MANUAL DE INGENIERÍA SOCIAL

¿Cómo actuar de la manera correcta?

Contenido

¿Por las PYME deberían preocuparse por los ataques de ingeniería social?

Las PYME son cada vez más conscientes de que se han convertido en objetivo de los ciberdelincuentes. Según la encuesta de 2019 que realizó Zogby Analytics por encargo de la Alianza Nacional de Ciberseguridad de los Estados Unidos, casi la mitad (44%) de las empresas con entre 251 y 500 empleados afirmaron haber sufrido una vulneración de datos oficial en los últimos 12 meses. La encuesta reveló que el 88% de las pequeñas empresas creen que son al menos un objetivo "algo probable" para los ciberdelincuentes, incluyendo a casi la mitad (46%) que creen que son un objetivo "muy probable".

El daño es real y extenso, lo que queda claramente reflejado en el informe anual del Centro de Denuncias sobre Delitos por Internet (IC3) del FBI. Tan solo en 2020, el IC3 recibió 19.369 denuncias de compromiso del correo electrónico corporativo (BEC)/compromiso de cuentas de correo electrónico (EAC), con pérdidas calculadas de más de 1.800 millones de dólares. Para quienes no lo saben, los ataques BEC y EAC son estafas sofisticadas dirigidas tanto a empresas como a particulares para realizar transferencias de fondos.

El 33% de las vulneraciones incluyeron ataques mediante ingeniería social, la segunda táctica más utilizada después del hacking, afirma el Informe de Investigaciones sobre Vulneraciones de Datos 2019.

Tras sufrir una vulneración,

37%

de las PYME experimentaron una pérdida financiera

25%

de las PYME se declararon en quiebra

10%

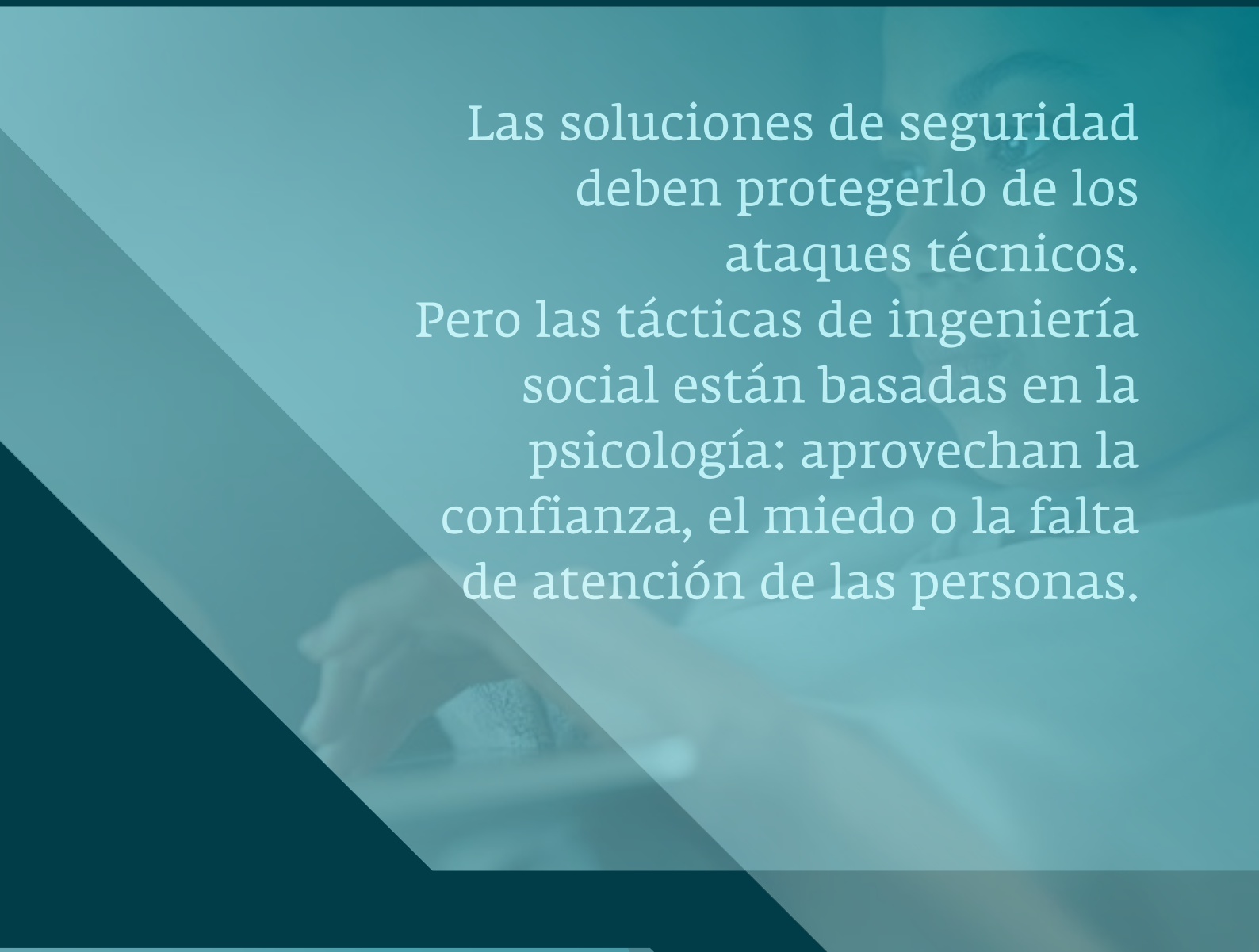
de las PYME cerraron la empresa

Fuente: NCSA

Introducción

El objetivo de este manual es ayudarlo a presentar el tema de la ingeniería social y sus riesgos a todos los empleados de la empresa. Los humanos somos seres emocionales, y la ingeniería social es una forma muy eficaz de aprovecharse de ello. Es más, los ataques de ingeniería social no suelen requerir conocimientos técnicos demasiado específicos por parte del atacante. A decir verdad, forzar a miles de usuarios a entregar información confidencial o a realizar acciones perjudiciales hasta ahora ha resultado bastante sencillo.

En las siguientes páginas, encontrará información general sobre las tendencias en ingeniería social, así como ejemplos de los tipos de ataques más comunes que pueden afectar la forma en que los empleados actúan online. También aprenderá a reconocer estos ataques y a protegerse a sí mismo y a su empresa.



Las soluciones de seguridad deben protegerlo de los ataques técnicos. Pero las tácticas de ingeniería social están basadas en la psicología: aprovechan la confianza, el miedo o la falta de atención de las personas.

Técnicas de ingeniería social

Phishing dirigido (o spear phishing)
Es un ataque dirigido a una persona, organización o empresa específica, a diferencia de las campañas típicas de phishing, que no están dirigidas a las víctimas en forma individual, sino que a cientos de miles de destinatarios.

Phishing de voz (o vishing)
Es un método similar al phishing pero que utiliza llamadas telefónicas fraudulentas en lugar de emails, en las que los ciberdelincuentes suelen hacerse pasar por representantes de bancos o compañías de seguros.

Phishing por SMS (o smishing)
Es un intento de ingeniería social que se lleva a cabo a través de SMS. En la mayoría de los casos, tiene como objetivo redirigir a los destinatarios a un sitio web donde se recopilan sus datos. Sin embargo, también hay campañas en las que se pide a las víctimas que envíen datos confidenciales directamente respondiendo con otro SMS.

(S)extorsión
La (S)extorsión es una estafa por correo electrónico que intenta chantajear a las víctimas mediante reclamos y acusaciones sin fundamento.

Suplantación de identidad
Esta técnica es la misma que en el mundo físico. Los ciberdelincuentes se ponen en contacto con los empleados, normalmente haciéndose pasar por su CEO (director general), e intentan manipularlos para que realicen alguna acción, como solicitar y aprobar transacciones fraudulentas.

Scareware
Es un software que utiliza diversas técnicas para generar ansiedad en las víctimas y obligarlas a instalar más códigos maliciosos en sus dispositivos. Por ejemplo, un falso producto antivirus engaña a los usuarios para que instalen un software específico que eliminaría el problema, pero en realidad se trata de un programa dañino.

Estafas de soporte técnico
Los atacantes intentan vender servicios falsos, eliminar problemas inexistentes o instalar una solución de acceso remoto en los dispositivos de las víctimas para obtener acceso no autorizado a sus datos.

Phishing

Probablemente, en algún momento, habrá recibido un email que parece provenir de un banco o de algún servicio popular online, donde se le pide que confirme sus credenciales o el número de su tarjeta de crédito. Esta es una técnica de phishing muy común. Sin embargo, las trampas de phishing cambian constantemente y a veces son difíciles de reconocer.

El phishing es una forma de ataque de ingeniería social en la que el atacante intenta acceder a las credenciales de inicio de sesión, obtener información confidencial o descargar malware. Las campañas de phishing pueden dirigirse a un gran número de usuarios en forma anónima, o también a una víctima específica o a un pequeño grupo de víctimas relacionadas, mediante una estafa personalizada (phishing dirigido). Los ataques centrados en individuos específicos (principalmente empresarios de alto perfil, como directores o propietarios de empresas) también se denominan "whaling" (del inglés, "caza de ballenas"), ya que los atacantes van tras "el pez gordo".

Los estafadores saben que es muy probable que su proveedor analice los mensajes en busca de contenido malicioso y los desvíe a la carpeta de correo no deseado. Es por eso que el contenido de los mensajes fraudulentos cambia con tanta frecuencia.

Según Google, los estafadores enviaron 18 millones de emails de suplantación de identidad sobre COVID-19 a los usuarios de Gmail por día en marzo de 2020.

Phishing

Desde que comenzó a desatarse la pandemia de COVID-19, los estafadores no han perdido el tiempo para intentar sacar provecho de la incertidumbre, el miedo y la escasez de suministros relacionados con la crisis. En marzo de 2020, se produjo una avalancha de spam con la temática de COVID-19, que propagaba malware y phishing para obtener información confidencial, u ofrecía productos falsos, tal y como revela el Informe de Amenazas de ESET del primer trimestre de 2020.

No es de extrañar que la pandemia se haya convertido en uno de los principales señuelos utilizados por los atacantes. La llegada de cualquier crisis trae consigo nuevas circunstancias que proporcionan un entorno ideal para que los ciberdelincuentes puedan innovar.

El 94% del malware se envía por correo electrónico.

Cada minuto se pierden 17.700 dólares por ataques de phishing.

Cada día se envían unos 14.500 millones de correos electrónicos de spam.

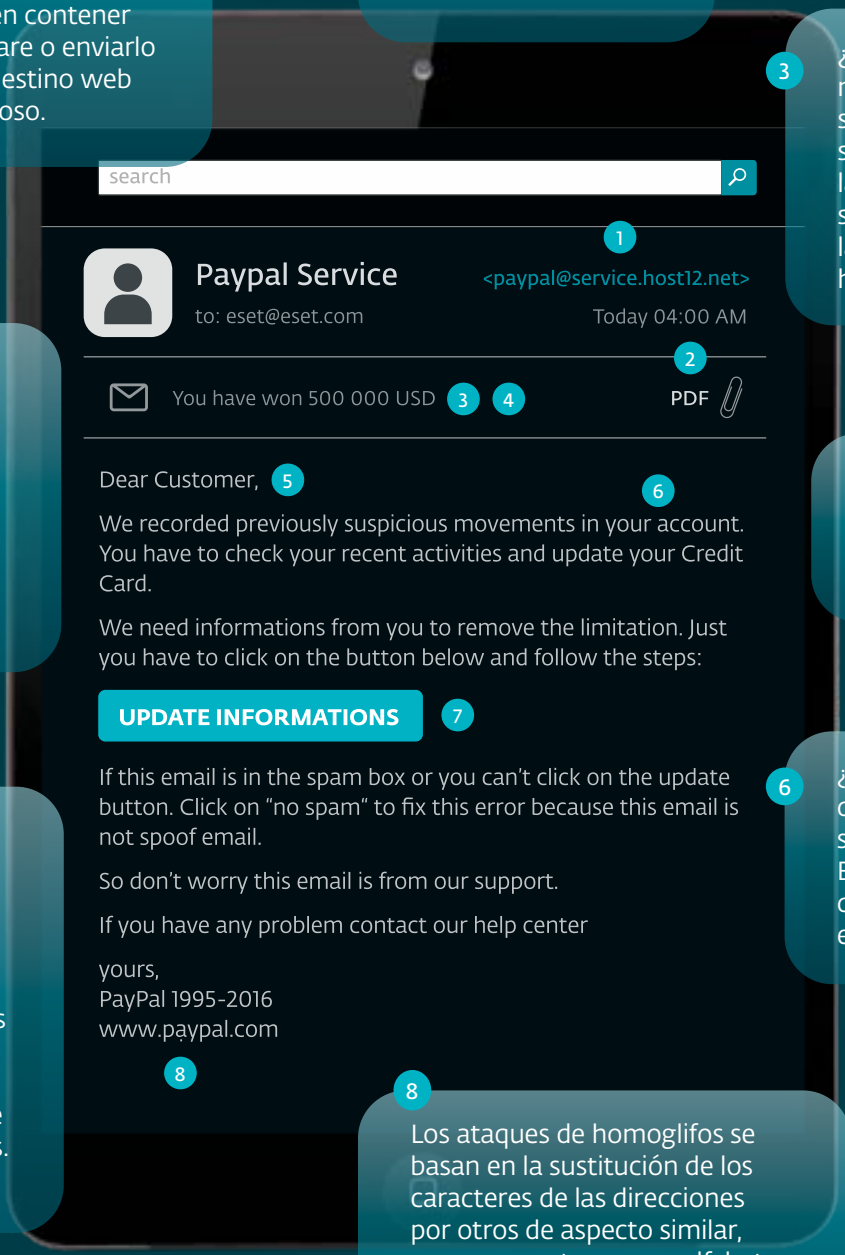
Fuentes: CSO, hostingtribunal.com

Características básicas del phishing

1 Si la dirección del email no le resulta familiar, maneje el contenido con precaución.

2 Espere lo peor de los adjuntos y de los links desconocidos. Pueden contener malware o enviarlo a un destino web malicioso.

3 ¿Da miedo o es muy bueno para ser verdad? Seguro sea una estafa, la ingeniería social se basa en las debilidades humanas.



4 El asunto no concuerda con el mensaje.

5 Si el saludo es general, puede ser una señal de que no va dirigido solo a usted, sino también a otras personas.

6 ¿La urgencia del mensaje es sospechosa? El estafador quiere que entre en pánico.

7 La mala ortografía y otros errores gramaticales son comunes en los correos de phishing que se tradujeron de otros idiomas.

8 Los ataques de homoglifos se basan en la sustitución de los caracteres de las direcciones por otros de aspecto similar, pero que pertenecen a alfabetos diferentes (como "ạ" en vez de "a" en paypal.com).

Phishing por SMS

El phishing por SMS es un tipo de phishing que utiliza el servicio de mensajería de texto. Este método también se hizo extensivo durante los primeros meses de la pandemia de COVID-19. En épocas confusas, por ejemplo, la gente empezó a recibir SMS que simulaban ser mensajes oficiales de sus gobiernos locales.

El objetivo de estos ataques es similar al del phishing: los ciberdelincuentes intentan obtener sus datos personales u obligarlo a hacer clic en un enlace a un sitio web malicioso. Los ciberdelincuentes envían SMS pidiendo una donación para personas en situaciones desesperadas, normalmente solicitando los datos de la tarjeta de crédito.

Al principio, a mucha gente le sorprendió que los hackers pudieran obtener sus números de teléfono sin su conocimiento. Pero como han señalado muchos expertos en ciberseguridad, es más fácil conseguir el número de teléfono de alguien que su correo electrónico, porque hay una cantidad finita de opciones de números telefónicos. En cambio, adivinar los nombres de las direcciones de correo electrónico es más difícil porque admiten más caracteres.

¿Qué tiene este SMS de sospechoso?

Un banco probablemente nunca le enviaría un enlace directo como este. Si no está convencido, puede ir a su banca online y comprobar si recibió el mismo mensaje allí. Siempre es más seguro ir a un sitio web oficial que hacer clic en un enlace sospechoso.

Vishing

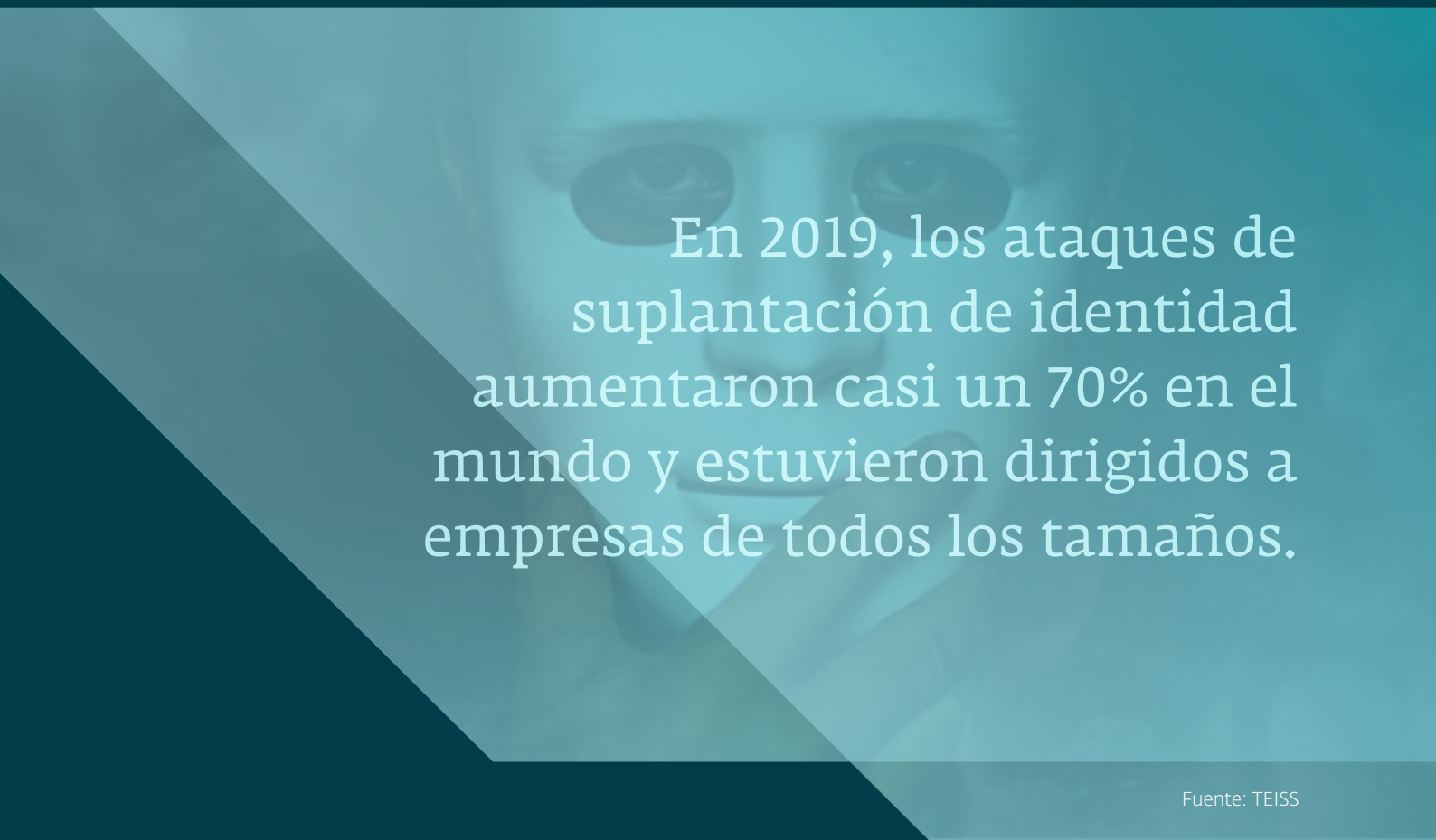
El **Vishing** requiere una capacidad de actuación aún mayor que otros tipos de estafa. Suele ocurrir así: Lo llama por teléfono un **estafador haciéndose pasar por el representante de una institución oficial**. Le informa que su cuenta bancaria fue comprometida o que tiene disponible un préstamo no solicitado en un intento de obtener su información personal y sus datos financieros. ¿Es demasiado bueno? Pídale más detalles y no comparta ningún dato confidencial de inmediato. También puede terminar la llamada y ponerse en contacto usted mismo con el servicio de atención al **cliente del banco, explicando la situación.**

Suplantación de identidad: Cuando un atacante se hace pasar por el CEO

La suplantación de identidad es otro método de ataque no técnico, utilizado por los ciberdelincuentes para hacerse pasar por personas de confianza mientras intentan manipular a otros. ¿Cómo puede reconocer si la persona que se puso en contacto con usted es un atacante en vez de su colega?

La suplantación de identidad se define como la práctica de hacerse pasar por un tercero, en este caso, para obtener información o acceso a una persona, empresa o sistema informático. Para lograr estos objetivos, los ciberdelincuentes hacen llamadas telefónicas, envían correos electrónicos o utilizan aplicaciones de mensajería, entre otros métodos. En muchos casos, los atacantes eligen nombres de la alta dirección de la empresa y confeccionan un correo electrónico que parece escrito por un gerente.

Es increíble la cantidad de información corporativa disponible en plataformas como LinkedIn que revelan la estructura de la empresa y los nombres de sus empleados. Un atacante puede utilizar estos datos para intentar contactarse con varios empleados de la empresa, pidiéndoles que realicen transferencias de dinero, paguen facturas o envíen datos importantes. Por eso la suplantación de identidad puede ser tan peligrosa para las empresas, ya que estos ataques podrían provocar una vulneración de datos y pérdidas financieras.

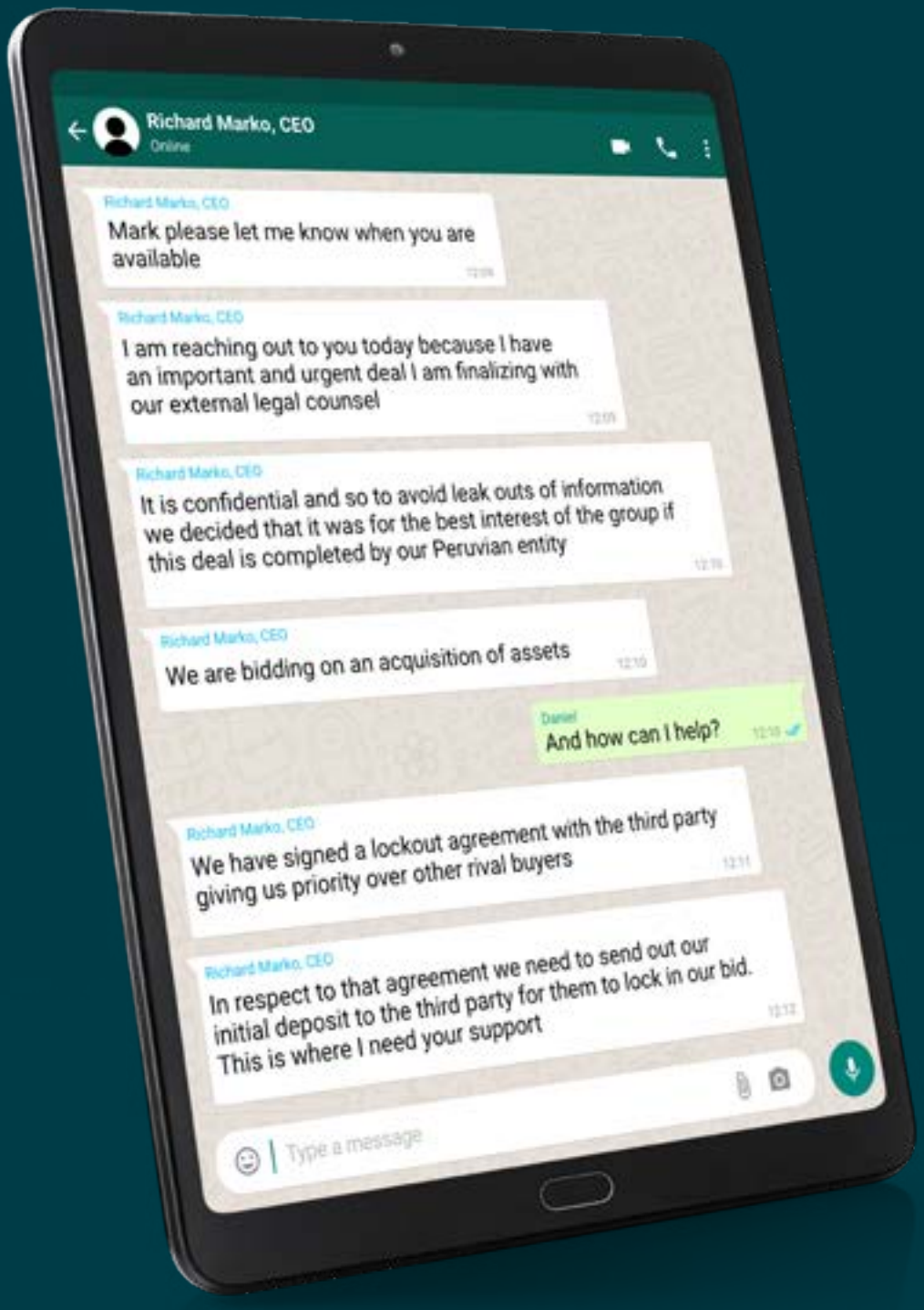


En 2019, los ataques de suplantación de identidad aumentaron casi un 70% en el mundo y estuvieron dirigidos a empresas de todos los tamaños.

Fuente: TEISS

Una historia real: Ataque de suplantación de identidad contra ESET

Los ciberataques pueden afectar a cualquier organización. En 2020, ESET se enfrentó a intentos de suplantación de identidad del CEO a través de mensajes de WhatsApp. El objetivo de estos intentos era fingir la existencia de una importante licitación que requería un depósito financiero.



Cómo detectar los ataques de suplantación de identidad

Cuanto más sepamos sobre los ataques de suplantación de identidad, mejor podremos evitarlos. Muchos intentan infundir una sensación de urgencia y miedo en sus víctimas. Ese sentimiento los lleva a a realizar la tarea deseada. Puede tratarse de algo que le parezca inusual y sospechoso, como compras que no estén relacionadas con su negocio o clientes que no reconoce. Los ciberdelincuentes también tratan de imponer un plazo corto para las tareas requeridas.

Los mensajes fraudulentos suelen contener errores gramaticales o usar incorrectamente la marca corporativa. Los atacantes más hábiles en la suplantación de identidad avanzada podrían crear un mensaje de email que se vea muy real, incluyendo una foto oficial de un empleado o una firma al final del mensaje. Por lo tanto, aunque la plantilla parezca legítima, tenga cuidado si lo que le pide el mensaje le resulta extraño.

PIENSE EN EL CONTEXTO

Tal vez se necesiten unos segundos más, pero siempre hay que plantearse si el correo electrónico tiene sentido. ¿Por qué exactamente este colega me está pidiendo que haga esta compra en particular o que le de esta información personal confidencial? Cualquier cosa inusual y que se desvíe de los procesos tradicionales debería ser una señal de alarma. Incluso cuando el correo electrónico aparentemente procede de una persona de confianza, como el CEO, podría ser un fraude. Manténgase alerta y verifique cualquier pedido con otros colegas.

¿FUERA DE LA OFICINA?

A veces, los ciberdelincuentes pueden saber que alguien no está en la oficina y actúan en su nombre. En ese caso, verifique la información en cuestión con su superior o sus compañeros de trabajo. Como dice el refrán, hay que mirar antes de saltar.

Cómo detectar los ataques de suplantación de identidad

COMPRUEBE LA DIRECCIÓN DE CORREO ELECTRÓNICO

¿Recibió un email corporativo desde una cuenta personal? La dirección quizá parezca pertenecer a alguien conocido. Pero siempre es mejor responder a esa persona a su email oficial. Además, los hackers pueden utilizar un correo electrónico que a simple vista se asemeja a la dirección corporativa oficial con una pequeña variación, por ejemplo, sustituyendo "m" por "rn".

Implemente el uso de la etiqueta "EXTERNO"

En un cambio reciente de la seguridad interna de ESET, cada correo electrónico proveniente de fuera del dominio de la empresa se etiqueta siempre como EXTERNO. Si bien esto no ayuda cuando el impostor que se hace pasar por el CEO finge enviar el correo electrónico desde su cuenta privada, es útil para identificar los correos electrónicos que intentan falsificar el dominio (como el caso de "m" y "rn").

VERIFIQUE SI ES LA PERSONA QUE DICE SER

Cuando recibe un mensaje sospechoso por WhatsApp, debe escribirle a la persona a su email devolverle la llamada. **Otra opción es preguntarle directamente a la persona, cara a cara.** No se preocupe por interrumpirlo, aunque esté ocupado. Por ejemplo, es posible que no quiera molestar a su CEO. Es algo natural, porque cuanto más elevado es el cargo del colega, más dudamos en acercarnos a él, en especial cuando está fuera de la oficina. En ese caso, considere la posibilidad de consultar a otro colega o superior. Por ejemplo, si alguien le reclama el pago de una factura grande y urgente atrasada, seguramente es (o debería ser) de conocimiento de su CFO (director financiero) o COO (director de operaciones), así que compruébelo con ellos. Recuerde: mantenerse alerta vale la pena.

"Hola, amigo. Usted no me conoce, pero yo lo conozco muy bien. Mejor de lo que cree. Esta es su contraseña, ¿verdad?"

Correos electrónicos como este pueden aparecer en el buzón de cualquiera. El misterioso extorsionador suele afirmar que ha estado grabando a la víctima con la cámara web mientras veía algún contenido para adultos y le exige que pague o, de lo contrario, se lo contará a su familia y a sus compañeros de trabajo (sextorsión). Para demostrar que realmente ha entrado a la PC, proporciona alguna contraseña que la víctima utiliza. Aún así, las estafas de (s) extorsión casi siempre son meras mentiras.

ESTAMOS EN LA EDAD DE ORO DE LAS ESTAFAS DE (S)EXTORSIÓN

La pandemia de COVID-19 es un claro ejemplo de cómo los hackers usan indebidamente la tecnología aprovechando el estado de crisis para difundir estafas. A medida que muchas empresas fueron adoptando el trabajo a distancia y las oficinas en casa, donde los empleados no estaban protegidos por la red corporativa, el número de amenazas web aumentó. Los ciberdelincuentes, por ejemplo, amenazaban con infectar a la víctima y a su familia con coronavirus si no pagaba la suma exigida.

Al pagarles a los cibercriminales, lo único que se logra es perder dinero y alimentar su negocio, ayudándolos a difundir más estafas.

COMPRENDA LO QUE QUIERE EL ATACANTE

Es importante saber que el objetivo principal de estos correos es hacer que la víctima pague, preferentemente en Bitcoins, lo que les permite a los hackers cobrar el dinero en forma anónima. Las estafas son un gran negocio: Según el Centro de Denuncias de Delitos en Internet del FBI, en 2020, la (s)extorsión por correo electrónico causó pérdidas de alrededor de 70,9 millones de dólares.

SEPA CÓMO REACCIONAR ANTE LAS ESTAFAS DE (S)EXTORSIÓN

No envíe dinero; no responda ni haga clic en ningún enlace o archivo adjunto. Si es víctima de una estafa de (s)extorsión, informe siempre a los departamentos de TI o de seguridad interna de la empresa. Y si su país lo permite, debe notificar el incidente a las autoridades pertinentes (por ejemplo, en el Reino Unido puede informarlo online en Action Fraud, y en los Estados Unidos puede presentar una denuncia en el sitio web del FBI).

La mejor prevención es crear una contraseña fuerte o una frase de contraseña. Además, el negocio de la venta de contraseñas es la razón por la que todo el mundo debe cambiar su contraseña de vez en cuando o utilizar factores de protección adicionales (autenticación en varias fases).

SI LA CONTRASEÑA ES CORRECTA, NO SE ASUSTE

Mencionar una contraseña real no es más que otra técnica para poner nerviosa a la víctima. Es posible que los atacantes conozcan su contraseña, pero probablemente sea lo único que tengan. Pueden haberla comprado en la Dark Web o haberla sacado de alguna fuga de datos.

NO SUBESTIME LOS DESAFÍOS DE SEGURIDAD DEL TRABAJO A DISTANCIA

Las oficinas y los lugares de trabajo flexibles son estupendos, pero solo si están bien protegidos y sabe cómo manejarlos. Las redes Wi-Fi son muy propensas a sufrir ataques, así que, si quiere asegurarse de que la conexión y los datos de la empresa están a salvo, es preferible que utilice una red privada virtual (VPN), que le permitirá crear una conexión segura a la red corporativa.

¿Cómo acceden los hackers a su computadora y a su cámara web?

Muchas veces utilizan malware, como un troyano, para infectar el dispositivo con software de escritorio remoto, pero para ello necesitan su ayuda. A veces, basta con que descargue algún software desconocido. Aunque parezca que consiguió lo que buscaba, puede haber algún malware escondido en el archivo. Sin saberlo, acaba de ayudar a los hackers a infectar su dispositivo. Y no espere que la luz de la cámara web se encienda en cuanto empiecen a acosarlo. De ser así, no se mantendrían en el anonimato, ¿verdad?

Si su equipo está infectado, el hacker no solo puede ver los momentos íntimos de su vida, sino que además puede capturar datos y documentos confidenciales o grabar sus conversaciones en caso de que también haya pirateado su micrófono.

Cómo reaccionar ante un mensaje de (S)extorsión

1. Actúe lenta y deliberadamente, y evite las acciones precipitadas.
Los delincuentes detrás de las estafas de (s)extorsión se aprovechan de las debilidades humanas e intentan manipularlo para que realice una acción perjudicial. Por lo tanto, si recibe un mensaje que trata de asustarlo, considere la posibilidad de que no sea cierto. Ante la duda, consulte siempre al departamento de TI o al soporte técnico del proveedor de seguridad.

2. No les pague a los extorsionadores.
Los emails de (s)extorsión suelen ser solo estafas. Esto significa que no hay ningún fundamento detrás de sus afirmaciones: lo más seguro es que no tengan nada suyo.

3. No interactúe con el email de ninguna manera.
No responda a la estafa, no descargue sus archivos adjuntos y no haga clic en los enlaces incrustados ni interactúe con ninguno de los contenidos, ya que estos elementos pueden llevarlo a un malware o a otras amenazas.

4. Revise/cambie su contraseña.
En algunos casos, los delincuentes prueban las credenciales filtradas y, si tienen éxito, utilizan la cuenta pirateada al menos para difundir sus mensajes. Por lo tanto, si un atacante le muestra algunas de sus contraseñas actuales, cámbielas inmediatamente y active un 2FA para aumentar su protección.

5. Envíe el correo electrónico a su departamento de TI.
Si su empresa no cuenta con personal de TI, lo menos que debe hacer es explorar el equipo y la red con una solución de seguridad confiable para asegurarse de que ninguna de sus contraseñas se ha filtrado o ha resultrado comprometida.

6. Proteja su cámara web.
Para evitar un posible uso indebido de la cámara web integrada, utilice un software de protección o al menos pegue un papel adhesivo sobre la cámara. De este modo, estará seguro de que los delincuentes no tienen forma de grabar un video suyo sentado delante del dispositivo.

7. Use una solución antispam.
Una solución de seguridad confiable con antispam lo ayudará a evitar que las estafas de (s)extorsión lleguen a su bandeja de entrada en el futuro.

Otras técnicas de ingeniería social que debería conocer

El **scareware** es un tipo de malware que intenta engañar a las víctimas para que compren y descarguen software potencialmente peligroso. Es un método que atrae rápidamente la atención de la gente y la asusta. Anuncios emergentes difíciles de cerrar, empresas de software con nombres de los que nunca ha oído hablar y exploraciones no autorizadas de su computadora en busca de virus: todas estas son características típicas del scareware.

El problema es que este tipo de programas suelen proceder a mostrar una lista de docenas o cientos de virus falsos. Pero en realidad los programas de scareware no están explorando su equipo y los resultados que dicen haber descubierto son falsos. Las advertencias sobre una infección solo lo están manipulando para que descargue malware. Estas estafas suelen basarse en programas de seguridad inexistentes, como Advanced Cleaner, SpyWiper o System Defender.

Utilice soluciones de software conocidos, probados y actualizados

Recuerde que una invitación para descargar software gratuito puede ser una estafa. También son muy útiles los bloqueadores de ventanas emergentes en los dispositivos laborales y los filtros de direcciones URL. Configure herramientas de seguridad web y firewalls para detener a los atacantes a tiempo.

Las **estafas de soporte técnico** están estrechamente relacionadas con el scareware. Pero, a diferencia del scareware, simulan proceder de una empresa consolidada, como Microsoft. No empezarán a explorar su equipo en forma automática. En cambio, pueden pedirle que abra algunos archivos, para luego explicarle que esos archivos muestran que hay un problema... que en realidad no existe. Según la Comisión Federal de Comercio (FTC) de los Estados Unidos, las estafas de soporte técnico no son para nada infrecuentes. En 2019, la FTC recibió más de 100.000 denuncias de este tipo de estafas.

Checklist para administradores de TI:
5 maneras de proteger su organización ante los ataques de ingeniería social

1. Capacite en forma periódica a todos los empleados en materia de seguridad IT, incluyendo a los directivos y al personal de TI. Recuerde que dicha capacitación debe mostrar o simular escenarios de la vida real. Los puntos clave del aprendizaje deben poder ponerse en práctica y, sobre todo, deben ser probados activamente fuera de la sala de capacitación.

2. Busque contraseñas débiles que podrían abrir las puertas de su red corporativa a los atacantes. Además, proteja las contraseñas con otra capa adicional de seguridad mediante la implementación de la autenticación en varias fases.

3. Implemente soluciones técnicas para ocuparse de las comunicaciones de spam, de modo que los mensajes de spam y de phishing se detecten, pongan en cuarentena, neutralicen y eliminen oportunamente. Las soluciones de seguridad (por ejemplo, muchas de las suministradas por ESET) ofrecen algunas o todas estas funcionalidades.

4. Cree políticas de seguridad fáciles de entender que los empleados puedan usar y que los ayuden a identificar los pasos que deben tomar cuando se encuentren con un ataque de ingeniería social.

5. Use una solución de seguridad y herramientas de gestión, como la consola ESET PROTECT Console, para proteger las endpoints y las redes de su organización. De esta forma, les dará a los administradores una visibilidad completa de la red así como la capacidad de detectar y mitigar las amenazas potenciales.

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad líderes en la industria para las empresas y los consumidores de todo el mundo. Con las soluciones de seguridad que van desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases, los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología a pleno. ESET brinda protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Para obtener más información, visite www.eset.com/latam.