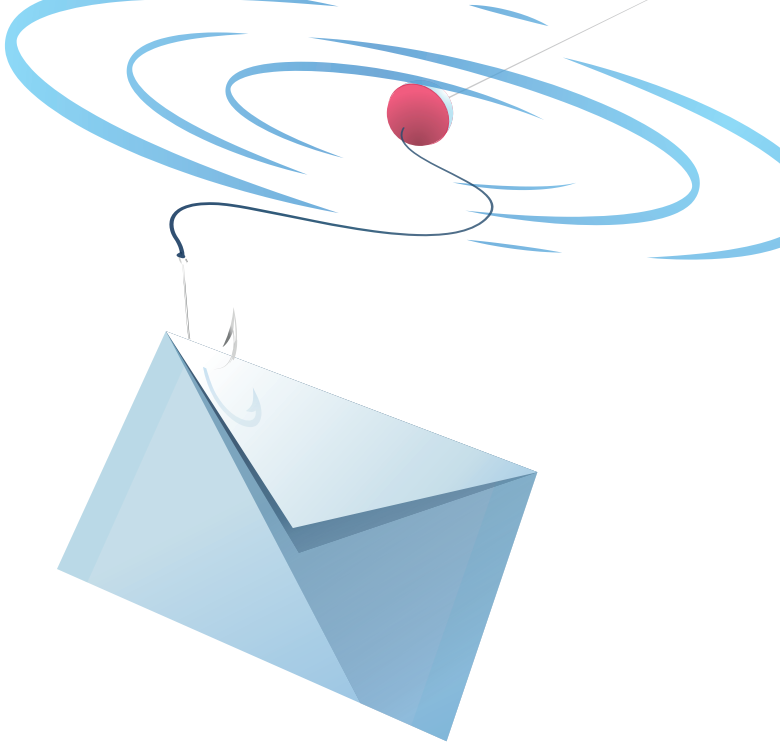
SOPHOS



No pique

El phishing es un gran negocio. Que no le pesquen.

Los ataques de phishing han crecido de forma meteórica durante el último año, debido a que los atacantes no dejan de refinar sus tácticas y, además, porque comparten los tipos de ataque que tienen éxito. Particularmente, están aprovechando la oferta de malware como servicio en la Web Oscura para aumentar la eficiencia y el volumen de sus ataques. De hecho, el 41 % de las empresas ya informan de ataques de phishing por lo menos una vez al día.[1]

En este informe nos sumergimos en la evolución reciente del phishing, cómo funciona y cómo se presenta. Y en tanto que los ciberdelincuentes seguirán acechando a los empleados sirviéndose de su tecnología, desarrollaremos aquí la importancia que tiene usar una defensa de varias capas contra los ataques de phishing mediante la combinación de avanzadas tecnologías de seguridad con empleados formados y concienciados sobre el phishing.

Más que spam molesto

Tradicionalmente, el phishing se asociaba a los delitos cibernéticos relacionados con la banca online: los malhechores envían un correo electrónico que engaña al usuario para que visite un sitio web que es un clon visual de la página de inicio de su banco, a fin de apoderarse de sus credenciales a través de un formulario falso.

Pero el phishing es mucho más que sitios de banca falsos y enlaces a pastillas milagrosas o entregas de paquetería; en realidad es un anzuelo esperando a que pique para entregarles información útil y valiosa.

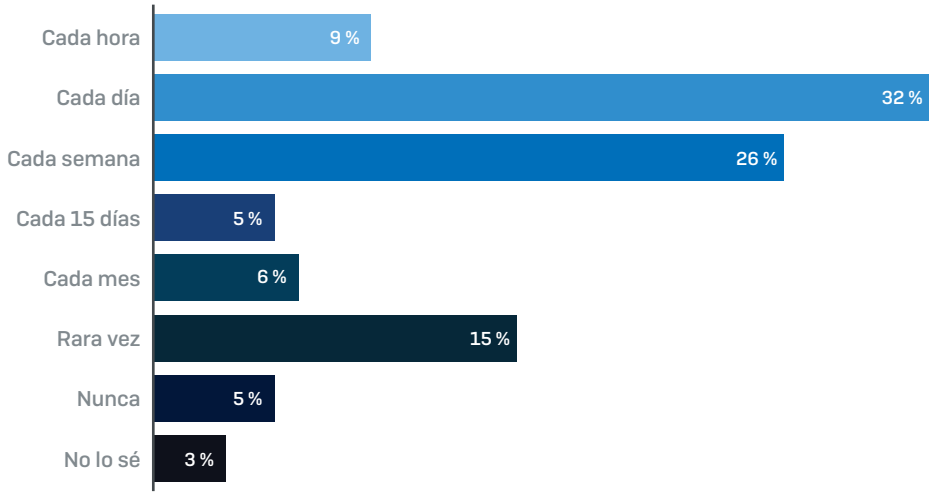
El 93%
de las filtraciones de datos incluyen phishing[2]

El phishing es un gran negocio

En los últimos años, el volumen de los ataques de phishing ha crecido exponencialmente, impulsado por servicios de la Web Oscura como los kits de phishing gratuitos y el phishing como servicio. Se ha convertido en algo muy sencillo, incluso para los atacantes menos capacitados técnicamente, aprovechar malware avanzado creado por alguien mucho más habilidoso.

El resultado es que los ataques de phishing ya forman parte de la vida cotidiana. El 41 % de los profesionales de TI informan de que su empresa experimenta ataques de phishing al menos una vez al día, mientras que más de tres cuartos (el 77 %) experimentan ataques cada mes como mínimo.[3]

Frecuencia de los ataques de phishing

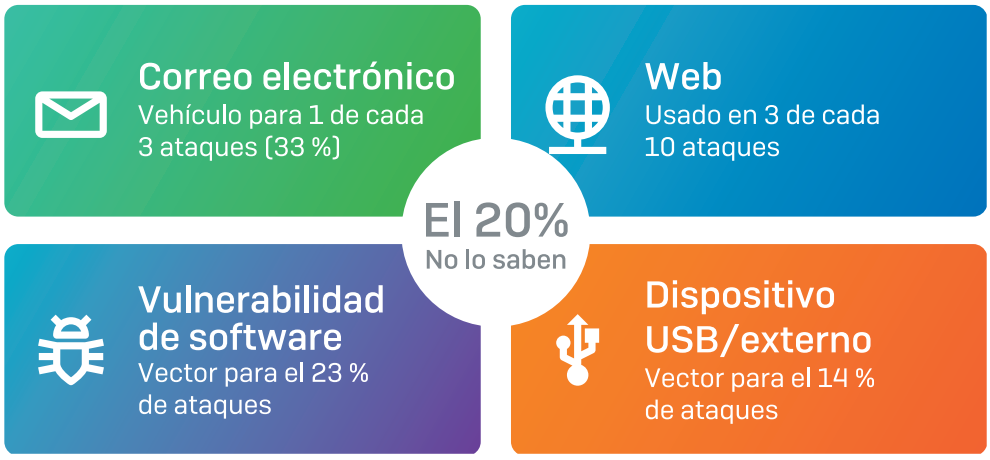


El vector de ataque más común

Una encuesta reciente a más de 3100 empresas reveló que el correo electrónico es el vector de ataque más común, puesto que se utiliza en el 33 % de los ciberataques con éxito. También se trata de un vector notablemente efectivo: el 53 % de las empresas que habían sufrido un ciberataque en el último año habían recibido correos electrónicos de phishing.[4]

Los correos electrónicos de phishing son con frecuencia la primera etapa de un ataque complejo con múltiples técnicas. Por ejemplo, al hacer clic en un enlace de un mensaje de phishing, se establece una conexión con un servidor de comando y control, que infecta la empresa con software malicioso.

1 de cada 3
ciberataques utilizan el correo electrónico como vehículo

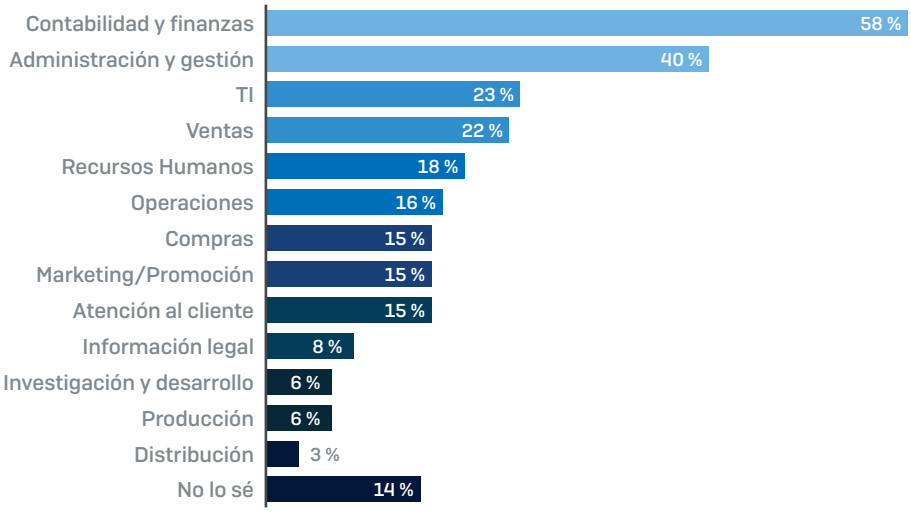


La principal motivación tras los ataques de phishing es el beneficio económico. El informe de las investigaciones sobre la fuga de datos de Verizon en 2018 reveló que:

- **El 59 % de los ataques tienen una motivación económica.** Esto incluye la recopilación de credenciales para su reventa en la Web Oscura, la infección de sistemas con ransomware o la suplantación de la identidad de directivos para convencer a los empleados para que transfieran fondos o datos valiosos.
- **El 41 % de los ataques tienen por objetivo conseguir acceso no autorizado al sistema.** Algunos ejemplos serían obtener acceso a la red de una empresa para robar datos u obtener el control de los sistemas.

Dada la motivación económica de la mayoría de ataques, no es de extrañar que los ciberdelincuentes se dirijan normalmente a empleados con acceso a las finanzas de la empresa para engañarles a fin de que realicen transferencias financieras a cuentas bancarias controladas por los atacantes. No obstante, también se dirigen a quienes gestionan procesos empresariales y controles de TI para dejar expuestas a las empresas a una serie de ataques entre los que se cuentan el ransomware y las extorsiones.[5]

Departamentos más afectados por los ataques de phishing



Por lo tanto, no resulta sorprendente que el phishing sea considerado el riesgo de seguridad más importante por los directores de TI, de quienes el 50 % lo ven como uno de los tres primeros riesgos. Asimismo, en el segundo lugar de la lista de riesgos están las personas, que incluyen el personal interno, los contratistas y los visitantes. Esto refleja la tendencia creciente de que los ciberdelincuentes explotan las vulnerabilidades y los comportamientos humanos en sus ataques.

% que lo considera uno de los tres primeros riesgos de seguridad

Mejorando la eficiencia y la productividad

Actualmente, el crimen organizado es el responsable del 89% de los ataques de phishing. Dado que el phishing se desarrolla como una actividad empresarial, las estrategias de ataque han seguido patrones de evolución con los que todos nos podemos identificar:

¿cómo puedo hacer que mi trabajo sea más fácil y trabajar de forma más eficiente y cómo puedo evolucionar a fin de aumentar las ganancias?

Esto ha dado lugar a unos métodos de distribución de ataques más eficientes, con servicios de phishing a demanda, kits de phishing listos para usar y nuevos tipos de ataques, como las estafas por correo electrónico corporativo comprometido (BEC, por sus siglas en inglés) dirigidas a activos de alto valor mediante métodos de ingeniería social.

El 89%

de los ataques de phishing están orquestados por grupos de delincuentes organizados profesionales

Kits de phishing gratuitos

¿Siempre ha deseado vender sus productos con el mismo éxito que el último iPhone lanzado al mercado? La mayoría de nosotros, si vemos una idea que funciona, de un amigo, un colega o un competidor, estamos tentados a "coger prestada" esa idea, ¿o no? Bien, la comunidad de phishing no es distinta. En realidad, está mejor organizada.

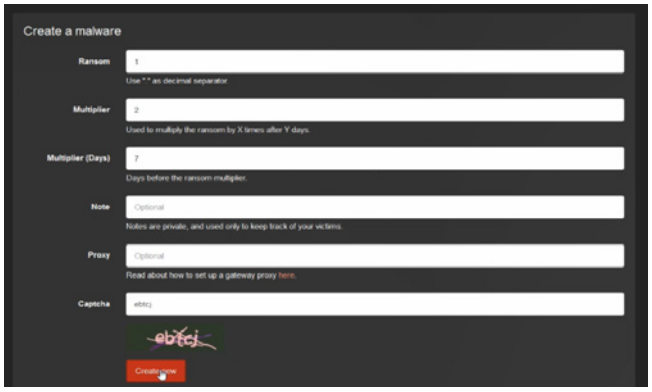
Una faceta interesante del ecosistema de phishing es que aunque el número de atacantes es elevado, solo un reducido número de ellos tiene los conocimientos suficientes como para crear un kit de phishing desde cero. Razón por la que actualmente los kits de phishing están disponibles de forma generalizada para su descarga en foros y plataformas de mercado de la Web Oscura. Unos kits que proporcionan a los atacantes todas las herramientas que necesitan para crear ataques de phishing rentables: correos electrónicos, códigos de páginas web, imágenes, etc.

Los autores de estos kits persiguen sus fines lucrativos mediante la distribución de estos kits entre los usuarios menos expertos ganando dinero de dos formas: con kits gratuitos que incluyen puertas traseras y que les permiten recopilar todos los datos recopilados a su vez por el emisor o directamente mediante su venta. Los kits más caros ahora incluso incluyen funciones como paneles de control para el seguimiento de campañas.

Ataques como servicio

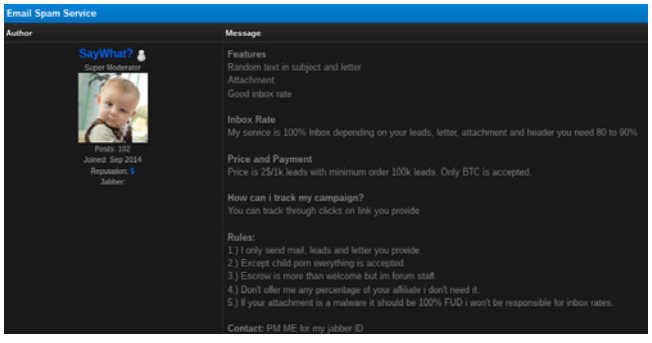
De hecho, los atacantes ya no necesitan saber cómo crear malware ni enviar mensajes de correo electrónico. Estamos viendo como las soluciones como servicio o de pago por uso están copando progresivamente la mayoría de las tecnologías de servicio online. El phishing no es diferente y la oferta de servicios para los atacantes tampoco deja de crecer:

- **Ransomware como servicio**: permite a los usuarios crear una cuenta online y rellenar un formulario web sencillo que incluye el precio inicial del rescate y un precio por pago tardío para las víctimas. El proveedor del servicio se queda con un porcentaje de cada rescate pagado ofreciéndose descuentos si el usuario es capaz de traducir el código del malware a lenguajes nuevos o si el volumen del ataque supera un determinado nivel.



Ransomware Satan: un servicio online que permite a los delincuentes crear su propio virus en minutos y comenzar a infectar sistemas Windows.

- **Phishing como servicio**: permite a los usuarios pagar por el envío de ataques de phishing, usando botnets globales para evitar el uso de rangos IP sospechosos ya conocidos. Se ofrecen incluso garantías en el sentido de cobrar a los usuarios solo por los mensajes de correo electrónico entregados, al igual que si se tratase de un servicio de marketing por correo electrónico legítimo.



Ejemplo de servicio de envío de spam: precio por correo electrónico enviado a una bandeja de entrada activa, con opción de registro incluso del nivel de seguimiento (clics).

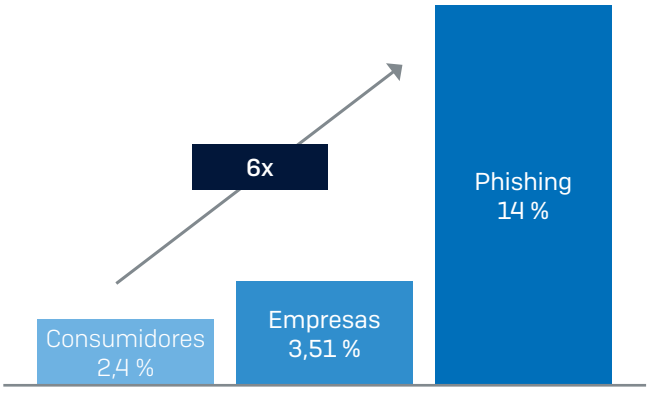
Estos servicios han provocado la explosión de ataques de phishing mencionada anteriormente, ya que cualquier atacante puede lanzar un ataque independientemente de sus capacidades técnicas.

Igual que el marketing, solo que seis veces mejor

Lo más preocupante de todo esto es que los servicios de la Web Oscura ahorran tiempo a los atacantes, por lo que pueden dedicar más tiempo a refinar sus campañas y pulir sus malvados conocimientos.

Y sus tácticas están permitiéndoles alcanzar unos resultados que serían la envidia de la mayoría de equipos de ventas y marketing. Así, la probabilidad de que los destinatarios hagan clic en un correo electrónico de phishing es seis veces superior que con un correo electrónico de marketing estándar.[6]

Nivel de seguimiento (clics) de correos de phishing



Este tiempo extra para I+D les ha permitido subir de forma importante el listón de las amenazas de phishing. Están aumentando las estafas por correo electrónico corporativo comprometido (BEC), un peligroso subconjunto de ataques de phishing que permite a los atacantes ampliar sus beneficios dirigiendo sus ataques contra objetivos corporativos de alto valor.

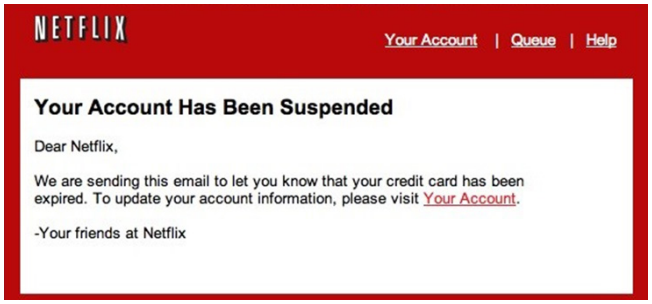
Cómo funciona el phishing

Como ya hemos dicho, el phishing es mucho más que correos electrónicos de banca falsos y avisos de entrega de paquetería. Más bien se trata de convencerle de proporcionar algo valioso a los atacantes. Y lo que en un principio era simplemente «phishing» ha evolucionado a tres tipos de ataques: los clásicos, el phishing masivo y spear phishing, y las estafas por correo electrónico corporativo comprometido, una variante del spear phishing.

Phishing masivo

Estos ataques son principalmente oportunistas. Aprovechan el nombre de marca de una empresa para atraer a los clientes de esa marca a sitios fraudulentos y engañarlos para que proporcionen información de sus tarjetas de crédito, credenciales de inicio de sesión y otra información personal que se venderá posteriormente con un beneficio económico.

- Dirigido contra activos personales
- Normalmente consumidores de productos o servicios de marcas
- Lotes y envíos impersonales
- Centrado en el robo de datos personales, como credenciales de inicio de sesión

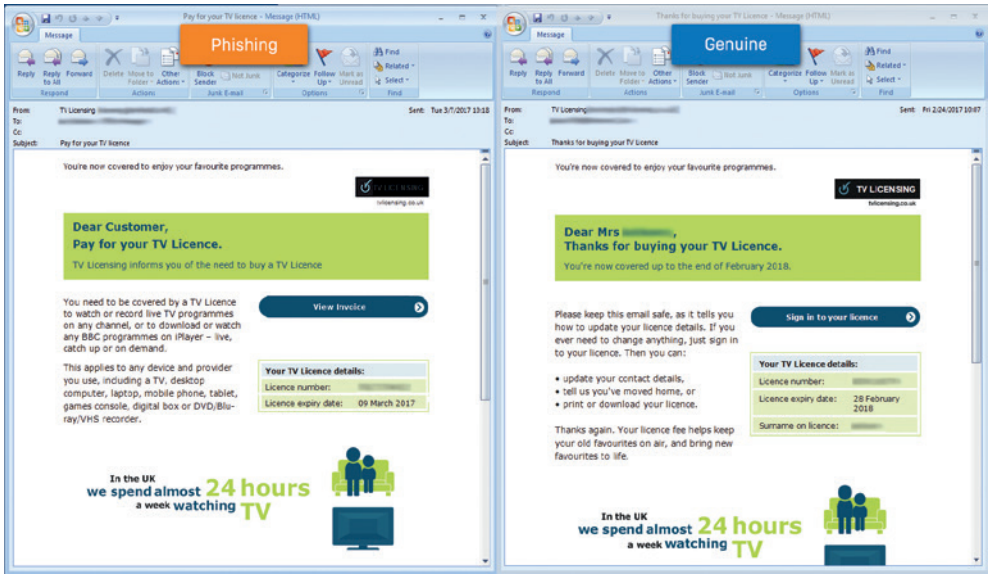


Ejemplo típico de phishing masivo "verifique su cuenta"

Spear phishing

El otro tipo de amenaza es la variedad de spear phishing, mediante la cual se envían correos electrónicos que suplantan un remitente específico o un origen de confianza a individuos concretos dentro de una empresa para inducirles a realizar determinadas acciones, como enviar dinero a cuentas fraudulentas.

- Dirigido contra activos de empresas específicas
- Normalmente un individuo o grupo específico en una empresa
- Direcciones de correo electrónico simuladas (falsas) para ayudar a la conversión
- Suplantación de fuentes de confianza y altos ejecutivos



Los correos electrónicos verdaderos y los de phishing frecuentemente son muy similares, tal y como muestra este convincente ejemplo de licencia de TV del Reino Unido.

Los ataques de spear phishing son cada vez más habituales, y los ciberdelincuentes siguen mejorando sus técnicas para incrementar su eficacia. En una encuesta reciente a 330 profesionales de TI, el 55 % confirmó que se había suplantado la identidad de sus directivos en ataques de spear phishing.[7]

Algunas variantes más dirigidas del spear phishing utilizan técnicas de ingeniería social para recopilar datos y aumentar la conversión. Se conocen como fraude CEO, Whaling y, más recientemente, estafas BEC (Business Email Compromise).

Estafa por correo electrónico corporativo comprometido

140 000 $
Pérdida media por estafa

Los ataques de estafa por correo electrónico corporativo comprometido reciben este nombre porque en lugar de falsificar las direcciones de los remitentes se comprometen las cuentas de correo electrónico de los empleados. Esta técnica dificulta mucho más su detección por parte de los usuarios finales.

- Dirigida contra información corporativa, acceso a credenciales o fondos de una empresa
- Una vez seleccionada una empresa para atacarla, los atacantes eligen a individuales concretos dentro de la empresa contra los que dirigir su ataque recopilando datos desde sitios como Facebook y LinkedIn para construir un ataque muy dirigido con correos electrónicos de phishing altamente creíbles.
- A continuación, el atacante aísla al individuo simulando que el correo electrónico procede de un directivo y añadiendo como factor de presión el tiempo, ya que estos mensajes se suelen enviar a última hora del día o la semana.

A diferencia de las campañas de phishing masivo o spear sphishing, estos ataques regularmente van dirigidos contra los fondos de empresas. Otra diferencia con respecto a los ataques de años anteriores, que proporcionaban los detalles de la cuenta bancaria de destino a las potenciales víctimas en adjuntos PDF, es que los ataques BCE actuales facilitan esta información solo cuando reciben una respuesta positiva por parte de la víctima. Después de todo, la cuenta fraudulenta es la inversión más importante del atacante y, por lo tanto, un activo importante que es necesario proteger para evitar que una víctima que detecte el fraude la denuncie a las autoridades.

En general, los ataques BEC son más difíciles de detectar, ya que los atacantes comprometen las cuentas de correo electrónico corporativo desde las que mandan los mensajes. De hecho, las últimas cifras del FBI indican que un impactante número de empresas están cayendo ante estos ataques, con pérdidas que en el 2016 alcanzaron los 3.100 millones de dólares afectando a 22.000 empresas.

Técnicas de phishing en evolución

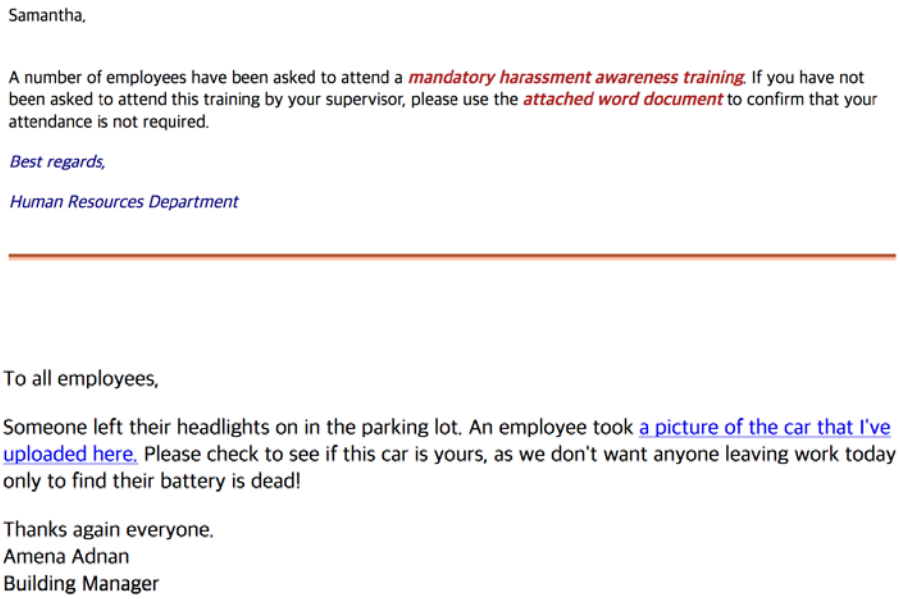
Las técnicas de phishing continúan evolucionando. A medida que las personas aprenden a reconocer esos mensajes demasiado buenos para ser verdad con premios fabulosos, los malhechores se van pasando a correos electrónicos simples y rutinarios con menos probabilidades de llamar la atención.

Esta investigación indica los 10 principales correos electrónicos que lograron engañar a sus destinatarios en la formación con simulaciones de Phish Threat de Sophos. Como puede ver, se trata de asuntos de correo electrónico muy «normales», temas que no suelen levantar sospechas.

ASUNTO DE CORREO ELECTRÓNICO	% ABIERTOS Y CON CLICS
[Jira] Se te ha asignado una tarea	39 %
Reunión de la próxima semana	29 %
Formación de sensibilización sobre el acoso	26 %
Coche que se ha dejado las luces encendidas	25 %
Mensaje de eFax de {Customer Name} - 2 página(s)	24 %
Citación de tráfico para {Email First Name} {Email Last Name}	22 %
Retraso en los pagos de peajes	21 %
Hombre sospechoso en las inmediaciones del edificio de {Customer Name}	20 %
IMPORTANTE - Encuesta anual a los empleados	19 %
Importante: nuevo sistema de correo electrónico en {Customer Name}	18 %

El correo electrónico de phishing más efectivo hacía referencia a JIRA, una popular herramienta de software, seguido de una solicitud de reunión o un correo de formación sobre el acoso, diseñado para hacernos entrar en pánico y saltarnos las comprobaciones de seguridad habituales.

Estos son solo dos de los ejemplos de correos electrónicos de phishing que hemos explicado y demuestran claramente la simplicidad y la eficacia de los mensajes rutinarios.



Samantha,

A number of employees have been asked to attend a *mandatory harassment awareness training*. If you have not been asked to attend this training by your supervisor, please use the *attached word document* to confirm that your attendance is not required.

Best regards,

Human Resources Department

To all employees,

Someone left their headlights on in the parking lot. An employee took a picture of the car that I've uploaded here. Please check to see if this car is yours, as we don't want anyone leaving work today only to find their battery is dead!

Thanks again everyone.
Amena Adnan
Building Manager

Detectar los indicios

¿Facturas falsas que le llegan informándole de que alguien ha comprado un vuelo con su tarjeta de crédito y pidiéndole que abra el documento adjunto para más información si quiere cuestionar el pago? Se trata de phishing masivo.

El 30%
de los correos de phishing se abren

Al igual que los avisos falsos de empresas de paquetería en los que se le pide confirmar la dirección de la empresa para que se le entregue mercancía sin entregar.

El spear phishing a grandes rasgos es lo mismo, solo que el señuelo es más específico. O como es el caso de los ataques BEC, seguramente el mensaje no contendrá enlaces ni adjuntos maliciosos, sino que más bien le pedirá que transfiera fondos haciendo el ataque más creíble.

De forma más sencilla, si un mensaje de correo electrónico fraudulento empieza por "Estimado cliente", es phishing. Pero si se dirige a usted por su nombre, es spear phishing. Y si procede de la dirección de correo electrónico de su jefe, es un ataque de estafa por correo electrónico corporativo comprometido (BEC).

Por supuesto, que muchos ataques de spear phishing apuntan todavía mucho mejor. Los delincuentes que se preparan a fondo sabrán su cargo, el número de su extensión, la cafetería a la que va a desayunar, sus amigos, el nombre de su jefe, el nombre de su jefe anterior e incluso la empresa encargada de la máquina de café de su empresa.

Y, como probablemente imaginará, en lo que se refiere al spear phishing, nada atrae el éxito como el propio éxito en sí. Cuanto más sepan estos estafadores, bandas de ciberdelincuentes o equipos de agentes patrocinados por gobiernos sobre su empresa, más creíbles serán sus intentos de phishing.

Esta información se puede adquirir de muchas formas, incluyendo:

- Ataques anteriores exitosos, como malware destinado a robar datos
- Documentos privados de la empresa, como directorios de teléfonos o diagramas organizativos que aparecen en los motores de búsqueda
- Páginas de redes sociales personales y de la empresa
- Antiguos empleados descontentos
- Datos comprados a otros criminales en la Web Oscura

Probablemente se le ocurran muchas otras formas mediante las que información "secreta" puede dejar de serlo. En definitiva, la conclusión es que comprender cómo funcionan estas tácticas puede significar que no abra uno del 30% de los correos electrónicos de phishing que se abren hoy en día.

Utilice este útil acrónimo para ayudar a sus usuarios a detectar las señales de un correo electrónico de phishing:

P: Promete unas ofertas increíbles

H: Hostiga para que conteste

I: Insiste para que actúe ya

S: Sensación de urgencia

H: ¡Haga clic en Eliminar!

En caso de duda, informe a su equipo de TI y elimínelo para avisar del mensaje de phishing a toda la empresa.

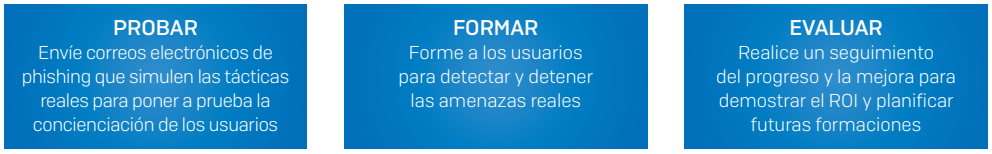
La lucha contra el phishing

Hay ataques de phishing de todo tipo, y desafortunadamente no existe ninguna fórmula infalible para detenerlos. La única respuesta contra los ataques de phishing es una defensa de varias capas que combine tecnologías avanzadas de seguridad y empleados formados y concienciados sobre el phishing. En Sophos, recomendamos a todas las empresas que adopten una triple estrategia:

1. Visibilidad y formación

En la lucha contra el phishing, sus usuarios son el eslabón más débil. De hecho, solo se necesitan 16 minutos de media para que alguien haga clic en un correo electrónico de phishing [Fuente: Informe de las investigaciones sobre la fuga de datos de Verizon en 2018].

- Puesto que sus usuarios son los que están en primera línea en los ataques de phishing, es fundamental concienciar y formar a las personas sobre cómo detectar (y evitar) los correos electrónicos de phishing. Un programa de **formación y simulación de phishing** efectivo consta de tres etapas:



2. Antes de la entrega

El 58 % del correo electrónico es spam y el 77 % de todos los mensajes de spam contienen un archivo malicioso[6]. Por tanto, una **puerta de enlace de correo electrónico segura** es un elemento esencial en la lucha contra el phishing, puesto que detecta los mensajes de phishing antes de que puedan llegar a las bandejas de entrada. Las tecnologías básicas que debe buscar incluyen:

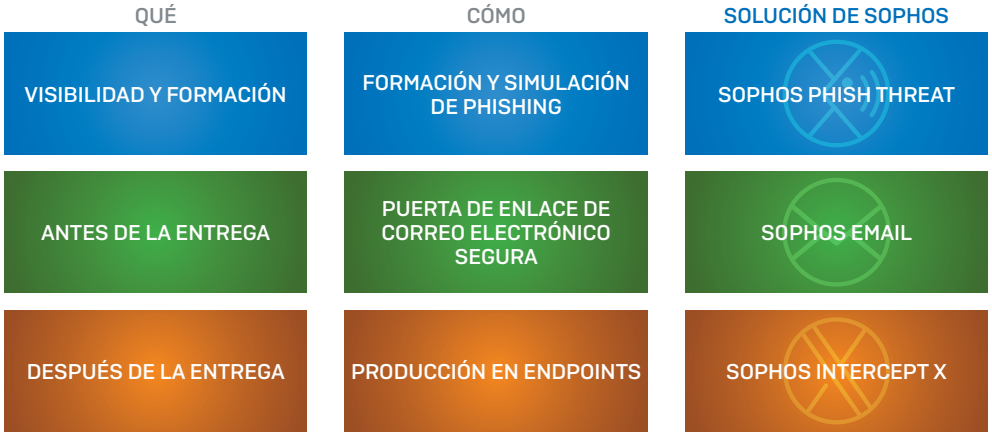
- **Antispam:** potentes trampas de spam de alcance global impiden que los mensajes lleguen a sus usuarios.
- **Reputación de remitentes:** filtrado por reputación de direcciones IP para bloquear mensajes no deseados en la puerta de enlace.
- **Autenticación de remitentes:** detecte suplantaciones de remitentes, anomalías en encabezados y contenido sospechoso en el cuerpo de los correos electrónicos.
- **Espacios seguros:** detone archivos sospechosos fuera de la red.
- **Bloqueo de direcciones URL maliciosas:** filtre enlaces maliciosos y protéjase contra ataques furtivos diferidos.

3. Después de la entrega

- La etapa posterior a la entrega es la última línea de defensa para proteger su empresa si un usuario hace clic en un enlace malicioso o abre un archivo adjunto infectado. Busque una solución de **seguridad para endpoints** que ofrezca técnicas tanto base como modernas, entre ellas:
- **Deep Learning:** bloquee amenazas desconocidas para evitar que se ejecuten en su empresa.
- **Antiexploits:** impida a los atacantes explotar vulnerabilidades en software legítimo.
- **Antiransomware:** evite el cifrado no autorizado de los recursos de su empresa.

Cómo puede ayudar Sophos

Sophos es el único proveedor que ofrece una protección completa contra el phishing (visibilidad y formación, antes de la entrega y después de la entrega), íntegramente gestionada a través de una única plataforma web.



31 %

de reducción en la predisposición de los empleados con Sophos Phish Threat

Sophos Phish Threat forma a sus usuarios finales y los pone a prueba mediante simulaciones de ataque automatizadas, formación de calidad de concienciación sobre la seguridad y métricas de informes procesables. Y funciona: de media, los clientes observan una reducción del 31 % en la predisposición de los empleados después de solo cuatro correos de formación de Phish Threat.

Con **Sophos Email**, puede volver a confiar en su bandeja de entrada. Bloquea a los impostores del phishing y protege a los empleados contra ataques que utilizan direcciones de correo electrónico fraudulentas que se hacen pasar por contactos de confianza. La combinación de técnicas de autenticación SPF, DKIM y DMARC con el análisis de encabezados de correo electrónico le permite identificar y permitir los correos legítimos, al tiempo que se bloquean los impostores.

Sophos Intercept X combina una gran variedad de técnicas tanto base como modernas (next-gen) para combatir la más amplia gama de ataques de ransomware y malware. Su red neuronal de Deep Learning se entrena con cientos de millones de archivos maliciosos para detectar amenazas desconocidas de forma proactiva.

Solo Sophos le permite gestionar todas sus tecnologías de prevención del phishing a través de una única plataforma web. Se llama Sophos Central. Todo está basado en Internet, lo que significa que no hay mantenimiento de servidores y se puede acceder en cualquier momento y lugar, con lo que se ahorra tiempo.

Empiece con un producto y añada otros cuando esté preparado.

No pique

1, 3, 5, 7 Fuente: Phishing Temperature Check, Freeform Dynamics en colaboración con The Register y Sophos, 2017

2 Fuente: Informe de las investigaciones sobre la fuga de datos de Verizon en 2018

4 El rompecabezas imposible de la ciberseguridad, Sophos, julio de 2019

6 Fuente: Verizon 2016 DBIR & Experian Email Benchmark Report Q4 2016

7 Fuente: SophosLabs, 2017

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

12-07-2019 WP-ES (PC)

SOPHOS