Análisis sobre el phishing 2021

Aunque el phishing ya lleva entre nosotros un cuarto de siglo, sigue siendo una técnica de ciberataque efectiva principalmente porque no deja de evolucionar. Los adversarios son rápidos a la hora de identificar nuevas oportunidades para el phishing (muchas de las cuales emergieron con la pandemia) y desarrollar nuevas tácticas y técnicas.

Para las organizaciones, el phishing suele ser el primer paso de un ataque complejo de varias fases. Los adversarios utilizan con frecuencia el phishing para engañar a los usuarios para que instalen malware o compartan credenciales que proporcionan acceso a la red de su víctima. Un correo electrónico aparentemente inofensivo puede acabar provocando un ataque de ransomware, criptojacking o robos de datos.

En este informe se incluyen las conclusiones más recientes sobre el phishing basadas en una encuesta independiente a 5400 profesionales de TI al frente de departamentos informáticos de todo el mundo, junto con un estudio de un caso de un ataque de phishing en el mundo real que provocó un incidente de ransomware multimillonario.

Según el Informe de investigación sobre filtraciones de datos de Verizon de 2021, el 36 % de los casos confirmados de filtraciones de datos implican phishing, lo que supone un incremento con respecto al 25 % de 2019. Utilice los resultados de esta encuesta para evaluar su propia posición de seguridad en relación con el phishing e identificar oportunidades para ampliar sus defensas.

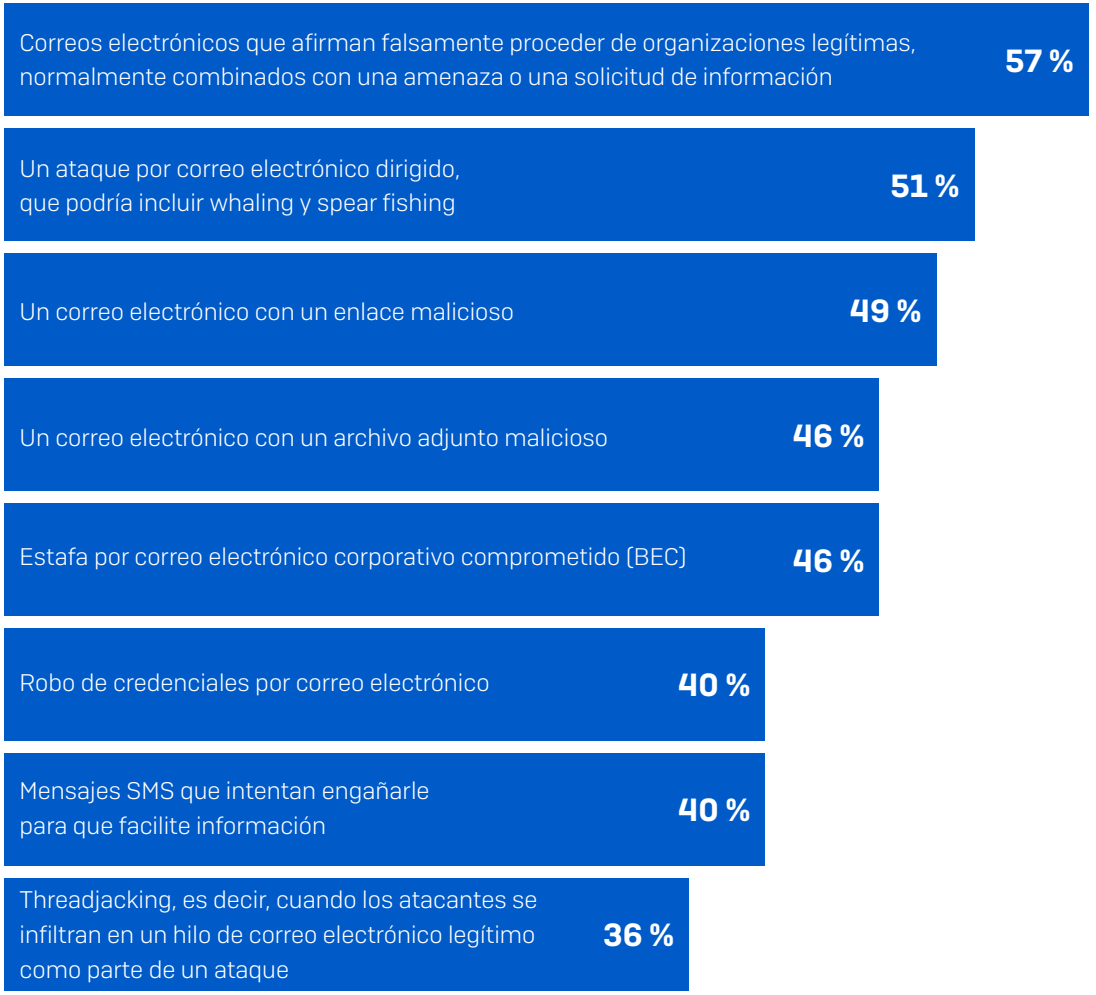
SOPHOS

1. Phishing significa cosas distintas para distintas personas

¿Qué es el phishing? Nuestra encuesta revela que incluso entre los profesionales de TI existen grandes diferencias en cuanto a lo que se considera un ataque de phishing. La interpretación más común es que se trata de *correos electrónicos que afirman falsamente proceder de organizaciones legítimas, normalmente combinados con una amenaza o una solicitud de información*. Si bien esta fue la respuesta más popular, menos de 6 de cada 10 (57 %) de los encuestados seleccionaron esta opción, lo que pone de manifiesto el amplio abanico de significados que se dan al phishing.

El 46 % de los encuestados consideran que las estafas por correo electrónico corporativo comprometido (BEC) son phishing, mientras que más de un tercio (36 %) entienden que el phishing incluye el threadjacking, es decir, cuando los atacantes se infiltran en una cadena de correo electrónico legítima como parte de un ataque.

¿Cuál de las siguientes opciones considera que es un ataque de phishing?



¿Cuál de estas opciones considera que es un ataque de phishing? [5400] Excluyendo algunas opciones de respuesta

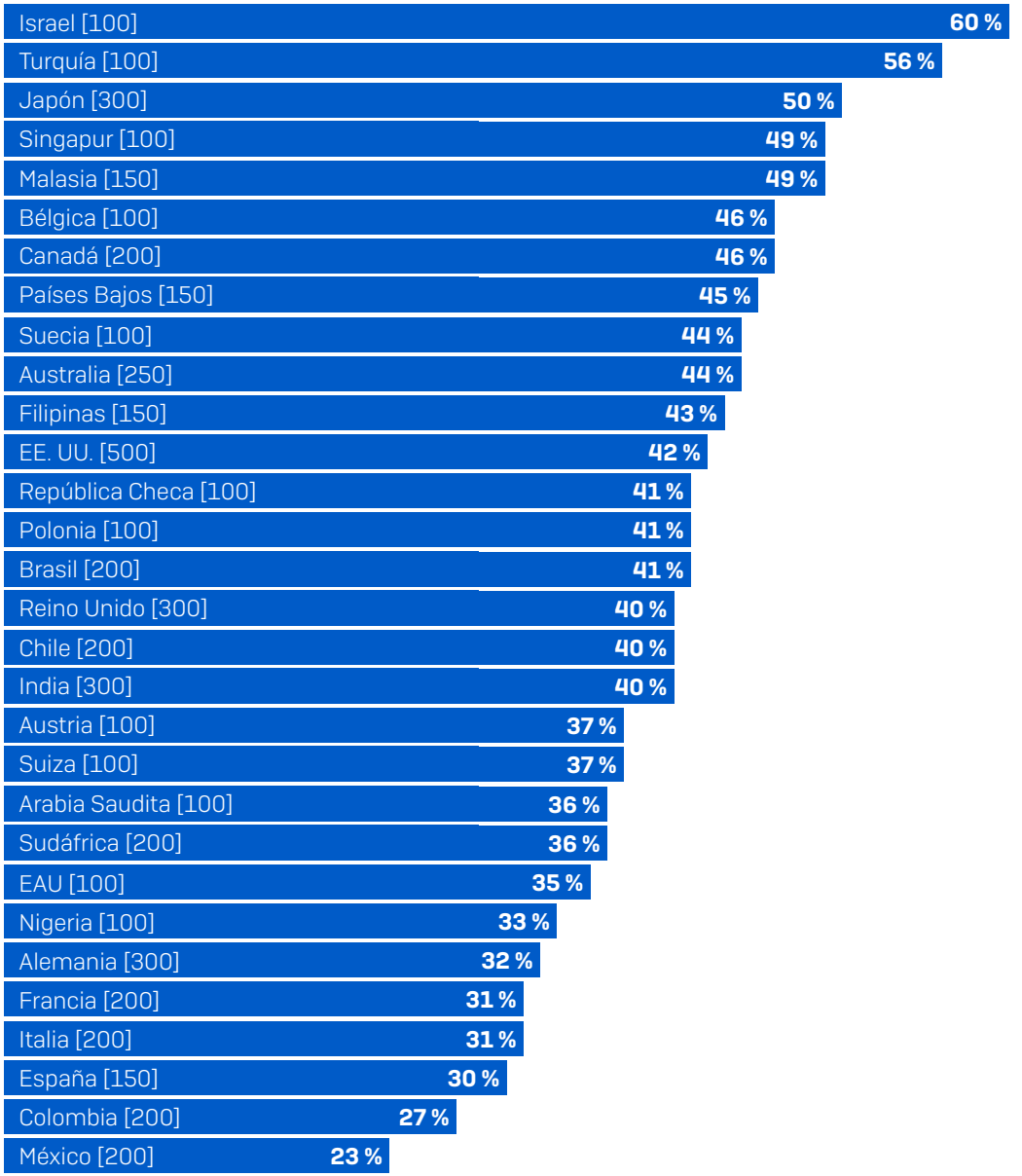
Los factores culturales tienen un gran impacto en cómo interpretan las personas el phishing. Por ejemplo, la proporción de encuestados de Israel que consideran phishing los mensajes SMS que intentan engañarle para que proporcione información duplica con creces el porcentaje de México (el 60 % frente al 23 %). Aunque muchos profesionales de TI llaman a esto smishing en lugar de phishing, los mensajes falsos que afirman proceder de marcas de confianza tienen el mismo efecto independientemente del método de transmisión.

Teniendo en cuenta estas notables diferencias entre los profesionales de TI en cuanto a cómo entienden o definen los ataques de phishing, cabe esperar una variedad de interpretaciones similar o superior entre los empleados no informáticos.

Comprender que el phishing significa cosas distintas para distintas personas es una conclusión significativa para cualquiera que se dedique a crear o gestionar programas de formación y concienciación sobre el phishing. Para que la formación sobre phishing sea efectiva, es importante garantizar que haya una definición base compartida del phishing para que lo que aprendamos pueda entenderse en el contexto correcto.

CONCLUSIÓN: TENGA EN CUENTA QUE PHISHING SIGNIFICA COSAS DISTINTAS PARA DISTINTAS PERSONAS A LA HORA DE OFRECER RECURSOS FORMATIVOS Y FORMACIÓN PARA LA CONCIENCIACIÓN DE LOS USUARIOS. SIN EL CONTEXTO CORRECTO, LA FORMACIÓN SERÁ MENOS EFECTIVA.

Encuestados que consideran que los mensajes SMS que intentan engañarles para que proporcionen información son phishing



¿Cuál de estas opciones considera que es un ataque de phishing? [números base en el gráfico] Mensajes SMS que intentan engañarle para que proporcione información

2. El phishing se ha incrementado considerablemente desde el inicio de la pandemia

El 70 % de los encuestados registraron un aumento de los ataques de phishing en su organización desde el inicio de la pandemia. Todos los sectores se vieron afectados, si bien el gobierno central registró el mayor incremento (77 %), seguido de cerca por los servicios empresariales y profesionales (76 %) y la sanidad (73 %).

La pequeña variación entre sectores (de solo 10 puntos porcentuales antes del redondeo*) demuestra que los adversarios no suelen discriminar e intentan llegar a tantas personas como pueden a fin de incrementar sus probabilidades de éxito.

La investigación de SophosLabs demostró que los adversarios fueron rápidos a la hora de aprovechar las oportunidades que presentó la pandemia y la consiguiente difuminación de la frontera entre el hogar y el trabajo, entre ellas:

- Rápido incremento del teletrabajo. Es probable que los atacantes esperaran que la gente bajara la guardia mientras se adaptaba a trabajar desde casa y a desenvolverse en un entorno no empresarial.
- Crecimiento de las entregas a domicilio. Los mensajes de phishing que se hacían pasar por empresas de envíos a domicilio se volvieron habituales durante los primeros meses de la pandemia cuando la gente empezó a recurrir en masa a las compras por Internet.
- Preocupación generalizada por la pandemia. Los adversarios se aprovecharon de la ansiedad de la gente y su necesidad de información sobre la COVID-19 con fraudes relacionados con la pandemia. Previeron que, con tanta preocupación, sería menos probable que la gente comprobara si un mensaje era legítimo antes de hacer clic.

Sector	Encuestados que registraron un aumento de los ataques de phishing en su organización desde el inicio de la pandemia
Gobierno central y entidades públicas independientes [117]	77 %
Servicios empresariales y profesionales [361]	76 %
Sanidad [328]	73 %
Medios de comunicación, ocio y entretenimiento [145]	72 %
Energía, petróleo/gas y servicios públicos [197]	72 %
Comercio minorista [435]	71 %
Educación [499]	71 %
Otros [768]	71 %
Gobierno local [131]	69 %
Distribución y transporte [203]	68 %
Servicios financieros [550]	68 %
Construcción y propiedad [232]	68 %
TI, tecnología y telecomunicaciones [996]	68 %
Fabricación y producción [438]	66 %

¿Ha notado algún cambio en el número de ataques de phishing en su organización desde el inicio de la pandemia? [números base en el gráfico] Sí, un gran aumento; Sí, un pequeño aumento

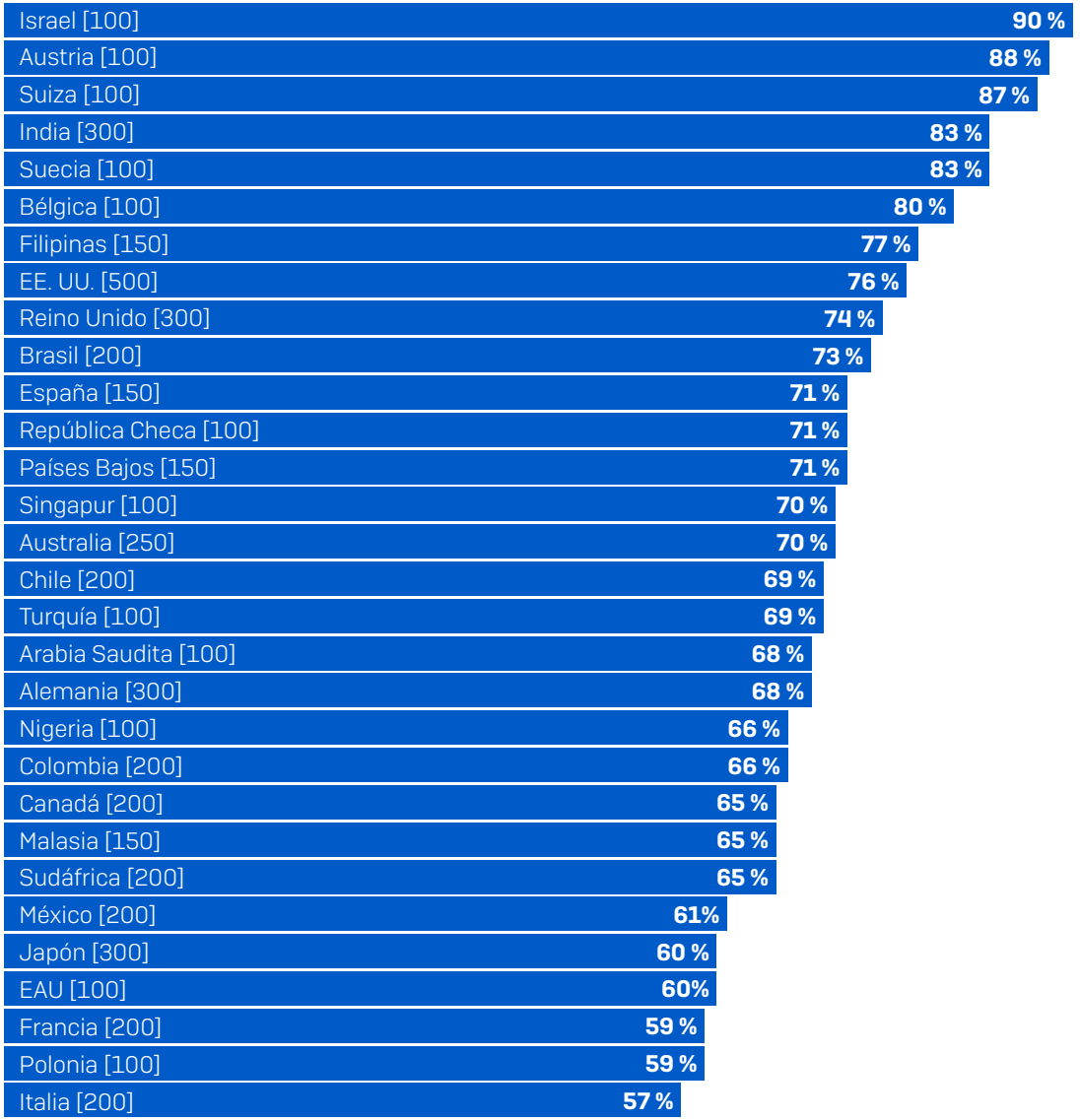
** Antes del redondeo, el 76,92 % de los encuestados del gobierno central registraron un incremento en comparación con el 66,43 % del sector de la fabricación, lo que supone una diferencia real del 10,48 %.*

Aunque las variaciones por sector fueron pequeñas, la encuesta reveló una diferencia considerable en los ataques de phishing registrados por país desde el principio de la pandemia. Por ejemplo, el 90 % de los encuestados en Israel registraron un aumento del phishing frente al 57 % en Italia. Estos resultados, aunque se vean influidos por la definición del phishing de los encuestados y su capacidad de rastrear y evaluar los ataques, ofrecen una información muy valiosa sobre la experiencia en el mundo real de los profesionales de TI que se encuentran en la primera línea.

Al igual que hay muchos tipos distintos de correos electrónicos de phishing, también existen muchos tipos de ciberdelincuentes diferentes tras ellos. Los grupos de adversarios más hábiles suelen centrar sus ataques dirigidos en países con un PIB más alto como Austria, Suiza y Suecia para maximizar su rendimiento económico, lo que probablemente contribuye al incremento generalizado del phishing en estos países. Al mismo tiempo, el phishing también se utiliza en los ataques "spray and pray" en el mercado de masas, en que los adversarios tienen la esperanza de que, si lo intentan con suficientes personas, al final alguien acabará cayendo en la trampa.

CONCLUSIÓN: NO CEJE EN SUS ESFUERZOS ANTIPHISHING. LOS CIBERDELINCUENTES UTILIZAN CADA VEZ MÁS ESTA TÉCNICA, Y NO SE SALVA NINGÚN SECTOR NI PAÍS.

Encuestados que han registrado un aumento del número de ataques de phishing en su organización desde el inicio de la pandemia



¿Ha notado algún cambio en el número de ataques de phishing en su organización desde el inicio de la pandemia? [números base en el gráfico] Sí, un gran aumento; Sí, un pequeño aumento

3. La mayoría de organizaciones tienen programas de concienciación sobre ciberseguridad para hacer frente al phishing

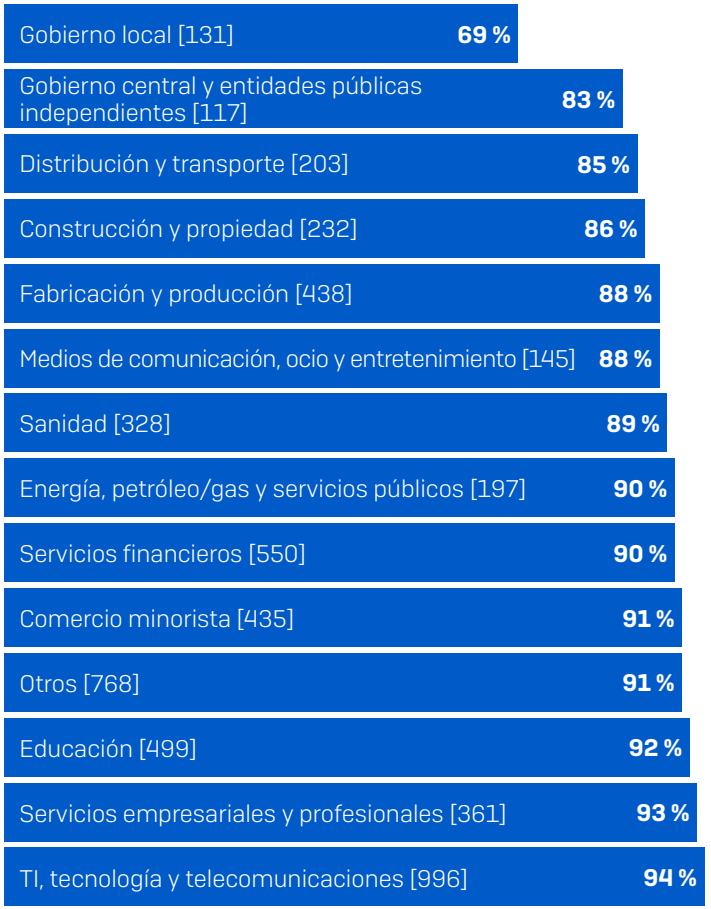
El 90 % de las organizaciones han implementado algún programa de concienciación sobre ciberseguridad para hacer frente al phishing, y un 6 % más tienen previsto poner alguno en marcha.

El enfoque más popular es la formación por ordenador, que utiliza el 58 % de las organizaciones. Más de la mitad (53 %) utiliza formación dirigida por humanos, y el 43 % realiza simulaciones de phishing. El 16 % de las organizaciones combinan las tres técnicas (formación por ordenador, formación dirigida por humanos y simulaciones de phishing) en sus programas de concienciación.

La encuesta reveló que el sector gubernamental va a la zaga en la organización de programas de concienciación sobre ciberseguridad para lidiar con el phishing, con las dos últimas posiciones ocupadas por el gobierno local (69 %) y el gobierno central (83 %). Esto resulta preocupante, porque las organizaciones gubernamentales son blancos frecuentes de ciberataques de alto impacto: el sector del gobierno central es más propenso a sufrir ataques de ransomware de tipo extorsión, mientras que el del gobierno local es más propenso a sufrir ataques de ransomware con cifrado de datos.

CONCLUSIÓN: SI FORMA PARTE DEL 10 % QUE AÚN NO TIENE NINGÚN PROGRAMA DE CONCIENCIACIÓN SOBRE CIBERSEGURIDAD PARA HACER FRENTE AL PHISHING, IMPLEMENTE UNO ENSEGUIDA.

Uso de programas de concienciación sobre ciberseguridad para hacer frente al phishing



¿Su organización tiene implementado algún programa de concienciación sobre ciberseguridad para hacer frente al phishing? [5400] Sí, tenemos programas de formación por ordenador; Sí, tenemos programas de formación dirigida por humanos; Sí, realizamos simulaciones de phishing

90 %

han implementado un programa de concienciación sobre ciberseguridad para lidiar con el phishing

58 %

organizan programas de formación por ordenador

53 %

organizan programas de formación realizada por humanos

43 %

realizan simulaciones de phishing

¿Su organización tiene implementado algún programa de concienciación sobre ciberseguridad para hacer frente al phishing? [5400] Sí, tenemos programas de formación por ordenador; Sí, tenemos programas de formación dirigida por humanos; Sí, realizamos simulaciones de phishing

4. Los programas de concienciación sobre el phishing están bien establecidos

Casi dos tercios (65 %) de los programas de concienciación sobre el phishing se implementaron hace entre uno y tres años, lo que refleja la respuesta de las organizaciones ante el cambio de técnica de los atacantes a mediados de la última década. La mejora de las ciberdefensas contra los ataques basados en Internet de mediados de la década de 2010 obligó a los adversarios a pasarse a nuevos vectores como el correo electrónico, lo que a su vez generó una gran necesidad de programas de formación para los usuarios.

Dado el incremento generalizado del phishing desde el inicio de la pandemia, resulta alentador que el 98 % de las organizaciones hubieran implementado su programa de concienciación sobre el phishing antes de que surgiera la COVID-19. Gracias a estos programas, los empleados se encontraron en una buena posición para resistir el aluvión de correos de phishing del último año.

¿Cuándo implementó su organización el programa de concienciación sobre ciberseguridad para hacer frente al phishing?	
En el último año	2 %
Hace 1-2 años	30 %
Hace 2-3 años	35 %
Hace 3-4 años	20 %
Hace 4-5 años	12 %
Hace más de 5 años	0 %
No lo saben	1 %

Encuestados cuya organización tiene un programa de concienciación implementado para lidiar con el phishing [4866]

CONCLUSIÓN: ASEGÚRESE DE REVISAR Y ACTUALIZAR PERIÓDICAMENTE SUS MATERIALES Y ACTIVIDADES DE CONCIENCIACIÓN SOBRE EL PHISHING PARA GARANTIZAR QUE SIGUEN SIENDO RELEVANTES Y ATRACTIVOS PARA SUS USUARIOS.

5. Unas medidas de seguimiento positivas dominan la evaluación de la efectividad de la formación

Casi todas (98 %) las organizaciones que ejecutan un programa de concienciación de los usuarios para hacer frente al phishing evalúan el impacto de sus esfuerzos. Medir y seguir los resultados permite a las organizaciones optimizar sus programas para mejorar los resultados.

Los enfoques más comunes son el seguimiento del número de correos electrónicos de phishing denunciados al equipo de TI (68 %) y/o el nivel de denuncias de phishing por parte de los usuarios (65 %). Resulta esperanzador que estas medidas positivas que reflejan una buena concienciación y comportamiento de los usuarios sean lo más habitual. Identificar y crear conciencia de una estafa de phishing permite a los equipos de TI evitar de forma proactiva que otros usuarios acaben siendo víctimas de la misma.

La mitad de las organizaciones (50 %) realizan un seguimiento del índice de clics en los correos electrónicos de phishing. Aunque se trate de una medida negativa (se centra en sucumbir al engaño), el índice de clics proporciona a los equipos de TI datos que les ayudan a dirigir los programas de concienciación allá donde más se necesitan y a adaptar el contenido a fin de que refleje la realidad de su organización. Cuantos más puntos de datos pueda rastrear, ya sean positivos o negativos, mejor.

98 % evalúan el impacto de su programa de concienciación

68 % realizan un seguimiento de las incidencias relacionadas con el phishing comunicadas al equipo de TI

65 % realizan un seguimiento del nivel de denuncias de correos electrónicos de phishing por parte de los usuarios

50 % realizan un seguimiento del índice de clics en los correos electrónicos de phishing

¿De qué realiza un seguimiento para evaluar el impacto de su programa de concienciación? [4866 encuestados cuya organización tiene implementado un programa de concienciación para hacer frente al phishing] Número de incidencias relacionadas con el phishing comunicadas al equipo de TI; Nivel de denuncia de correos electrónicos de phishing por parte de los usuarios; Índice de clics en correos electrónicos de phishing. No evaluamos el impacto de nuestros programas de concienciación sobre el phishing. Excluye algunas opciones de respuesta

CONCLUSIÓN: REVISE PERIÓDICAMENTE SUS PROGRAMAS DE FORMACIÓN DE USUARIOS A LA LUZ DE LOS RESULTADOS DE SUS EVALUACIONES Y CÉNTRESE EN RECONOCER Y CELEBRAR LOS COMPORTAMIENTOS POSITIVOS.

Estudio de caso: Cómo un correo electrónico de phishing llevó a un ataque de ransomware multimillonario

El equipo de Sophos Rapid Response fue llamado recientemente para ayudar a una empresa que estaba sufriendo un grave ataque de ransomware. Una vez contenido el ataque, el equipo de Rapid Response investigó el incidente para entender cómo se había iniciado. A continuación se detalla lo que descubrió.

Tres meses antes del ataque, un empleado recibió un correo electrónico de phishing. El correo parecía proceder de un compañero de otra oficina; es probable que los atacantes hubieran accedido a la cuenta de correo electrónico del compañero a fin de engañar a otros empleados para que confiaran en el mensaje.

El mensaje era muy breve y estaba mal redactado. Pedía al empleado que hiciera clic en un enlace para comprobar un documento. El enlace era en realidad un enlace web malicioso y, cuando el empleado hizo clic en él, permitió a los atacantes obtener acceso a las credenciales del administrador del dominio.

El equipo de Rapid Response cree que el correo electrónico de phishing fue enviado por un agente de acceso inicial, un ciberdelincuente que se dedica a obtener acceso a los entornos de las organizaciones para después vender el acceso a otros adversarios, que pueden utilizarlo en distintos tipos de ataques, por ejemplo, de ransomware o robo de datos.

En este caso, el equipo de TI de la víctima intervino y desactivó el ataque de phishing. Aparentemente, todo había terminado.

Ocho semanas después, sin embargo, un ciberdelincuente instaló y ejecutó dos herramientas, Cobalt Strike y PowerSploit PowerView, en el ordenador de la víctima. Se trata de herramientas comerciales que utilizan de forma legítima técnicos de pruebas de penetración, pero también ciberdelincuentes con propósitos maliciosos. Seguramente los atacantes utilizaron PowerView para realizar un reconocimiento de la red, mientras que Cobalt Strike les proporcionó persistencia, lo que les permitió permanecer en la red.

Durante unas dos semanas después de la actividad exploratoria de los atacantes todo se calmó. El equipo de Rapid Response cree que esto se debe a que el agente de acceso inicial estaba buscando a un comprador adecuado para las credenciales de acceso.

Una vez vendidas, los nuevos "propietarios" se apresuraron a sacar partido de su compra. Enseguida aparecieron en la red, instalaron Cobalt Strike en más equipos y empezaron a recopilar y robar información.

Tres meses después del correo electrónico de phishing original, los atacantes activaron el ransomware REvil a las 04:00 hora local y exigieron un rescate de 2,5 millones de dólares.

Consiga una protección contra el phishing basada en IA con Sophos Email

El Machine Learning avanzado **identifica a los impostores del phishing y los ataques BEC**

La búsqueda en tiempo real de indicadores clave de phishing **bloquea las técnicas de ingeniería social**

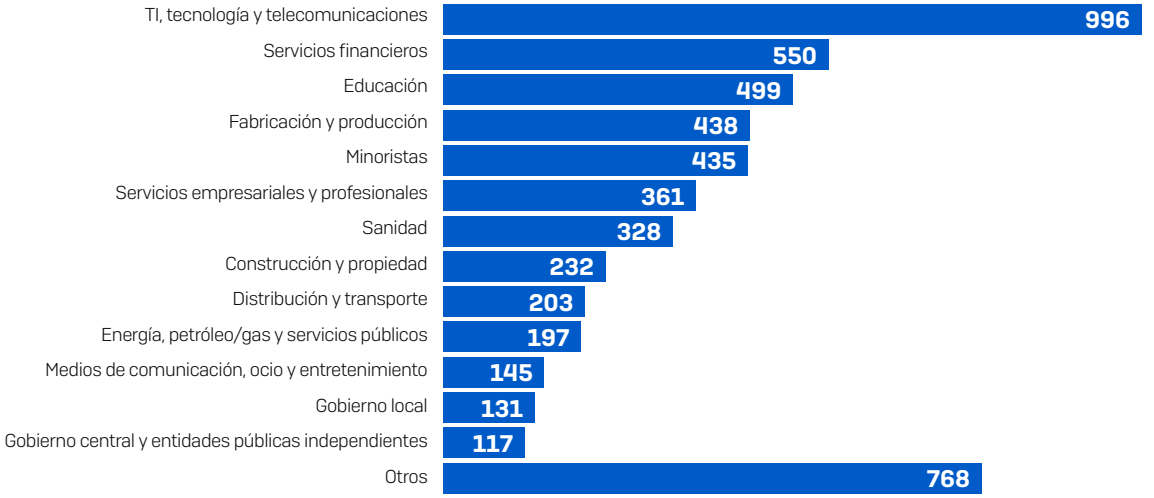
La protección anterior y posterior a la entrega detiene **los enlaces maliciosos y el malware**

Más información y evaluación gratuita en es.sophos.com/email

Acerca de la encuesta

Sophos encargó a la consultora independiente Vanson Bourne la realización de una encuesta a 5400 directores de TI de organizaciones medianas (100-5000 empleados) de 30 países. La encuesta se llevó a cabo en enero y febrero de 2021. Los encuestados también procedían de sectores tanto públicos/gubernamentales como privados.

Número de encuestados por sector



Número de encuestados por país

País	N.º de encuestados	País	N.º de encuestados	País	N.º de encuestados
Australia	250	India	300	Arabia Saudita	100
Austria	100	Israel	100	Singapur	150
Bélgica	100	Italia	200	Sudáfrica	200
Brasil	200	Japón	300	España	150
Canadá	200	Malasia	150	Suecia	100
Chile	200	México	200	Suiza	100
Colombia	200	Países Bajos	150	Turquía	100
República Checa	100	Nigeria	100	EAU	100
Francia	200	Filipinas	150	Reino Unido	300
Alemania	300	Polonia	100	EE. UU.	500

13-08-2021 WPES (NP)

SOPHOS