proofpoint.

SUITE DE FORMACIÓN SOBRE ANTIPHISHING DE PROOFPOINT

VENTAJAS PRINCIPALES

- Cambio del comportamiento de los usuarios para reducir los riesgos asociados a los ataques de phishing y ransomware.
- Priorización y mejora de la respuesta a incidentes.
- Formación multilingüe y coherente en todo el mundo.
- Seguimiento de los resultados y el progreso, con informes en tiempo real.

Los líderes en seguridad y sus equipos son conscientes de las dificultades para reducir los ataques de phishing y ransomware. Las protecciones técnicas no pueden impedir todos los ataques contra los usuarios, son incapaces de evitar errores humanos, y no ofrecen las ventajas a largo plazo que aporta una formación eficaz para concienciar en materia de seguridad.

La formación continua produce resultados cuantificables. Nuestra suite de formación antiphishing combina exámenes, educación, refuerzo y evaluación, y puede utilizarse junto con nuestra metodología de formación continua, que ofrece resultados demostrados líderes del sector. Se trata de la mejor solución posible si su principal interés es garantizar la capacidad de los usuarios para defenderse ante los ataques de phishing.

SIMULACIONES DE PHISHING DE THREATSIM

Nuestras simulaciones de phishing ThreatSim® le ayudan a conocer el nivel de vulnerabilidad de su empresa ante una variedad de ataques de phishing y de phishing selectivo (spearphishing). Con miles de plantillas de phishing diferentes de 13 categorías distintas, puede evaluar la respuesta de los usuarios ante distintos tipos de amenazas, como:

- Adjuntos maliciosos
- Enlaces incrustados
- Solicitudes de datos personales

Añadimos nuevas plantillas todos los meses. Nuestras plantillas de phishing de ThreatSim se crean a partir de la inteligencia de amenazas de Proofpoint; otras reflejan peticiones de los clientes o temas que dependen de la época del año.

Los usuarios que caen en la trampa de un ataque simulado reciben formación que denominamos "enseñanza a tiempo" (o "just-in-time teaching"). De esta forma, aprenden el objetivo del ejercicio, los peligros de los ataques reales y cómo evitar en el futuro caer en la trampa. También puede ayudar a sus usuarios más vulnerables asignando de forma automática formación interactiva a todo el que se deje engañar por el phishing simulado.

MÓDULOS DE FORMACIÓN INTERACTIVOS

Nuestros módulos de formación interactivos ofrecen a los usuarios ejercicios prácticos para que reconozcan y eviten los ataques de phishing y otros timos de ingeniería social. Ofrecemos una combinación de módulos basados en juegos y casos reales. Puede incluso personalizar el contenido al principio y final de cada módulo.

Los módulos de formación, optimizados para móviles y disponibles bajo demanda, cumplen la norma sobre accesibilidad Sección 508 de Estados Unidos y el estándar Web Content Accessibility Guidelines (WCAG) 2.0 AA. La duración de cada módulo es de entre 5 y 15 minutos.

La suite de formación sobre antiphishing incluye ocho módulos de formación distintos:

Módulo de formación	Descripción
Seguridad del correo electrónico	Enseña a los usuarios a identificar y evitar: • Contenido manipulado • Enlaces maliciosos y falsificados • Archivos adjuntos no seguros • Peticiones de datos inapropiadas
Anti-Phishing Phil	Módulo basado en un juego que enseña a los usuarios a detectar ataques de phishing mediante la identificación de direcciones URL fraudulentas.
Anti-Phishing Phyllis	Módulo que enseña a los usuarios mediante un juego a reconocer los mensajes de correo electrónico de phishing mediante la identificación de las señales de peligro.
Protección del correo electrónico - Serie básica	Incluye los cuatro minimódulos siguientes, que le permiten ofrecer cursos breves, pero prácticos, que abordan riesgos específicos para los usuarios del correo electrónico: • Introducción al phishing • Cómo evitar enlaces peligrosos • Cómo evitar los archivos adjuntos peligrosos • Phishing de introducción de datos
Protección del correo electrónico - Serie avanzada	Basada en la serie "Protección del correo electrónico - Serie básica", incluye estos tres módulos muy especializados sobre amenazas del correo electrónico sofisticadas: • Herramientas de protección del correo electrónico • Seguridad del correo electrónico en dispositivos móviles • Amenazas de phishing dirigido
Protección frente al ransomware	Proporciona cursos breves, pero completos sobre cómo reconocer e impedir los ataques de ransomware. Los usuarios aprenden también a aplicar las mejores prácticas a otras amenazas de phishing y malware.
Ingeniería social	Va más allá de la amenaza del phishing y explica los peligros asociados al smishing, el vishing, las redes sociales y los ataques en persona. Los usuarios también aprenden a detectar técnicas y trampas habituales de ingeniería social.
Formación sobre direcciones URL	Explica cómo se crean las direcciones de Internet (URL), las señales de alerta más frecuentes, y cómo identificar y evitar los enlaces maliciosos.

PHISHALARM Y PHISHALARM ANALYZER (MÓDULOS OPCIONALES)

PhishAlarm® es un complemento para cliente de correo electrónico que permite a sus empleados denunciar los mensajes sospechosos con un solo clic. Los usuarios que denuncian el correo electrónico sospechoso ven inmediatamente un mensaje emergente o de correo electrónico de agradecimiento. PhishAlarm® Analyzer ordena los mensajes comunicados según la prioridad y mejora la respuesta a incidentes, para que los administradores puedan revisar rápidamente los detalles más importantes, tomar una decisión y actuar. Juntas, estas herramientas pueden reducir las posibilidades de riesgo en relación a los ataques de phishing activos.

INTELIGENCIA EMPRESARIAL SOBRE EL RIESGO DE LOS USUARIOS

Evalúe y analice los resultados. Tendrá acceso a una gran variedad de informes detallados que le proporcionan información amplia y detallada de los resultados de sus evaluaciones y cursos de formación. Como administrador, puede ver todos los detalles de los principales atacantes y los reincidentes, y descubrir qué elementos didácticos son más eficaces. Esto le ayuda a planificar las medidas con eficacia y a abordar las áreas de vulnerabilidad.