de consecuencias solamente como último recurso. Nuestros clientes consideran que un exceso de estos últimos disminuye el interés de los empleados por el programa. Sin embargo, si trabaja en un sector muy regulado o con requisitos especiales de confidencialidad, es posible que el palo sea necesario.

SECCIÓN 4

El papel fundamental de los datos

Probablemente, tras conseguir la aprobación para poner en marcha su programa de concienciación en seguridad, esté deseando comenzar con los ataques de phishing simulados y la formación para usuarios avanzados.

Pero es importante contar antes con un buen plan estratégico. Para maximizar las ventajas (reducir el riesgo para los empleados) y minimizar los costes (el tiempo de los empleados), lo primero es proporcionar conocimientos básicos, conocer las vulnerabilidades de los usuarios y centrar la formación allí donde más se necesita.

Construcción de la base

Es posible que su primer instinto como experto en seguridad sea simular ataques de phishing avanzados o formar a los usuarios para que puedan identificar las mayores amenazas que acechan a su organización. Aunque este impulso es totalmente lógico, no tendrá el impacto que espera, si los empleados no disponen de los conocimientos básicos.

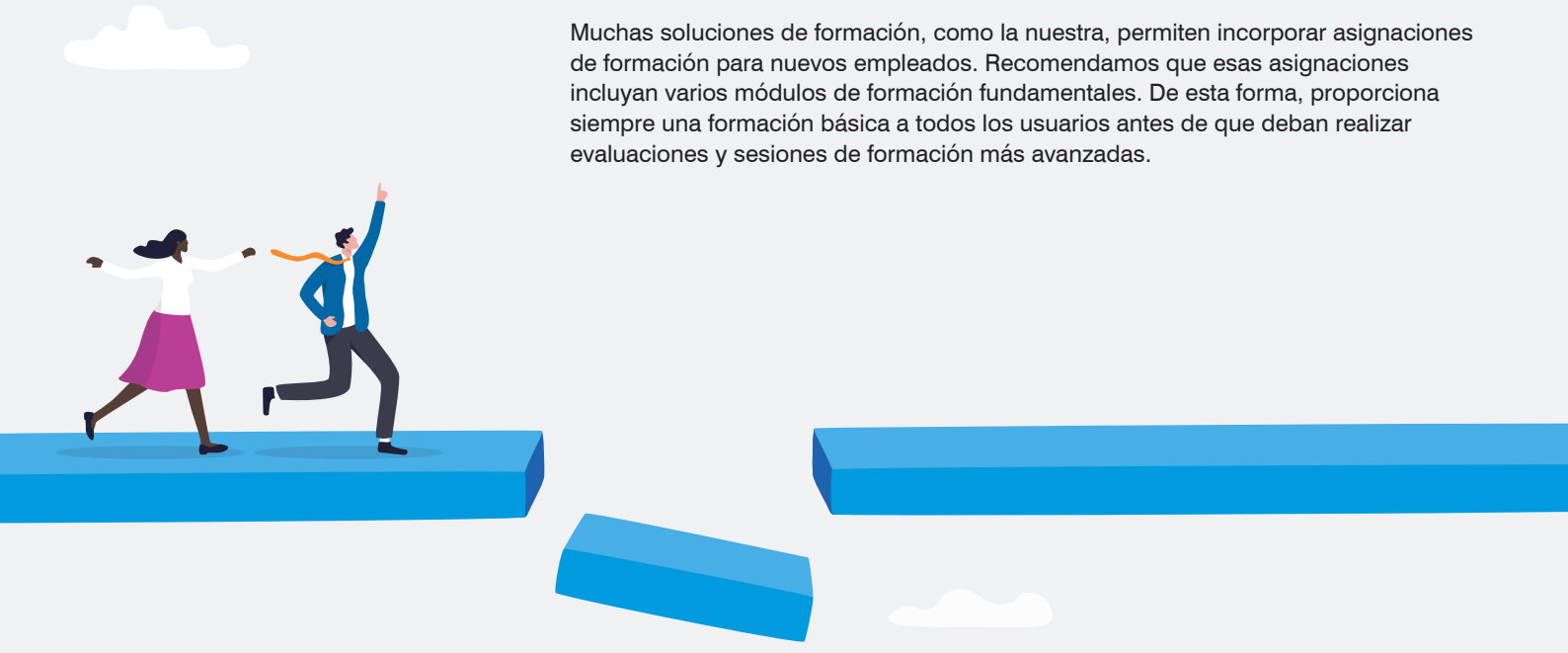
En nuestro informe State of the Phish 2020, descubrimos que muchos trabajadores no son capaces de definir términos como phishing y ransomware.

	Correcto	Incorrecto	No lo sé	
¿Qué es PHISHING?	61 %	24 %	15 %	• Solo el 49 % de los trabajadores de EE. UU. respondieron correctamente. • Los trabajadores alemanes eran los más propensos a reconocer este término (66 %).
¿Qué es RANSOMWARE?	31 %	31 %	38 %	• El año pasado, a nivel mundial, el 45 % de los trabajadores respondieron correctamente a esta pregunta. Esta caída del nivel de conocimiento podría ser una consecuencia de 2018, cuando los ataques de ransomware se redujeron de manera importante, lo que disminuyó las posibilidades de que los equipos de seguridad trataran este tema con los usuarios.

Fuente: State of the Phish 2020

Por eso recomendamos impartir una formación básica acerca de temas esenciales, como los conceptos básicos sobre seguridad y phishing, antes de evaluar o impartir formación sobre temas más avanzados.

Muchas soluciones de formación, como la nuestra, permiten incorporar asignaciones de formación para nuevos empleados. Recomendamos que esas asignaciones incluyan varios módulos de formación fundamentales. De esta forma, proporciona siempre una formación básica a todos los usuarios antes de que deban realizar evaluaciones y sesiones de formación más avanzadas.



Identificación de los usuarios vulnerables y los VAP

Con el modelo VAP descrito en la introducción, su programa debe prestar especial atención a los usuarios que suponen un riesgo elevado debido a que:

- Son especialmente vulnerables a las tácticas de ciberataque.
- Reciben numerosos ataques.
- Tienen privilegios de acceso a datos, sistemas o recursos valiosos.

(Consulte "Un modelo centrado en las personas, para medir y mitigar los riesgos asociados a los usuarios", en la página 3).

Cómo medir las vulnerabilidades, ataques y privilegios

Para descubrir las vulnerabilidades, los ataques de phishing simulados y las evaluaciones del conocimiento con preguntas son herramientas inestimables que le permiten detectar quién necesita más formación, a qué tácticas son vulnerables sus empleados y qué áreas debe proteger.

Cuantificar el riesgo de los usuarios con el modelo VAP le permite centrar su programa de formación y reducir el riesgo con más rapidez.

En el caso de los ataques, saber qué usuarios reciben un mayor número de ataques, las tácticas utilizadas y el tipo de ciberdelincuentes requiere información de la solución de inteligencia sobre amenazas que utiliza su equipo de seguridad. Nosotros identificamos a estas personas muy atacadas, o VAP, a través de Attack Index, una puntuación combinada que tiene en cuenta los siguientes factores:

- **Tipo de atacante.** El nivel de sofisticación del atacante y, a su vez, el riesgo para la organización. Por ejemplo, un atacante financiado por un estado consigue una puntuación mucho más alta que un ciberdelincuente cualquiera.
- **Tipo de objetivos.** Una forma de describir el grado de precisión del ataque. ¿Afectó la amenaza a un solo usuario o a todo el planeta? ¿Se centraba en un usuario, empresa, sector o región particular? ¿O se trataba de una campaña generalizada que afectó a medio mundo? Cuanto más dirigida sea la amenaza, mayor puntuación obtiene.
- **Tipo de amenaza.** Este componente se refiere a la clase de malware utilizado en el ataque. En la mayoría de los casos, el malware utilizado en un ataque puede revelar la gravedad de la amenaza o el grado de esfuerzo realizado por el atacante. Un troyano de acceso remoto (RAT) o un ladrón de contraseñas, por ejemplo, consigue una puntuación más alta que un intento de phishing genérico de credenciales de particulares.

Para conocer los privilegios, las organizaciones pueden comenzar por hacer un inventario de todos los recursos potencialmente valiosos a los que tienen acceso los empleados: datos, autoridad financiera, relaciones estratégicas, etc.

Lógicamente, el cargo del empleado en la empresa es un factor que cuenta a la hora de determinar y calificar sus privilegios. Pero no es el único y, con frecuencia, ni siquiera es el más importante. Un asistente de dirección puede ser más atractivo para un espía que un mando intermedio, ya que el asistente tiene acceso al calendario del CEO. De la misma forma, una enfermera de un hospital con acceso a las historias clínicas de los pacientes puede ser un objetivo más útil para los ladrones de identidades que el CEO.

Hábitos respecto a las contraseñas

utilizan un administrador de contraseñas

alternan entre 5 y 10 contraseñas distintas

introducen manualmente una contraseña distinta en cada inicio de sesión

utilizan las mismas 1 o 2 contraseñas para todas las cuentas

Fuente: State of the Phish 2020

Uso de los datos de VAP más allá de la formación

Cuantificar el riesgo de los empleados con el modelo VAP le permite centrar su programa de formación y reducir el riesgo con más rapidez. Además, puede ofrecer contexto que permita saber por qué los ciberdelincuentes dirigen los ataques a esos usuarios. Con esta información, puede vigilar más de cerca a estos usuarios y a otros con cargos similares, y desplegar controles adaptables, como aislar la actividad del navegador o incrementar los requisitos de autenticación, según las necesidades.

La combinación de todos estos datos con la inteligencia sobre amenazas, incluida la detallada información que proporciona una herramienta como Proofpoint Targeted Attack Protection (TAP), ofrece una mejor idea sobre si los empleados reciben contenido malicioso.

Es útil saber si los usuarios hacen clic en mensajes de phishing simulado e incluso es más importante averiguar si hacen clic en contenido malicioso real, aunque el clic esté bloqueado. Estos datos ponen de relieve los riesgos y lagunas de protección potenciales.

Más allá del phishing: otros temas de seguridad sensibles

El phishing es el tema más recurrente en la formación para concienciar en materia de seguridad. Sin embargo, centrar su programa solamente en las amenazas por correo electrónico puede dejar brechas en otras áreas muy importantes.

Plantéese utilizar una evaluación de conocimientos de amplio alcance para descubrir qué saben sus empleados sobre temas de ciberseguridad y sobre las políticas o normas de su organización.

Nuestro informe State of the Phish 2020 desveló varios comportamientos de riesgo. Estas son solo algunas de las conclusiones:

- El 45 % de los empleados admiten utilizar las mismas contraseñas para varias cuentas.
- Solo el 49 % protegen con contraseña sus redes Wi-Fi domésticas.
- El 26 % creen que se pueden conectar con seguridad a una red Wi-Fi gratuita en un lugar de confianza (como una cafetería o un aeropuerto).
- El 17 % no están seguros de si las redes de acceso abierto de estos lugares son seguras.

Estos comportamientos exponen a su organización a un grave riesgo. Diversificar su programa para abordar estas y otras áreas de vulnerabilidad potenciales puede reducir su nivel de exposición.

Cuando trate estos temas, utilice casos reales y ejemplos auténticos. Los detalles relevantes y concretos ayudan a los usuarios a entender cómo trabajan los ciberdelincuentes y por qué es importante.

Un programa ágil

Cada organización tiene un panorama de amenazas, una base de usuarios y una cultura de conciencia sobre seguridad propios. Y tan importante como planificar con antelación es la agilidad.

Un programa ágil se adapta a los cambios de circunstancias, para dirigir la formación específicamente a los empleados adecuados en el momento oportuno. De esta forma, será un programa global, eficaz y eficiente. Además, ayudará a reducir el riesgo para los usuarios, aprovechando al máximo las escasas una o dos horas al año que la mayoría de las empresas pueden dedicar a la formación para concienciar en materia de seguridad.

Los programas más eficaces ofrecen ejercicios de formación que reflejan las amenazas reales y potenciales. Adapte su programa a medida que cambien las circunstancias. La vida es imprevisible y hay cambios repentinos que pueden generar lagunas de conocimientos y riesgos para los usuarios.

A continuación se citan algunos ejemplos de situaciones en las que puede cambiar su plan según las necesidades o al descubrir nuevas vulnerabilidades:

- Las evaluaciones de phishing muestran que los usuarios reconocen los ataques basados en enlaces, pero no detectan los que emplean archivos adjuntos.
- Su organización ha recibido un gran volumen de ataques BEC.
- Su equipo de seguridad del correo electrónico ha observado que los ciberdelincuentes utilizan un tipo de phishing o de ataque concreto.
- En sus evaluaciones de conocimientos, advierte que un departamento específico tiene problemas con un tema determinado.

Automatización de la formación de seguimiento

Automatizar estos esfuerzos puede agilizar aún más el programa. Por ejemplo, nuestros clientes utilizan la función de inscripción automática de nuestra solución para asignar automáticamente sesiones de formación en función de cómo responden los usuarios ante los ataques simulados y las evaluaciones de conocimientos. Esta función ofrece formación a los usuarios que más la necesitan, pero no les obliga a realizarla en ese momento preciso.

El seguimiento automatizado es una buena forma de adaptar la formación a las vulnerabilidades y carencias reales, en lugar de asignar la misma formación a todos los usuarios en un enfoque global. La formación dirigida ahorra tiempo a los usuarios y facilita la incorporación de otras personas interesadas.

Posibilidad para los usuarios de ponerse a prueba

Otra forma de adaptar la formación es permitir que los usuarios demuestren que conocen los conceptos de ciberseguridad y que tienen un buen comportamiento. Si los usuarios han realizado la formación básica, siempre rechazan (o denuncian) los ataques de phishing simulados y obtienen buenos resultados en las evaluaciones de conocimientos, es posible que necesiten menos formación general.

La opción de poder demostrar sus conocimientos puede ayudar a los usuarios a aceptar la formación y ofrecerles un incentivo para participar más activamente en las evaluaciones.

SECCIÓN 5

Los parámetros que importan: la medida del éxito

Si tiene en marcha un programa para concienciar en seguridad, probablemente ya conoce la tasa de clics, también conocida como tasa de fallos. Es la primera y principal estadística que nos transmiten los clientes que intentan medir la efectividad de su programa. Y, sin lugar a dudas, es un parámetro importante.

Tasa de denuncias

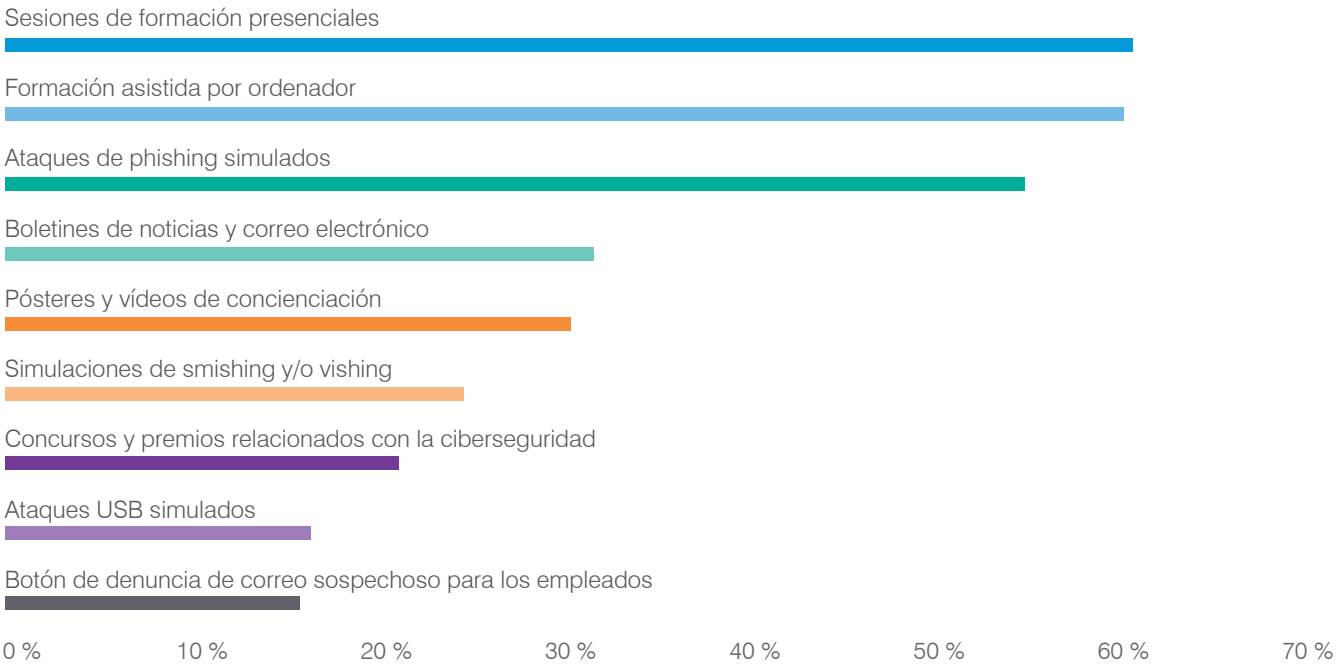
Sin embargo, no es el único factor que debe controlar. Cuantificar el porcentaje de mensajes de correo electrónico que los usuarios denuncian de forma activa (ya sean reales o simulados) ofrece información clave.

Los add-on de denuncias de mensajes de correo electrónico permiten a los usuarios alertar fácilmente a su equipo de seguridad si detectan mensajes sospechosos. Estas herramientas también miden cuántos usuarios que reciben mensajes de phishing simulado lo denuncian, lo que se conoce como tasa de denuncias.

Desafortunadamente, según nuestra encuesta de State of the Phish 2020, solo el 15 % de las organizaciones utilizan estas herramientas en su programa para concienciar en seguridad.

Nuestros datos ponen de manifiesto que varían más las tasas de denuncias que las tasas de clics, lo que indica que esta última es un mejor indicador general del cambio de comportamiento.

Herramientas que usan las organizaciones en sus programas*



* Se admiten varias respuestas.

Fuente: State of the Phish 2020

Niveles de conocimientos

Otro dato importante es el nivel de conocimientos. La tasa de clics y la tasa de denuncias pueden medir la resistencia de los usuarios ante los ataques de phishing. Pero las evaluaciones de conocimientos miden cuánto saben de otros temas, como la privacidad de los datos, las contraseñas y la seguridad para móviles.

Por ejemplo, es posible que las empresas o departamentos sometidos a muchas normativas necesiten formación específica. Es fundamental conocer el nivel de conocimientos de los usuarios y saber si está mejorando o empeorando.

Medición de las tasas de clics y de denuncias

Si envía un mensaje de phishing simulado, ¿qué se considera una "buena" tasa de clics? La respuesta depende de dos factores principales:

- El nivel de dificultad y focalización del mensaje de phishing simulado.
- La experiencia que tienen sus empleados.

En general, las tasas de clics (o tasas de fallos) inferiores al 5 % se consideran buenas. Pero una valoración más precisa requiere su en comparación con la tasa media de fallos (del inglés, AFR) de muchas otras organizaciones.

Proofpoint, junto con muchos otros proveedores, ofrece la AFR de distintas plantillas de phishing simulado. Como se muestra en esta captura de pantalla, una tasa de fallos del 5 % refleja un resultado peor que la media para algunas plantillas.

En general, las tasas de clics (o tasas de fallos) inferiores al 5 % se consideran buenas.

Comparación de la tasa media de fallos de nuestro producto ThreatSim® *(en verde)*.

Jump in this quick meeting	Corporate	8%
FREE GDPR Readiness Tools - Targets Legal or HR	Commercial	3%
College Admissions Help	Consumer	2%
Online dating - Message waiting	Proofpoint - Consumer	5%

Por eso, comparar sus resultados con estas AFR proporciona una mejor información del nivel de concienciación sobre phishing de los usuarios. Las AFR pueden cambiar con el tiempo a medida que haya más organizaciones que utilicen determinadas plantillas.

En el caso de las tasas de denuncias (los usuarios que reconocen un mensaje de phishing simulado y lo denuncian), el valor recomendado es un 70 %. Algunos de nuestros clientes consiguieron tasas de denuncias superiores al 80 %, junto con una tasa de fallos baja.

Uno de nuestros clientes ahorró

345 000 $

en gastos de personal mediante el empleo de un componente de nuestra solución CLEAR.

Cómo medir el efecto

Los parámetros para medir el nivel de concienciación en seguridad son importantes y deben ser accesibles en su software. Sin embargo, el verdadero objetivo de todo programa de concienciación en materia de seguridad es reducir el riesgo para el usuario.

En este sentido, los parámetros externos pueden ayudar a evaluar y demostrar el valor de su programa. Parámetros de medición destacados:

- Número de infecciones de malware y reparación de equipos de usuarios
- Tiempo y recursos gastados en la gestión de buzones de correo malicioso
- Número de ataques de phishing desconocidos que consiguen su objetivo
- Horas de inactividad de los empleados

Estos parámetros pueden ayudarle también a conseguir la aceptación continua de su programa por parte de personas clave. Uno de nuestros clientes ahorró 345 000 dólares en gastos de personal mediante el empleo de un componente de nuestra solución Closed-Loop Email Analysis and Response (CLEAR). Puede leer sobre este tema en el informe de "The Total Economic Impact Of Proofpoint Advanced Email Protection" (El impacto económico total de la protección avanzada del correo electrónico de Proofpoint).

Uso de sus datos para cambiar la conversación

Muchos de los parámetros empleados para calificar la formación sobre concienciación en seguridad, como "tasa de fallos", tasa de clics", etc., pueden tener connotaciones negativas y resaltar los errores, en lugar de los hitos conseguidos. Otros, como las tasas de denuncias y los niveles de conocimientos, destacan los comportamientos positivos, en lugar de los negativos. Además, muestran mejor cuál es el resultado de los usuarios que actúan como línea de defensa frente a los ataques dirigidos actuales.

Utilice estos datos para ilustrar cómo los usuarios mejoran el estado de seguridad de su organización. Suponga que un empleado denuncia un mensaje malicioso real y que su equipo de respuesta a incidentes ha podido eliminarlo antes de que pusiera en riesgo a su organización. Este tipo de casos pueden ayudarle a vender su programa internamente ante las personas clave y a mejorar la cultura de seguridad en su empresa.

SECCIÓN 6

Más allá de la formación: cómo instaurar una cultura de seguridad

Aproximadamente el 99 % de las organizaciones afirman proporcionar formación de concienciación sobre phishing a sus empleados[2]. Sin embargo, el 43 % reconoce que solamente forman a parte de sus usuarios. No sorprende que el phishing siga siendo el tipo de amenazas con más probabilidades de provocar una fuga de datos.

¿Qué podemos mejorar? La respuesta está en desarrollar una cultura de seguridad sistemática, sostenible y personalizada, una cultura que cale en la organización en su conjunto, en todos los usuarios y actividades digitales.

Este enfoque requiere una inversión concertada de tiempo, esfuerzo, recursos, y aceptación en toda la empresa. Pero los resultados pueden ser inestimables. Una cultura de seguridad robusta puede mejorar el nivel de seguridad, el cumplimiento y los resultados empresariales de su organización. Elaborada de manera adecuada, puede incluso elevar la moral y la productividad de los empleados.

2 Proofpoint. "State of the Phish 2022", febrero de 2022.

¿Qué es una cultura de seguridad?

Según Keman Huang y Keri Pearlson, investigadores de la MIT, una cultura de seguridad es el conjunto de "creencias, valores y actitudes que motivan un comportamiento de los empleados de protección y defensa de la organización frente a ciberataques"[3].

En otras palabras, los empleados (todos los empleados) son agentes activos en la defensa de los datos, los sistemas y los recursos de la organización.

Para instaurar una cultura de seguridad, necesita cambiar la percepción que tienen de ella sus empleados. Una cultura de seguridad deber formar parte del ADN de su cultura corporativa. Debe inspirar, y perdurar.

Qué conforma una cultura

Una cultura de ciberseguridad cuenta con tres factores sobrepuestos:

- **Responsabilidad respecto a la ciberseguridad.** Los empleados sienten que ellos y sus compañeros son responsables de actuar para impedir incidentes de seguridad.
- **Comprensión de la importancia de la ciberseguridad.** Los empleados son conscientes de que las ciberamenazas constituyen un riesgo material para el éxito de la organización y de que podrían afectarles personalmente.
- **Capacidad para actuar.** Los empleados se sienten empoderados gracias a sus conocimientos de ciberseguridad, deben tener la seguridad de que conocen la política de seguridad y la confianza en que la organización les apoyará si cometen un error de seguridad no intencionado.

Características una cultura de seguridad robusta

Una cultura de seguridad robusta:

- **Es holística y continua.** Una cultura de seguridad necesita ir más allá de la formación y las simulaciones de phishing esporádicas. El objetivo es elevar la moral y con el fin de crear una plantilla más comprometida y segura. Puede hacerlo de muchas maneras: una cultura de seguridad promueve el aprendizaje y la concienciación a través de contenido relevante y personalizado, y de actualizaciones del cambiante panorama de amenazas. Los usuarios reciben mensajes de correo electrónico y otros recordatorios que ayudan a los empleados a comprender por qué forman parte del programa y cómo les ayuda tanto a nivel profesional como personal. Y se les anima a denunciar con confianza las actividades sospechosas.
- **Tiene defensores transversales.** El apoyo va de los ejecutivos a la dirección pasando por los usuarios finales. Además del cuerpo directivo, otros defensores pueden ser los departamentos de seguridad, tecnología de la información, RR. HH., cumplimiento y relaciones públicas[4].
- **Crea expectativas y las mantiene.** Esto implica la elaboración y aplicación de políticas de seguridad que impulsen pautas culturales.

3 Keman Huang and Keri Pearlson (MIT). "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture" (Lo que la tecnología no puede solucionar: instauración de un modelo de cultura de ciberseguridad empresarial), enero de 2019.

4 SANS Institute. "2021 Security Awareness Report: Managing Human Cyber Risk" (Informe 2021 sobre concienciación en seguridad: gestión de ciberriesgos asociados a las personas), Noviembre de 2021.

Las ventajas

Una cultura de seguridad sólida puede contribuir a la misión de la organización y proporcionar ventajas significativas y cuantificables. Estos son solo algunos ejemplos:

Mayor agilidad y resiliencia

Una cultura de seguridad anima a los usuarios a identificar amenazas potenciales. También permite a los equipos de seguridad reaccionar ante las amenazas y neutralizarlas antes. La agilidad y la resiliencia aumentan cuando los usuarios están inspirados, comprometidos y se apoyan entre sí para conseguir un efecto de red. Las ventajas se extienden por toda la organización.

Reducción de riesgos para la organización

Vivimos en una era de plantillas remotas e híbridas, la nube y dispositivos personales. Y, por lo general, esto quiere decir que los riesgos se multiplican. Una cultura de seguridad robusta puede garantizar la tranquilidad de los directivos, y permitirles centrarse en otras áreas de negocio.

Cumplimiento sin complicaciones

El cumplimiento de las normativas estatales, los estándares de la industria y las políticas de seguridad internas será más fácil. Esto reduce las probabilidades de recibir multas y otras sanciones.

Ventaja competitiva

Los clientes y partners elegirán su empresa frente a la competencia si tienen la sensación de que hacer negocios con usted es más seguro. Promueva la seguridad como valor fundamental.

Obstáculos habituales

Las organizaciones gastan millones en herramientas de seguridad, servicios y personal. Sin embargo, incluso con esas inversiones, muchos siguen ignorando su principal factor de riesgo: las personas.

Neutralizar el factor humano es la medida de seguridad más importante que se puede adoptar. También es una de las que resulta más complicada. Las actividades de concienciación pueden parecer molestas. Algunos empleados tienen la sensación de que se interponen en su trabajo "real". Muchos se resisten a las exigencias adicionales, como la denuncia de mensajes sospechosos o la asistencia a webinars de formación. Y el personal técnico y de RR. HH. puede tener reparos a la hora de poner en práctica una cultura de seguridad porque no están equipados para instaurarla y mantenerla.

Los desafíos son los siguientes:

- Vender la idea a la alta dirección
- Cuantificar de manera convincente la rentabilidad de la inversión
- Convencer a los usuarios de que la formación y concienciación en seguridad son positivas y conseguir que formen parte activa
- Cambiar el comportamiento de los usuarios

Hacerlo realidad con el marco ACE

La motivación es fundamental para generar una sólida cultura de seguridad, e intervienen tres ingredientes principales. El primero es la autonomía. Esto significa convertir el aprendizaje en una experiencia personalizada y autónoma para cada usuario. El segundo es la maestría. Esto significa dotar a los usuarios con las herramientas y el tiempo que necesitan para progresar y alcanzar un buen nivel de conocimientos y habilidades en ciberseguridad. Y el ingrediente final es el propósito. Esto significa dar a los usuarios la sensación de que forman parte de una misión más importante que ellos mismos.

Uso del marco ACE

A continuación incluimos tres pasos que puede adoptar para contribuir a instaurar una cultura de seguridad sostenible. Se trata de un proceso continuo con tres elementos al que llamamos marco ACE.

A Analizar vulnerabilidad de los usuarios

Cada organización es diferente, con riesgos y prioridades de seguridad exclusivos.

Pregúntese lo siguiente:

- ¿Qué saben los usuarios?
- ¿Quién es objeto de ataques? ¿Con qué tipo de ataques?
- ¿Qué harían los usuarios si tuvieran que enfrentarse a amenazas?
- ¿Qué creen? ¿Qué piensan de la ciberseguridad?

Gracias al análisis de estas y otras preguntas podrá determinar dónde están las vulnerabilidades.

C Cambiar comportamientos

Crear una cultura de seguridad es un proceso continuo, y no un evento puntual. Adopte una estrategia holística.

Eso significa ponerse en contacto con los empleados con regularidad a través de múltiples canales de comunicación. Estos podrían incluir boletines de noticias, artículos de blog internos y actualizaciones sobre las últimas amenazas y vectores de ataque.

Ofrezca una amplia variedad de contenido y personalícelo. Todo el mundo es distinto y reacciona y aprende de manera diferente. No olvide resaltar de manera constante la importancia de la seguridad de una forma positiva,

E Evaluar el progreso y medir el éxito

Comparta los indicadores que muestran el progreso, la mejora continua y la rentabilidad. Estas medidas validan su inversión, demostrando el valor de una cultura de seguridad para la dirección y la organización en su conjunto.

Aproveche la menor ocasión. Después de un ataque, demuestre de qué forma una cultura más robusta de la seguridad habría permitido reducir el tiempo, el dinero y el esfuerzo necesarios para resolver un incidente, o sencillamente ayudado a la organización a evitarlo.

Hay muchas formas de medir el nivel de concienciación en seguridad de su organización, para que pueda determinar cómo ha cambiado la cultura de seguridad el comportamiento de los usuarios.

Concretamente:

- Tasas de clic de sus usuarios más vulnerables
- Tasas de denuncias en simulaciones de ataques de phishing
- Precisión con la que los usuarios pueden identificar amenazas reales

Por qué es importante

La instauración de una cultura de seguridad sólida y continua beneficia absolutamente a todos los usuarios, desde los directivos y ejecutivos al equipo de seguridad, los jefes de departamento y los usuarios.

Sin embargo, no existe un modelo universal. Cada organización tiene una personalidad diferente y unas necesidades únicas. Algunas de estas diferencias tienen que ver con la empresa. Otras con el sector. Y cada cultura a su vez vienen impulsada por una amplia variedad de factores internos y externos.

Mediante la instauración y mantenimiento de un programa que consiga la aprobación de todos los niveles, la concienciación en seguridad queda arraigada en los valores fundamentales de su organización. Para crear una verdadera cultura de seguridad no basta con una sesión puntual de formación en seguridad. Se trata de una mentalidad que fundamenta las actividades profesionales y personales del día a día.

Esta sección es una introducción general a la instauración de una cultura de seguridad.

Fara obtener más información sobre las culturas de la seguridad y el marco ACE, descargue nuestro libro electrónico *Más que formación de concienciación: instauración de una cultura de seguridad sostenible, y su importancia*

SECCIÓN 7

Conclusiones y recomendaciones

El objetivo de su programa de formación para concienciar en materia de seguridad debe ser cambiar los comportamientos más relevantes para la misión de su organización.
Para conseguirlo, la mejor solución consiste en combinar formación general y dirigida que responsabilice a los usuarios mediante consejos prácticos.

Si aún no ha adoptado un enfoque centrado en las personas para su formación de concienciación en materia de seguridad, ha llegado el momento de comenzar. Estos son los cinco pilares de un programa eficaz y eficiente:

Las personas son la prioridad

Cualquier empleado de su organización puede ser un posible objetivo. En cualquier momento, cualquier persona de su organización puede mejorar o dañar su nivel de seguridad.

La formación para concienciar a sus empleados en materia de seguridad es una de las medidas más importantes que puede aplicar para proteger a su empresa. Cuando los usuarios sepan reconocer, rechazar y comunicar los intentos de phishing, habrá creado una última línea de defensa contra las mayores ciberamenazas actuales.

Planifique el despliegue

Cada organización es diferente y no habrá dos programas de formación iguales, pero como se describe en la sección 2, el suyo debe incluir los siguientes elementos:

- Definición de las necesidades de formación
- Identificación de los usuarios que tienen necesidades de formación concretas
- Definición de actividades
- Creación y administración de calendarios
- Comunicación y prueba de los primeros pasos
- Definición de la frecuencia y la distribución de las actividades del programa

El éxito de su programa depende en gran medida de su planificación y diligencia.

Implique a sus empleados

Mantener el interés de los usuarios es fundamental para que el programa funcione. Pero hasta el programa mejor intencionado puede resultar tedioso si los participantes no tienen experiencias positivas y gratificantes.

Los programas que mejor funcionan:

- Emplean su marca para que los usuarios adviertan su relevancia claramente.
- Utilizan principios de aprendizaje demostrados científicamente para cambiar el comportamiento.
- Refuerzan la formación con una combinación de distinto contenido y material multimedia.
- Reclutan a los mejores profesionales en toda la organización para conseguir su apoyo y mejorar.
- Orientan a los usuarios con las dosis adecuadas de incentivos y consecuencias.

Use datos para identificar a los usuarios vulnerables, ofrecer formación dirigida y garantizar la agilidad

Sus primeros pasos deben ser proporcionar conocimientos básicos, conocer las vulnerabilidades de los empleados y dirigir la formación donde más se necesita. En ese sentido, los ataques de phishing simulados y las evaluaciones de conocimientos con preguntas ofrecen información valiosísima sobre dónde concentrar los esfuerzos de formación. La inteligencia sobre amenazas que proporciona información de los ataques a los que se enfrentan sus empleados también puede ayudar a adaptar el contenido de la formación a las amenazas del mundo real. Y saber qué usuarios tienen acceso a los datos más confidenciales de la organización le puede ayudar a personalizar la formación y aplicar otros controles de seguridad a los usuarios con más privilegios.

Las opciones de formación de seguimiento y la posibilidad de rechazarla para usuarios con experiencia y de bajo riesgo le permiten mantener la agilidad a escala.

Mida el éxito del programa con parámetros internos y externos

Las tasas de clics (o las tasas de fallos) para los mensajes de phishing simulados son importantes. Pero las tasas de denuncias pueden ser un indicador incluso mejor de la resiliencia de los empleados ante los ataques.

Las evaluaciones de conocimientos pueden medir su nivel de conocimiento de otros temas.

Finalmente, los parámetros externos, como las infecciones de malware y el tiempo de inactividad, muestran el efecto y el valor de su programa.

Estos parámetros pueden ayudarle también a conseguir la aceptación continua de su programa por parte de personas clave. Utilice estos datos para destacar cómo los usuarios mejoran el estado de seguridad de su organización. Estas métricas no solo le ayudarán a promover mejor su programa internamente, sino impulsar la cultura de seguridad en su empresa.

Más información

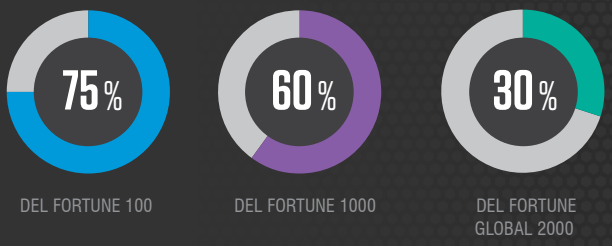
Para obtener más información sobre el conocimiento de ciberseguridad de sus usuarios, sus puntos fuertes y débiles, y cómo puede impulsar un cambio de comportamiento, realice nuestra Evaluación de riesgos del personal en proofpoint.com/es/people-risk-assessment.

Por qué Proofpoint

A diario, analizamos más de:

2600 MILLONES DE MENSAJES DE CORREO	**49 000 MILLONES** DE URL	**1900 MILLONES** DE ADJUNTOS
1700 MILLONES DE MENSAJES DE MÓVIL	**430 MILLONES** DE DOMINIOS WEB	**143 000** CUENTAS DE REDES SOCIALES

Confían en nosotros más de:



DEL FORTUNE 100 | DEL FORTUNE 1000 | DEL FORTUNE GLOBAL 2000

8000 GRANDES EMPRESAS

200 000 PEQUEÑAS EMPRESAS

MÁS INFORMACIÓN

Para obtener más información, visite **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**.

proofpoint.

0504-001-06-02 10/22