proofpoint.

LIBRO ELECTRÓNICO

La concienciación: escudo anticiberataques

Lo que desconocen los usuarios sobre las ciberamenazas, y por qué puede perjudicarles

Introducción

Se suele decir que "*lo que desconoces no puede hacerte daño*". Pero esto no podría ser menos cierto en el caso de las ciberamenazas.

Lo que los usuarios desconocen sobre las ciberamenazas puede dañarles a ellos, y a su organización. Son objetivo permanente de los ciberataques. Los pasos en falso provocados por la falta de conocimientos podrían dar lugar a interrupciones de la actividad, pérdidas económicas y de datos, y daños a largo plazo.

Este libro electrónico analiza los ataques reales que evidencian el doble papel de los usuarios, como principales objetivos de los ciberdelincuentes y como defensores en primera línea.

Abarcan cinco grandes categorías de ciberataques y otros ciberdelitos que tienen relación directa o se inician con el compromiso de los usuarios:

- Phishing
- Ataques Business Email Compromise (BEC)
- Ransomware
- Ataques en la nube
- Ataques de correo electrónico basados en la web

También incluimos algunas conclusiones de nuestro informe State of the Phish 2022 que destacan los conocimientos, la vulnerabilidad y la resiliencia de los usuarios en estas áreas. Los datos tienen implicaciones claras para los responsables de la seguridad que buscan proteger a sus usuarios, sus datos y sus marcas. También subrayan abiertamente por qué las personas constituyen el nuevo perímetro y, por lo tanto, deberían estar en el centro de sus iniciativas de ciberseguridad.

SECCIÓN 1

Phishing

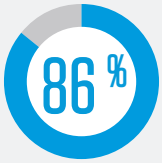
El phishing es un tipo de ingeniería social.

Distribuidos a través de mensajes de correo electrónico o de texto, los mensajes de phishing utilizan una creciente variedad de técnicas para aprovecharse de la psicología humana. Los ciberdelincuentes aprovechan la confianza de los usuarios para conseguir información financiera, credenciales de sistemas y otros datos sensibles.

Tendencias

Con el paso de los años, el phishing se ha ido convirtiendo cada vez más en una herramienta de referencia para los ciberdelincuentes. Según el *2021 Internet Crime Report* (Informe sobre delitos en Internet de 2021) del FBI, el phishing y otros ataques similares fueron responsables de más del 38 % del conjunto de los presuntos ciberdelitos denunciados en EE. UU. el año pasado. En 2021, se denunciaron 323 000 intentos de phishing. Eso supone casi 83 000 denuncias más que en 2020 y 209 000 más que en 2019[1].

La investigación para el informe *State of the Phish 2022* pone de relieve la enorme prevalencia y eficacia de los ataques de phishing. Los datos demostraron que en 2021:



de las organizaciones sufrieron ataques de phishing masivos[2]

1 de cada 5

usuarios abrieron un adjunto en ataques simulados de phishing

1 de cada 10

usuarios hicieron clic en un enlace en ataques simulados de phishing

Ejemplo real: apagón de la red eléctrica ucraniana

El diciembre de 2015, la red eléctrica de Ucrania sufrió un apagón, que dejó sin servicio durante seis horas a cerca de 225 000 personas. Fue el primer ciberataque reconocido públicamente que generó cortes de energía[3].

Los ciberdelincuentes responsables del ataque dedicaron meses a la planificación y recopilación de inteligencia. Una de las técnicas que utilizaron para poner en práctica su plan fue el phishing dirigido. En este caso, los objetivos fueron miembros del equipo de TI y administradores de sistemas de las tres empresas de distribución de energía de Ucrania (conocidas como oblenergos)[4].

1 FBI IC3. "Internet Crime Report 2021" (Informe sobre delitos en Internet de 2020), marzo de 2022. Disponible en: https://www.ic3.gov/Home/AnnualReports.

2 Proofpoint define el phishing masivo como ataques indiscriminados "comerciales" que envían el mismo mensaje de correo electrónico a muchas personas dentro de la misma organización.

3 SANS Industrial Control Systems (ICS) and Electricity Information Sharing and Analysis Center (E-ISAC). "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case" (Análisis del ciberataque contra la red eléctrica de Ucrania: caso práctico de defensa), 18 de marzo de 2016.

4 ICS and E-ISAC.

Cómo sucedió

Para comprometer estos usuarios, los ciberdelincuentes enviaron un archivo adjunto malicioso de Microsoft Word que parecía proceder de una fuente de confianza. Una vez abierto, el documento mostraba un cuadro emergente que solicitaba la activación de las macros. Si el usuario aceptaba, el malware BlackEnergy3 infectaba la máquina, proporcionando una puerta trasera a los ciberdelincuentes[5].

Estos ataques de phishing dirigido proporcionaron a los ciberdelincuentes acceso a la red de la compañía eléctrica. A partir de ahí, los atacantes dedicaron meses a infiltrarse en las redes de control industrial SCADA (control de supervisión y adquisición de datos) de las empresas para preparar su gran ataque. Utilizaron varios métodos, incluido el acceso a controladores de dominio de Microsoft Windows para recopilar incluso más credenciales de cuentas de usuario[6].

El desenlace

El apagón fue breve. Sin embargo, hicieron falta meses para que los centros de control de los oblenergos (entidades regionales de distribución) afectados volvieran a estar completamente operativos. Y como reveló un informe sobre el ataque, el incidente "sentó un nefasto precedente para la protección y seguridad de las redes eléctricas en todo el mundo"[7].

Phishing: posibles consecuencias

Cómo podría haber ayudado la concienciación de los usuarios

Como la mayoría de los ciberataques, el apagón de la red de 2015 se inició con un mensaje de correo electrónico de phishing. Después de engañar a un empleado para que abriera un adjunto infectado, los ciberdelincuentes pasaron meses recopilando inteligencia y penetrando con mayor profundidad en el entorno.

La formación para concienciar en materia de seguridad podría haber ayudado a impedir que se iniciara el ataque. El empleado no habría abierto ni interactuado con el adjunto, lo que habría impedido la entrada del ciberdelincuente.

5 Kim Zetter *(Wired)*. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" (Dentro del astuto e inaudito ataque a la red eléctrica de Ucrania), 3 de marzo de 2016.

6 Ibid.

7 Ibid.

SECCIÓN 2

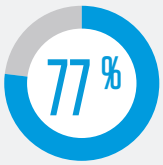
Ataques Business Email Compromise (BEC)

Los ataques Business Email Compromise (BEC) se dirigen a organizaciones de todos los tamaños y sectores.

En ellos, los atacantes se hacen pasar por una persona o entidad en la que confía el destinatario, como el director ejecutivo o un proveedor de la empresa. A partir de ahí, el ciberdelincuente convence al destinatario para que realice transferencias bancarias, desvíe nóminas, realice cambios en los datos bancarios para futuros pagos u otras acciones. Cuando la víctima detecta el error, suele ser demasiado tarde para recuperar las pérdidas.

Tendencias

Las campañas BEC pueden proporcionar pingües beneficios. El *2021 Internet Crime Report* afirma que los ataques BEC provocaron una pérdida ajustada de 2400 millones de dólares el año pasado solo en EE. UU[8]. Dada la recompensa potencial, no sorprende que el informe *State of the Phish 2022* encontrará que el 77 % de las organizaciones de todo el mundo habían sufrido ataques BEC en 2021.



de las organizaciones de todo el mundo sufrieron ataques BEC en 2021

Los ataques BEC suelen ser enormemente sofisticados, contar con una buena financiación y estar cuidadosamente planificados y estudiados[9]. Muchos atacantes centran sus esfuerzos en el fraude de facturas de proveedores debido a las considerables transacciones entre empresas que pueden interceptar. Los fraudes de facturas falsas son una táctica habitual. En estos ataques, el estafador se hace pasar por un proveedor y desvía pagos que deberían ir a los proveedores reales.

Ejemplo real: Ubiquiti pierde 46,7 M$ por fraude de proveedores

Otra estrategia BEC bien conocida, pero igualmente eficaz, es el llamado fraude del CEO, por el que los ciberdelincuentes se hacen pasar por el CEO u otro alto ejecutivo de la empresa. Por lo general, envían un mensaje de correo electrónico a alguien del departamento financiero para solicitar una transferencia de fondos (el dinero a menudo acaba en una cuenta internacional que controla el atacante).

Ubiquiti Inc. sufrió un ataque mediante este tipo de estafa BEC. Los ciberdelincuentes consiguieron sustraer 46,7 millones de dólares de la empresa tecnológica antes de que nadie se diera cuenta de que había un problema. Los usuarios con la autoridad suficiente para transferir fondos podrían no cuestionarse las solicitudes de carácter financiero procedentes de altos ejecutivos, incluso si parecen inusuales.

Cómo sucedió

A mediados de mayo de 2015, y solo unas semanas después de haberse estrenado en el puesto, el nuevo director financiero (CFO) de Ubiquiti recibió mensajes de correo electrónico en apariencia procedentes del CEO de la empresa y de un abogado de Londres. El estafador que se hacía pasar por el CEO explicaba que la empresa estaba en trámites de realizar una adquisición importante. En el mensaje se pedía al CFO la mayor discreción y que realizara varias transferencias bancarias para garantizar el éxito del acuerdo. El impostor continuó con el envío de instrucciones de correo falsas y datos bancarios, y solicitando la autorización de los pagos[10].

8 FBI IC3.

9 Proofpoint. "¡Cuidado con las estafas por correo electrónico! Un repaso de los ataques BEC de mayor envergadura, más audaces y más descarados", abril de 2022.

10 Nathan Vardi *(Forbes)*. "How a Tech Billionaire's Company Misplaced $46.7 Million and Didn't Know It" (Cómo una multimillonaria empresa tecnológica extravió 46 M$), febrero de 2016.

El desenlace

En el transcurso de 17 días, el CFO hizo 14 transferencias bancarias (por un total de 46,7 M$) a cuentas de China, Hungría, Rusia y Polonia. Entonces, a principios de junio, un agente del FBI se puso en contacto con el verdadero CEO de la empresa. Los agentes le informaron de que una gran suma de dinero había sido robada de la cuenta de la sede de Ubiquiti en Hong Kong[11]. Era la primera vez que el CEO oía hablar de las transferencias bancarias.

En agosto de 2015, Ubiquiti hizo público en un informe financiero trimestral de la Securities and Exchange Commission (SEC) de EE. UU. que había descubierto un fraude en junio, y describía el incidente como la "suplantación de empleados y solicitudes fraudulentas de una entidad externa".

Ubiquiti fue capaz de recuperar solamente parte de sus pérdidas y el daño a la reputación de la empresa fue importante. Su CFO dimitió justo antes de que la empresa hiciera público el ataque BEC. Una investigación interna concluyó que sus controles internos sobre las comunicaciones financieras eran ineficaces, y la empresa tuvo que fortalecer sus controles.

BEC: posibles consecuencias

Pérdidas económicas directas

Pérdida de datos

Cómo podría haber ayudado la concienciación de los usuarios

El fraude de proveedores y otras formas de estafas BEC son por naturaleza ataques centrados en las personas. Solamente tienen éxito cuando los destinatarios piensan que están interactuando con alguien en quien confían. De haber contado con una formación de concienciación en materia de seguridad eficaz, el CFO podría haber sabido cómo identificar los indicios reveladores de que los mensajes procedían de un impostor y no del CEO ni de los abogados de la empresa.

Combinada con controles fiscales adecuados, la formación de los usuarios puede educar a sus empleados para que detecten de manera instintiva dominios parecidos o no relacionados, URL no seguras y técnicas de ingeniería social que podrían engañar a usuarios con menores conocimientos.

11 Ibid.

12 KrebsonSecurity. "Tech Firm Ubiquiti Suffers $46M Cyberheist"
(La empresa tecnológica Ubiquiti sufre un ciberrobo por valor de 46 M$), agosto de 2015.

SECCIÓN 3

Ransomware

En esencia, el ransomware es una herramienta que permite la extorsión. Se trata de malware que bloquea los datos y los sistemas informáticos hasta que las víctimas pagan un rescate para recuperar el acceso.

Generalmente, el ciberdelincuente exige el pago en criptomonedas, como bitcoines, ya que el dinero se mueve con rapidez y es difícil de seguir. La petición a menudo viene con una fecha límite: si las víctimas no pagan a tiempo, pierden los datos para siempre o tendrán que pagar una cantidad mayor para recuperarlos. Para presionar todavía más a las víctimas, los atacantes a menudo amenazan con publicar los datos. En algunos casos, las víctimas no recuperan los datos ni pagando.

Los cifradores y bloqueadores de pantalla son los principales tipos de malware utilizados en los ataques de ransomware. Los primeros cifran los datos de un sistema, haciendo imposible utilizar su contenido sin una clave de descifrado. Los bloqueadores de pantalla utilizan una pantalla de "bloqueo" para impedir el acceso de los usuarios al sistema atacado.

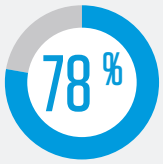
Los ataques de ransomware han existido durante décadas. Sin embargo, han captado una gran atención mediática en los últimos años debido a los grandes trastornos que provocan, los enormes pagos que exigen y la infraestructura crítica contra la que dirigen sus ataques, en especial en los sectores energético y de la atención sanitaria.

Además, han experimentado una clara evolución; los operadores de ransomware a menudo compran el acceso a grupos ciberdelictivos que se infiltran en objetivos importantes y después venden el acceso a otros por una parte de las ganancias obtenidas ilícitamente. Los grupos que ya distribuyen malware bancario u otros troyanos también pueden convertirse en parte de una red de afiliados de ransomware. El resultado es un ecosistema robusto y lucrativo en el que personas y organizaciones aumentan su nivel de especialización para optimizar los beneficios para todos, excepto claro está, para las víctimas.

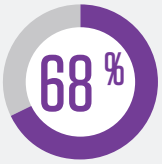
Tendencias

Los ataques de ransomware también van en aumento. El "*informe sobre investigaciones de fugas de datos de 2022*" de Verizon señala que los ataques de ransomware aumentaron un 13 % entre 2020 y 2021, tanto como en los últimos cinco años juntos[13].

A continuación presentamos algunos de los resultados del informe *State of the Phish 2022* de Proofpoint:



de las organizaciones sufrieron ataques de ransomware por correo electrónico en 2021



de las organizaciones resultaron infectadas por ransomware

de las organizaciones infectadas han pagado un rescate

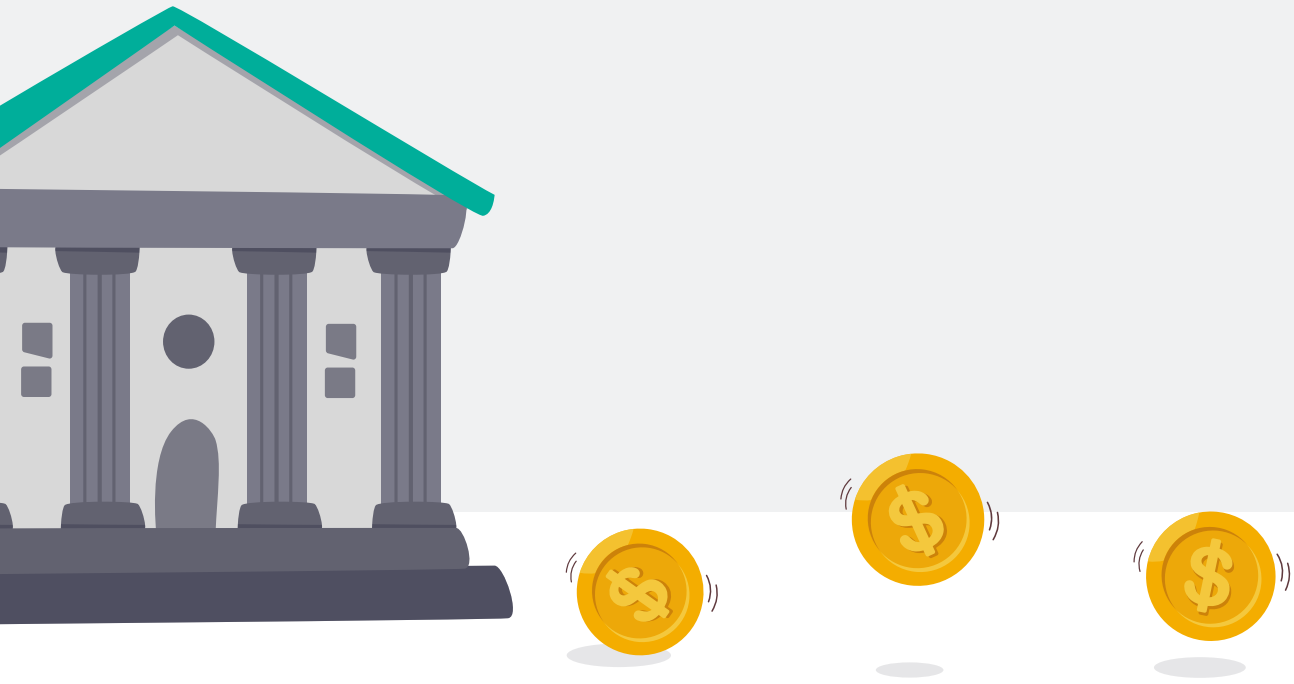
13 Verizon. "Data Breach Investigations Report" (Informe sobre las investigaciones de fugas de datos), mayo de 2022.

Ejemplo real: varios ataques de ransomware simultáneos siembran el caos en Costa Rica

Un importante ataque de ransomware golpeó al Gobierno de Costa Rica en abril, en el que se vieron afectadas cerca de 30 instituciones. Entre ellas, el Ministerio de Hacienda, la Caja Costarricense de Seguro Social e incluso el Instituto Metereológico Nacional. El grupo de ransomware Conti reivindicó la autoría de la campaña y exigió un rescate de 10 millones de dólares a cambio de no revelar la información confidencial que había extraído de los servidores del Ministerio de Hacienda antes del ataque[14].

Cuando el gobierno se negó a pagar, Conti aumentó la petición de rescate a 20 millones; poco después el grupo empezó a subir los archivos robados a su sitio web. En un intento desesperado y fallido de obtener el pago, el grupo Conti rebajó su exigencia a 15 millones[15]. Además, en un extraño y desconcertante giro de la historia, los ciberdelincuentes amenazaron con derrocar al gobierno[16].

A finales de mayo, mientras el Gobierno de Costa Rica seguía intentado recuperarse del ataque del grupo Conti, el servicio nacional de salud (CCSS) sufrió un ataque de ransomware lanzado por un grupo llamado Hive. La agencia se percató del ataque cuando sus impresoras empezaron a producir copias de la nota de rescate de Hive, que no incluía un importe[17]. Esa demanda llegaría más tarde, cuando Hive pidió a la CCSS un pago de 5 millones de dólares en bitcoines a cambio de no filtrar información confidencial[18].



14 Carly Page *(TechCrunch)*. "Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates" (Aumentan los temores entre los países pequeños después de que se intensifique el ataque de ransomware Costa Rica), 20 de mayo de 2022.

15 Carla Rosch *(Rest of World)*. "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting" (Un ciberataque masivo en Costa Rica provoca el sufrimiento de los ciudadanos), 1 de junio de 2022.

16 Matt Burgess *(Wired)*. "Conti's Attack Against Costa Rica Sparks a New Ransomware Era" (El ataque de Conti contra Costa Rica inaugura una nueva era de ransomware), 12 de junio de 2022.

17 KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions" (Costa Rica empeñada en el intento de rebautizarse del grupo de ransomware Conti para eludir sanciones), 31 de mayo de 2022.

18 Alonso Martinez *(Delfino)*. "Cybercriminals Request $5 million in Bitcoins from the CCSS" (Un grupo de ciberdelincuentes exige 5 M$ en bitcoines a la CCSS de Costa Rica), 2 de junio de 2022.

Cómo sucedió

Según los investigadores de amenazas, un miembro del grupo Conti conocido como "MemberX" utilizó credenciales robadas para conseguir acceso a través de una conexión VPN a un sistema del Ministerio de Hacienda de Costa Rica[19]. En 24 horas desde el primer ataque de Conti, los ciberdelincuentes habían cifrado los archivos del organismo público e inutilizado dos sistemas críticos: el servicio digital de impuestos y del sistema de TI del control aduanero[20].

Algunos especulan que Conti podría haber contado con ayuda interna. De hecho, un mensaje publicado por el grupo en la Internet oscura (Dark Web) afirmaba que "personal interno del gobierno [costarricense]" proporcionó ayuda, un actor de amenazas llamado "UNC1756"[21].

En el caso de Hive, el grupo utiliza un modelo de ransomware como servicio (RaaS) para sus ataques. El grupo y sus afiliados envían mensajes de correo electrónico de phishing con adjuntos maliciosos, buscan credenciales VPN, y utilizan servidores del protocolo de escritorio remoto (RDP) vulnerables para desplazarse lateralmente por la red vulnerada. Según una alerta del FBI sobre Hive, el grupo suele filtrar datos y cifrar los archivos de la red. A partir de ahí deja una nota de rescate en cada directorio afectado dentro de un sistema de la víctima. Esta nota proporciona instrucciones sobre cómo comprar el software de descifrado y amenaza con divulgar los datos de la víctima filtrados en el sitio de Tor, "HiveLeask"[22].

Algunos expertos en ciberseguridad creen que los mismos ciberdelincuentes participaron en los dos ataques de ransomware de primavera. Sugieren que Hive utilizó su campaña para ayudar a rebautizar Conti y evitar las sanciones internacionales que prohíben los pagos por extorsión a ciberdelincuentes que operan en países conocidos por tolerar (no fomentar) esta actividad[23]. Hive ha afirmado en su sitio web no tener relación con Conti[24].

El desenlace

Como resultado del primer ataque de ransomware de mediados de abril, la economía costarricense perdía unos 30 millones de dólares al día. El gobierno se vio obligado a cerrar muchos sistemas críticos durante la caótica fase de corrección. Solo la Cámara de Comercio Exterior de Costa Rica calculó pérdidas superiores a 125 millones de dólares en los primeros dos días del ataque[25].

19 Ionut Ilascu *(BleepingComputer)*. "How Conti Ransomware Hacked and Encrypted the Costa Rican Government" (Cómo el ransomware Conti pirateó y cifró datos de un número de organismos de Costa Rica), 21 de julio de 2022.

20 Matt Burgess *(Wired)*. "Conti's Attack Against Costa Rica Sparks a New Ransomware Era" (El ataque de Conti contra Costa Rica inaugura una nueva era de ransomware), 12 de junio de 2022.

21 Claudia Glover *(Tech Monitor)*. "'We will overthrow the government' – Does Conti have help inside Costa Rica?" ("Derrocaremos al gobierno" - ¿Cuenta Conti con ayuda dentro de Costa Rica?), 17 de mayo de 2022.

22 Informe FBI FLASH. "Indicators of Compromise Associated with Hive Ransomware" (Indicadores de compromiso asociados al ransomware Hive), 25 de agosto de 2021.

23 KrebsonSecurity. "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions" (Costa Rica empeñada en el intento de rebautizarse del grupo de ransomware Conti para eludir sanciones), 31 de mayo de 2022.

24 Ibid.

25 Carla Rosch *(Rest of World)*. "A Massive Cyberattack in Costa Rica Leaves Citizens Hurting" (Un ciberataque masivo en Costa Rica provoca el sufrimiento de los ciudadanos), 1 de junio de 2022.

El gobierno también tuvo que dar de baja las páginas web de las agencias atacadas. Contrató ayuda técnica de otros gobiernos, incluido el de EE. UU., y de empresas tecnológicas como Microsoft. EE. UU. ofreció incluso 5 millones de dólares por información que llevara a la detención o condena de cualquier que participara en un ataque de ransomware de Conti[26].

A principios de mayo, el nuevo presidente de Costa Rica, Rodrigo Chaves Robles, declaró el estado de emergencia de ciberseguridad, calificando el ataque de Conti un acto de terrorismo. Unas semanas después, Hive lanzó su ataque.

El Gobierno de Costa Rica tardó semanas en recuperarse. A mediados de junio, algunas agencias habían conseguido por fin reanudar su actividad.

Ransomware: posibles consecuencias

Interrupción de la actividad

Pérdida económica (consecuencia del pago de rescates y las medidas relacionadas con la corrección del ataque)

Pérdida de datos (si los atacantes cumplen las amenazas de filtrar datos si no se paga el rescate)

Cómo podría haber ayudado la concienciación de los usuarios

Algunos informes sugieren que el ataque de ransomware contra Costa Rica pudo contar con la ayuda de personal interno. Sin embargo, muchas infecciones de ransomware son consecuencia de compromisos anteriores por correo electrónico. Los ciberdelincuentes utilizan técnicas como el phishing para robar credenciales de usuarios que puedan concederles acceso a sistemas críticos.

Formar a los usuarios para que detecten y denuncien los mensajes sospechosos, especialmente en combinación con el análisis automatizado de bucle cerrado, puede reducir enormemente el riesgo de ransomware y de otras formas de malware.

Los usuarios deberían instintivamente desconfiar de adjuntos de archivos y URL, en particular los que vienen en mensajes de correo electrónico que aprovechan instintos humanos, como el beneficio personal, la curiosidad, el miedo, la indignación e incluso la indefensión. Y deberían identificar los indicios que apuntan a que el remitente podría no ser quien dice ser.

26 Elizabeth Montalbano *(Threatpost)*. "Conti Ransomware Attack Spurs State of Emergency in Costa Rica" (El ataque de ransomware de Conti obliga al gobierno a declarar el estado de emergencia en Costa Rica), 10 de mayo de 2022.

SECCIÓN 4

Ataques en la nube y usurpación de cuentas

Los ciberdelincuentes van donde van los usuarios. Y estos utilizan cada vez más la nube. La pandemia de COVID-19 ha acelerado la migración a la nube y, como consecuencia, los ataques a este entorno son cada vez más habituales. Tal y como explica nuestro *informe El factor humano 2022*, el compromiso de cuentas cloud se ha convertido en una característica sustancial y permanente del panorama de ciberamenazas, al nivel del phishing y el malware.

El compromiso de cuentas cloud consiste en hacerse con el control de la cuenta cloud de un servicio de correo web o de colaboración legítimo. Estas usurpaciones de cuentas cloud pueden ofrecer a los ciberdelincuentes acceso a una amplia variedad de datos, contactos, eventos de calendario mensajes de correo electrónico y otras herramientas del sistema. Y el abuso de una única autenticación de inicio se sesión único puede ofrecer a los ciberdelincuentes vía libre a muchos sistemas distintos del entorno, y provocar un daño generalizado.

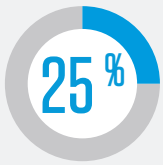
Las herramientas que suelen utilizar los atacantes para comprometer las cuentas cloud y que facilitan la usurpación son las siguientes:

- Ataques de fuerza bruta que automatizan el descubrimiento de credenciales.
- Ataques de phishing, incluido el phishing de tokens OAuth.
- Reciclado de credenciales, o *stuffing*, que emplea combinaciones de nombres de usuario y contraseñas procedentes de robos anteriores.
- Malware, como registradores de pulsaciones y ladrones de credenciales.

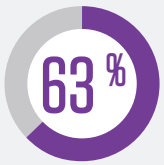
La persistencia parece ser otro ingrediente fundamental del compromiso de cuentas cloud.

Tendencias

Los datos del *informe El factor humano 2022* indican que más del 90 % de inquilinos cloud supervisados recibieron ataques todos los meses. Casi un cuarto (25 %) fueron víctimas de un ataque que consiguió su objetivo, mientras que el porcentaje total de inquilinos comprometidos en el transcurso del año fue del 63 %.



de los ataques a inquilinos de nube supervisados tuvieron éxito



fue el porcentaje de inquilinos de nube comprometidos en 2021

Las usurpaciones de cuentas cloud son a menudo difíciles de detectar, complicadas de resolver y perjudiciales para su cuenta de resultados. Un reciente estudio encontró que la pérdida económica media anual para las empresas como consecuencias del compromiso de cuentas cloud es de 6,2 millones de dólares. Las organizaciones también sufren, de media, 138 horas de tiempo de inactividad de aplicaciones por este motivo[28].

Aplicaciones cloud maliciosas

Las aplicaciones no aprobadas o shadow IT contribuyen al problema de las aplicaciones cloud maliciosas. Las aplicaciones cloud de terceros (o externas) son aquellas que se integran con un servicio cloud, pero que no las suministra el proveedor de nube. Utilizan OAuth, un protocolo de autenticación que permite a las aplicaciones obtener acceso limitado a un servicio cloud. OAuth también les permite utilizar la información de cuenta o los datos de un usuario sin mostrar sus credenciales[29].

En principio, todo parece práctico y seguro. Desafortunadamente, es relativamente fácil abusar de estas aplicaciones. Cuando las instalan, los usuarios a menudo hacen clic en "Aceptar" sin prestar atención al ámbito de los permisos. Una vez que los atacantes consiguen el acceso OAuth, pueden comprometer o secuestrar las cuentas cloud. Y lo que es peor, cuentan con acceso persistente a las cuentas y datos de los usuarios hasta que se revoque explícitamente el token OAuth.

27 Proofpoint. "El factor humano 2022", mayo de 2022.

28 Ponemon Institute. "2021 Ponemon Report: The Cost of Cloud Compromise and Shadow IT." (Informe de Ponemon 2021: Coste del compromiso de cuentas cloud y las shadow IT), abril de 2021.

29 Proofpoint. "Lo que todos los profesionales de la seguridad deberían saber sobre las aplicaciones OAuth de terceros", mayo de 2022.

Archivos maliciosos almacenados en la nube

Una vez que el atacante se apodera de una cuenta cloud, puede cargar archivos maliciosos para preparar el terreno para otras actividades maliciosas, como el robo de datos o el fraude de transferencias bancarias. Por ejemplo, en una estrategia de phishing de Microsoft SharePoint, un ciberdelincuente subió un archivo malicioso a una cuenta cloud comprometida. Los permisos de uso compartido de archivos se cambian a "Públicos", para que el nuevo enlace anónimo pueda compartirse con cualquiera. A partir de ahí, el atacante envía mensajes de correo electrónico o comparte el enlace con los contactos del usuario comprometido u otros objetivos. Una vez que los destinatarios abren el archivo y hacen clic en el enlace malicioso, quedan infectados[30].

Nuestros investigadores de amenazas descubrieron recientemente un nuevo giro en los ataques cloud: los ciberdelincuentes persiguen los datos en la nube y lanzan ataques tipo ransomware a través de infraestructura de la nube. Y en el proceso comprometen aplicaciones cloud empresariales de uso generalizado, como SharePoint Online y OneDrive dentro de la suite Microsoft 365[31].

A pesar del peligro evidente que los archivos comprometidos por un atacante presentan para la nube, el informe *State of the Phish 2022* descubrió que solo el 37 % de los usuarios saben que los archivos almacenados en la nube pueden ser maliciosos.

Ejemplo real: campaña OiVaVoii

La nube facilita la colaboración y el uso compartido de datos. Pero además es un entorno de amenazas complejo, que crece rápidamente en medio de la transformación digital y el trabajo remoto e híbrido.

Una reciente campaña contra usuarios de alto valor, incluidos miembros del consejo de administración, demostró por qué los usuarios de todo el escalafón corporativo deben tener cuidado a la hora conceder permisos a las aplicaciones cloud. Esto es así incluso si esas apps parecen inofensivas y de remitentes legítimos.

30 Itir Clarke, Eilon Bendet y Doyle Groves. *(Proofpoint)*. "Why OneDrive and SharePoint Attacks Are Successful and How to Fight Back" (El éxito detrás de los ataques contra OneDrive y SharePoint y cómo combatirlos), octubre de 2020.

31 Or Safran, David Krispin, Assaf Friedman y Saikrishna Chavali *(Proofpoint)*. "Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive" (Proofpoint descubre una funcionalidad de Microsoft 365 potencialmente peligrosa que puede secuestrar archivos almacenados en SharePoint y OneDrive), junio de 2022.

Cómo sucedió

En enero de 2022, nuestros investigadores observaron por primera vez una campaña maliciosa contra la nube híbrida, OiVaVoii, y descubrieron cinco aplicaciones OAuth maliciosas asociadas a ella[32].

Al menos tres de las apps externas maliciosas fueron diseñadas por dos "creadores verificados". Esos creadores eran con toda probabilidad cuentas de usuarios administrativas comprometidas dentro de inquilinos de Microsoft 365 legítimos. De las dos aplicaciones restantes, al menos una fue diseñada por un creador no verificado. Esto sugiere que los ciberdelincuentes estaban utilizando un tercer entorno de nube pirateado o inquilino de Microsoft 365 malicioso dedicado.

El desenlace

Una vez que los atacantes habían creado las apps, enviaban la solicitud de autorización a través del correo electrónico a varios usuarios, incluidos altos ejecutivos. Muchos de esos usuarios autorizaron las apps. Esa sencilla acción permitió a los ciberdelincuentes generar tokens OAuth en nombre de los usuarios atacados y consumar la usurpación de cuentas. Todas las apps asociadas a la campaña OiVaVoii solicitaron permisos similares de los usuarios, principalmente para acceso a buzones de correo (lectura y escritura). Una vez que los usuarios aceptaron las solicitudes, los ciberdelincuentes tuvieron libertad para enviar mensajes de correo electrónico maliciosos interna y externamente, robar información sensible, etc.

Ataques en la nube: posibles consecuencias

Usurpación de cuentas

Pérdida de datos
(como consecuencia de malware que accede al entorno o por sustracción directa de datos por parte de apps maliciosas)

Interrupción de la actividad
(por ransomware y otros tipos de malware que acceden al entorno)

Cómo podría haber ayudado la concienciación de los usuarios

Como en la mayoría de los ataques por correo electrónico, los ataques basados en la nube dependen de la interacción humana para que, de forma inconsciente cedan sus credenciales, instalen apps maliciosas y hagan clic en sitios web de uso compartido de archivos de confianza para alojar archivos maliciosos.

Formar a las personas para que utilicen de forma segura los servicios cloud, y presten atención a la hora de autorizar apps desconocidas debería ser una parte crítica de su programa de concienciación en materia de seguridad.

32 Eilon Bendet, Assaf Friedman y David Krispin *(Proofpoint).* "OiVaVoii – An Active Malicious Hybrid Cloud Threats Campaign" (OiVaVoii - Una campaña de amenazas contra la nube híbrida muy activa), enero de 2022.

Por qué la autenticación multifactor no es una solución milagrosa

Muchas organizaciones concienciadas con la seguridad enseñan a sus empleados a utilizar la autenticación multifactor (MFA) como herramienta para ayudar a proteger las cuentas de los usuarios, y con razón. MFA es otra capa de seguridad que ayuda a proteger las cuentas cuando un atacante intenta iniciar sesión con credenciales robadas. Al iniciar la sesión, se obliga al usuario a introducir no solo su nombre de usuario y su contraseña, sino además un código desde su teléfono, tarjeta de acceso o llave de seguridad física. MFA reduce enormemente las posibilidades de que los ciberdelincuentes puedan comprometer cuentas a través de credenciales robadas solamente, y debería formar parte de todos los programas de seguridad.

Pero no es infalible. Los kits de phishing de uso fácil se lo ponen muy sencillo a los ciberdelincuentes a la hora de eludir estas protecciones. Microsoft afirma que los ciberdelincuentes consiguieron eludir la autenticación MFA en ataques que se dirigieron contra más de 10 000 organizaciones desde septiembre de 2021. Una vez que los atacantes consiguieron acceder, utilizaron las cuentas comprometidas para lanzar ataques BEC[33].

Estos ataques generalmente empiezan por un mensaje de correo electrónico de phishing, por lo que resulta fundamental enseñar a los usuarios a identificar y denunciar los mensajes sospechosos. En el ataque de Microsoft, los mensajes de phishing incluían un adjunto HTML. Al abrirlo, el archivo redirigía a los usuarios a un servidor proxy que interceptaba el tráfico entre los usuarios y la pantalla de inicio de sesión.

Los usuarios también deberían saber que jamás tienen que abrir archivos adjuntos procedentes de remitentes desconocidos. Esto es especialmente importante en los tipos de archivos que normalmente no se envían por correo electrónico.

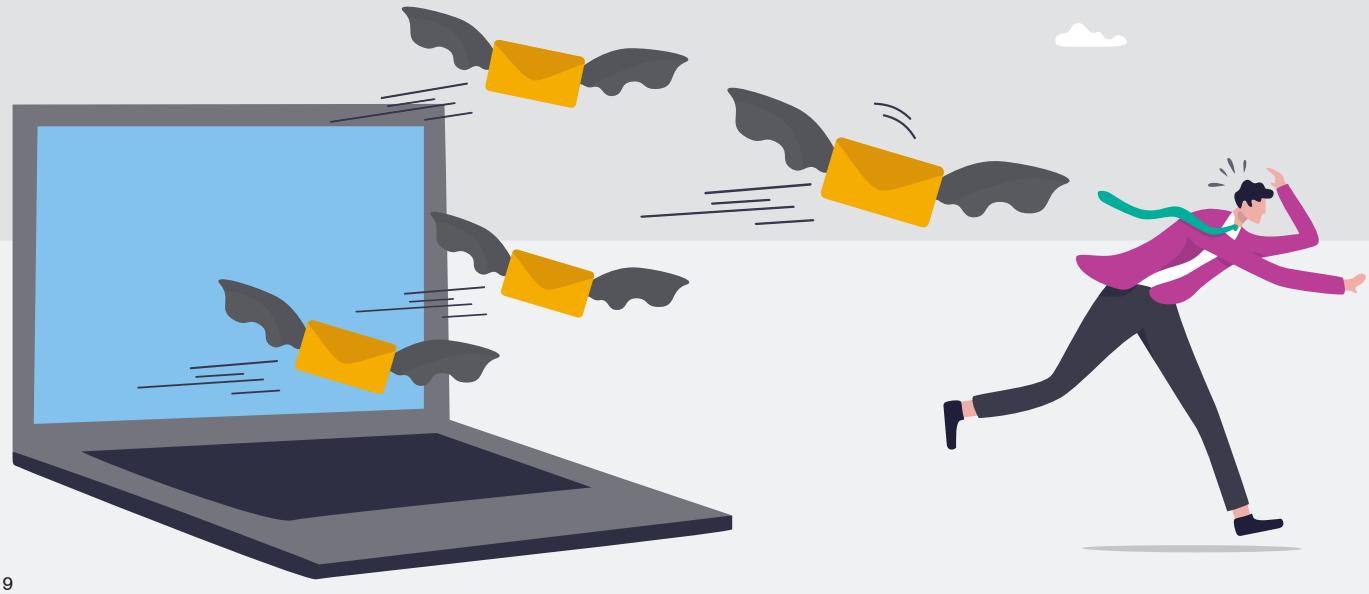
33 Microsoft. "From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud" (Del robo de cookies a estafas BEC: los ciberdelincuentes utilizan sitios de phishing de AiTM como punto de entrada para cometer fraude financiero), julio de 2022.

SECCIÓN 5

Ataques de correo electrónico basados en la web

El auge del teletrabajo ofrece a los ciberdelincuentes todavía más oportunidades de conseguir acceso a los sistemas empresariales. La mayoría de los empleados utilizan redes privadas virtuales (VPN) para acceder a la red de su empresa cuando trabajan fuera de la oficina. Y también utilizan sus propios dispositivos para conectarse a recursos empresariales. Estos son los mismos dispositivos que utilizan para acceder a sus cuentas de correo electrónico web personales. Por el contrario, muchos trabajadores utilizan dispositivos de la empresa para acceder a sus cuentas personales.

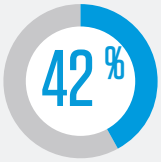
Si los ciberdelincuentes comprometen cuentas no relacionadas con el trabajo de un usuario, pueden encontrar sus credenciales para las aplicaciones, datos y sistemas de la empresa. También pueden aprovechar el hecho de que muchos empleados utilizan sus cuentas de correo personales o números móviles para la autenticación de dos factores o el restablecimiento de contraseñas. Con esa información en su poder, los atacantes no tienen que hacer mucho para acceder a las redes corporativas.



Tendencias

Los datos recopilados para el informe *State of the Phish 2022* sugieren la existencia de muchos usuarios en riesgo de ataques por correo electrónico basados en la nube que podrían provocar daños a sus empleadores.

Además, todo indica que muchos usuarios podrían dar por sentado que sus proveedores de correo web les protegen frente a estos ataques.



de los usuarios acceden al correo electrónico personal en dispositivos de la empresa.

de los usuarios saben que su proveedor de correo electrónico personal no puede bloquear todos los mensajes peligrosos

Nuestra investigación descubrió que:

Ejemplo real: LAPSUS$

En ocasiones, lo que importa a los ciberdelincuentes tanto o incluso más que ganar dinero es provocar trastornos y atraer la mayor atención posible. Eso describe perfectamente a la red de extorsión LAPSUS$, que surgió a finales de 2021. Se cree que el grupo podría estar todavía activo a pesar de que varios de sus miembros (todos ellos con edades comprendidas entre los 16 y los 21 años) fueron arrestados por la policía británica en marzo[24].

Cómo sucedió

En unos pocos meses, el grupo intentó extorsionar al Ministerio de Sanidad de Brasil y publicó capturas de pantalla de herramientas internas relacionadas con NVIDIA, Samsung y Vodafone[35]. Llamó la atención por su nada convencional método de extorsión. Robaba datos sensibles y entonces amenazaba con publicarlos en Internet a menos que la víctima pagara. Básicamente, se trataba de un ataque de ransomware, pero sin ransomware.

El desenlace

El grupo era tan descarado que realizaba encuestas entre los usuarios en la app Telegram para que votaran el tipo de datos de la víctima que deberían publicar a continuación[36]. Para conseguir acceder a las redes de la empresa en la que querían infiltrarse, LAPSUS$ a menudo atacaba las cuentas de correo electrónico personales de los empleados para buscar credenciales y sistemas que permitieran el acceso remoto[37].

34 Scott Ikeda *(CPO Magazine)*. "Suspected Lapsus$ Hackers Arrested; London Group Between the Ages of 16 and 21" (Detenidos hackers supuestamente miembros de LAPSUS$; un grupo radicado en Londres con edades entre los 16 y los 21 años), marzo de 2022.

35 KrebsonSecurity. "A Closer Look at the LAPSUS$ Data Extortion Group" (Análisis detallado de la red de extorsión de datos LAPSUS$), marzo de 2022.

36 Lily May Newman *(Wired)*. "The Lapsus$ Hacking Group Is Off to a Chaotic Start" (El grupo de hackers LAPSUS$ tiene un comienzo caótico), marzo de 2022.

37 Microsoft. "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction" (El grupo de ciberdelincuentes DEV-0537 busca la filtración y destrucción de datos de las organizaciones que ataca), marzo de 2022.

Los equipos de Microsoft Security se refieren al grupo LAPSUS$ como "DEV-0537".

"A diferencia de la mayoría de grupos ciberdelictivos, que intentan pasar desapercibidos, DEV-0537 no parece cubrir sus huellas", afirma el gigante de software. "Llega incluso a anunciar sus ataques en redes sociales o publicitar su intento de comprar credenciales de empleados de las organizaciones en su punto de mira"[38].

La "publicidad" del grupo incluía mensajes de Telegram en los que LAPSUS$ intentaba reclutar empleados y otros agentes internos en empresas de telecomunicaciones, de software y de juegos, operadoras de centros de llamadas y hosts de servidores. Su objetivo: sobornar a los empleados para obtener credenciales VPN u otra forma de acceso remoto. LAPSUS$ también ofrecía dinero a los empleados que colaboraran. Uno de los anuncios describía una oportunidad de ganar 20 000 dólares a la semana[39].

Microsoft Security también ha comunicado que LAPSUS$ consiguió acceso inicial a las víctimas por otros métodos. Uno de ellos fue la compra de credenciales y tokens de sesión en foros clandestinos de ciberdelincuencia. Otro método fue la búsqueda de repositorios de códigos públicos para credenciales expuestas.

Ataques de correo electrónico basados en la nube: posibles consecuencias

Pérdida de datos | Interrupción de la actividad | Pérdida económica | Daños a la reputación

Cómo podría haber ayudado la concienciación de los usuarios

El grupo LAPSUS$ utilizó varias tácticas, concretamente:

- Compromiso de correo electrónico web y acceso remoto
- Reclutamiento de empleados, proveedores o partners comerciales de la empresa
- Robo de datos confidenciales y propiedad intelectual
- Peticiones de rescate

Formar a los usuarios para que fueran capaces de proteger sus credenciales, utilizar su correo electrónico personal con seguridad e informar de las peticiones de rescate habría ayudado mucho.

38 Ibid.

39 KrebsonSecurity. "A Closer Look at the LAPSUS$ Data Extortion Group" (Análisis detallado de la red de extorsión de datos LAPSUS$), marzo de 2022.

SECCIÓN 6

Conclusiones y recomendaciones

El reto es determinar la mejor manera de formar a sus empleados sobre un panorama de amenazas en constante evolución, y mantenerlos informados. En última instancia, su objetivo es motivarlos para que permanezcan tan vigilantes frente a las ciberamenazas como sus equipos de seguridad. A partir de ahí pueden convertirse en defensores proactivos.

Para que funcione la formación para concienciar en materia de seguridad, los usuarios necesitarán comprender la pregunta "¿qué importa?" ¿Por qué deben preocuparse por las ciberamenazas? ¿Por qué defender su organización es en parte su responsabilidad? La respuesta sencilla es que ellos constituyen el nuevo perímetro. Y para que la organización tenga la más mínima oportunidad de mantener a raya a los ciberdelincuentes modernos, debe adoptar un enfoque centrado en las personas de la seguridad.

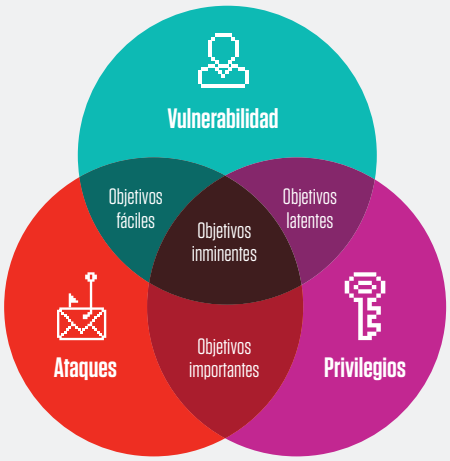
Los cinco tipos de ciberamenazas y ejemplos de ataques abordados en este libro electrónico tienen un denominador común: se dirigen contra las personas. Los atacantes consiguen la ayuda de los usuarios (voluntaria o involuntariamente) para impulsar sus campañas y conseguir sus objetivos.

Estas amenazas e incidentes ayudan a demostrar que las personas son el factor fundamental del panorama de amenaza actual. Por eso, la formación para concienciar en materia de seguridad de los usuarios debería ser un elemento central de su estrategia de ciberseguridad.

Priorice lo que importa

Todos los que pueden influir en el estado de ciberseguridad de la organización deben aprender buenas prácticas de ciberseguridad. Pero debe adoptar medidas deliberadas y estratégicas para evaluar y formar a su plantilla.

Además, dé prioridad a los temas que sepa que son importantes para su sector y empresa, así como para las personas que trabajan en ella. Considere el uso de los ejemplos reales incluidos en este libro electrónico para ayudarle a conectar con los usuarios para los que más impacto puedan tener estos sucesos. La razón está en que con total seguridad tendrán que enfrentarse a ataques similares por la naturaleza de su cometido, función, lugar y método de trabajo u otros factores.



Utilice a su favor la inteligencia sobre amenazas

La inteligencia sobre amenazas puede ayudarle a decidir cuándo impartir un curso concreto a determinadas personas. Para aprovechar a su favor la información detallada sobre las amenazas conocidas y emergentes, resulta fundamental identificar a los siguientes tipos de usuarios:

Usuarios muy vulnerables: en función de su comportamiento, su propensión a hacer clic en mensajes de correo de phishing simulados y su participación en cursos de formación.

Usuarios muy atacados: los que reciben un gran volumen de ataques, sobre todo ataques sofisticados, muy dirigidos o una combinación de ambos.

Usuarios con muchos privilegios: los que tienen acceso a datos valiosos, sistemas y otros recursos críticos que la organización debe proteger.

En pocas palabras, un enfoque eficaz de seguridad centrado en las personas requiere que los empleados y departamentos de su organización sepan que reciben ataques y son objetivo en un momento dado. Esto también significa conocer los métodos que utilizan los ciberdelincuentes para intentar comprometer a los usuarios y el entorno.

Evalúe permanentemente los parámetros de concienciación en seguridad claves para medir su éxito

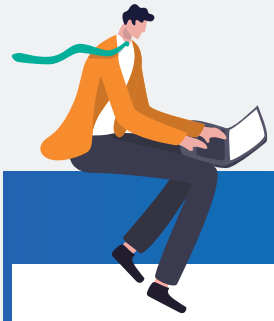
Evite encasillar su visión del éxito de la formación en un solo parámetro, como las tasas de fallos de las pruebas de phishing. La medida del "éxito" debe incluir múltiples componentes y tener en cuenta factores propios de la empresa.

Sugerimos utilizar los siguientes parámetros:

- Fallos en simulaciones de phishing
- Denuncias de simulaciones de phishing
- Evaluaciones de conocimientos
- Precisión de mensajes denunciados
- Participación en formación

A modo de último consejo, recuerde que la formación para concienciar en materia de seguridad necesita evolucionar para no quedarse atrás ante el cambiante panorama de las amenazas. Asegúrese de que la orientación que ofrece es relevante para los usuarios, ya que su organización también cambia constantemente. Los parámetros descritos anteriormente pueden ayudar a medir de manera continua la eficacia de sus programas y ajustarlos en caso necesario.

Para obtener más detalles sobre estrategias para mejorar sus programas para concienciar en materia de seguridad, descargue el informe *State of the Phish 2022* de Proofpoint.



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:

- **75 %** DEL FORTUNE 100
- **60 %** DEL FORTUNE 1000
- **30 %** 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**.