Blinde su empresa ante amenazas cibernéticas y fraudes electrónicos

Christian David Pineda Sainz
Gabriel Guevara Gutiérrez

Las empresas enfrentan a un enemigo tecnológico cada vez mejor diseñado para extraer información confidencial. Aunque hay formas de evitarlo, los ataques se enfocan en el error humano derivado de una situación apremiante en la que el usuario cede ante la presión.

Para entender la relación que lleva del *spear phishing* al *vishing* y *smishing*, debemos comenzar por comprender el término *phishing*, acuñado en la década de 1990, y que es una variante de la palabra *fishing* o pescar en inglés. Es, entonces, un símil entre la acción de un pescador que lanza un anzuelo con cebo al agua para engañar a los peces y atraparlos, y los atacantes que envían mensajes fraudulentos por algún medio digital para engañar a una víctima y conseguir su información personal o para que realice alguna acción determinada.

Así, el *phishing* es una técnica de fraude que se centra en la utilización de historias falsas, engaños, errores humanos o técnicas de presión por medio de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para manipular a las víctimas u obtener información personal (nombres de usuario, contraseñas, números de tarjetas de crédito, entre otros datos). A medida que los medios digitales se incorporaron a la vida cotidiana de las personas, el *phishing* creció y mejoró sus técnicas de engaño y manipulación. Hoy, una de las más efectivas es el *spear phishing*.

El término *spear* es un anglicismo referido a una lanza que se dirige de forma específica y directa hacia un objetivo determinado; metafóricamente un ataque de *phishing* es: 1) mucho más preciso y mejor diseñado y 2) dirigido a un objetivo o grupo determinado. Estos factores lo hacen diferente de un ataque de *phishing* clásico que es general porque se envía a múltiples usuarios, pues se espera que alguno de ellos se identifique con el mensaje y "muerda el anzuelo". En la práctica, podemos decir que, en su mayoría un ataque de tipo *spear phishing* es un ataque dirigido a un individuo, grupo u organización que busca engañar a la víctima para que divulgue datos personales o confidenciales, descarguen algún *malware*, envíen dinero al atacante o realicen alguna acción específica. Es decir, el atacante busca manipular a la víctima al hacerse pasar por un agente conocido por él por lo que le envía información que parece real por medio de correos electrónicos, mensajes de texto, aplicaciones de *chat* o llamadas telefónicas.



Imagen de Tima Miroshnichenko en Pexels.

Para crear el mensaje malicioso el atacante lleva a cabo los siguientes pasos: 1) define el objetivo o grupo de ellos (víctima); 2) realiza una investigación profunda del objetivo a partir de obtener la mayor información posible, tanto de la víctima como de todo lo relacionado a ella, y 3) redacta el mensaje de *spear phishing* con la información recopilada y técnicas de ingeniería social. Para los puntos 1 y 2, el atacante requiere haber conseguido información personal o confidencial de la víctima. Por esta razón, todo el personal debe ser muy cuidadosos con la protección de la información confidencial de la organización y con la personal.

Existen diversos tipos de *spear phishing*, pero son dos en los que toda empresa debe poner especial atención: *Business Email Compromise* (BEC) y *whaling*:

- *BEC*. Es un ataque con impacto en el nivel de empresa, organización o negocio, es decir, el impacto o daño se dirige en el nivel corporativo, ejemplo: filtración de datos de todos los clientes, filtración de datos de nómina, etcétera.
- *Whaling*. Este término en español significa "caza de ballenas", lo que metafóricamente hace referencia a ir por "los peces más grandes" de la organización. De esta manera, el ataque se dirige a uno o más ejecutivos de alto nivel de la organización.



Imagen de Sora Shimazaki en Pexels.

El uso de estos tipos de *spear phishing* no sólo está dirigido en contra de empresas de gran tamaño, pues también la pequeña y mediana empresa es un objetivo importante en la mira de los ciberdelincuentes.

En general, el *spear phishing* es una de las formas de *phishing* más dañinas porque el atacante adapta el contexto de la información para que sea lo más convincente posible para tener mayor probabilidad de lograr engañar a la víctima.

En cuanto al *vishing* (abreviatura de *voice phishing*) o *phishing* por voz, hace referencia a una técnica de fraude que se realiza por medio de llamadas o mensajes de voz para engañar a las personas y conseguir información personal de los usuarios o que realicen alguna determinada acción. Si bien, antes de acuñar este término ya existían diversas formas de fraude telefónico que involucraban engañar a las personas para algún propósito particular, es hasta principios de la primera década del siglo XXI, con el avance de la tecnología en materia de voz, como por ejemplo la voz sobre IP (VoIP), que se expandió la capacidad de la telefonía y permitió que se llevaran a cabo ataques con mayor alcance y mucho más sofisticados, de donde deriva el término *vishing*. Un caso típico de *vishing* es el siguiente:

> Buen día [su nombre], le hablo del Banco [su banco], pues recibimos una alerta de que acaba de realizar una compra por un monto de 37 mil pesos en el sitio web Trivago. Esta transacción se hizo con su tarjeta de crédito que finaliza con 6666. Requerimos los otros 12 dígitos de su tarjeta para cancelar esta transacción.

Saben su nombre, saben su banco, saben incluso la terminación de su tarjeta; también, le ofrecen ayuda en algo importante para usted, como las finanzas personales. Inconscientemente su guardia baja, empieza a confiar y es cuando el problema surge. Este ataque tiene dos fases: 1) obtener su información y 2) realizar una llamada convincente. Algunas de las medidas que se pueden tomar para protegerse de este ataque son: destruir completamente la correspondencia que llega a su domicilio, principalmente de bancos y tiendas en línea; no compartir fotos en redes sociales, pues en ellas se comparte información sensible sobre sus hábitos y ubicaciones; desactivar la ubicación de su teléfono, sobre todo si saca fotos con él; sólo acceda a los servicios bancarios por medio de las aplicaciones oficiales, si los hace por medio de los portales web hágalo sólo en su computadora personal y asegúrese de que tenga un antivirus que detecte sitios web fraudulentos y herramientas de seguimiento de las búsquedas en internet (*keyloggers*).

El teléfono celular es una especie de trampolín por medio del que los defraudadores pueden tener acceso a información privada

El termino *smishing* es la abreviatura de *SMS phishing* o *phishing* por mensajes de texto. Utiliza los mensajes de texto vía celular o SMS (*Small Message Service*) como medio para realizar actividades fraudulentas de *phishing*.

Conforme los teléfonos celulares fueron más accesibles entre la población, la comunicación por mensajes de texto vía celular se popularizó y alcanzó fines comerciales y promocionales en la década de 1990 y la primera del siglo XXI; posteriormente, la introducción de teléfonos inteligentes fue el eslabón para conectar los mensajes de texto con los fraudes tipo *phishing* acuñando así el término de *smishing*. Un ejemplo típico es: "La entrega se intentó 2/2 veces, confirme sus datos o su artículo será devuelto: https://upsposata.xyz/mx".

Si se analiza el ejemplo, podemos identificar que hay tres elementos a destacar en este mensaje: 1) "intento" no lleva tilde; podría parecer un detalle insignificante, pero las empresas cuidan mucho que la redacción y ortografía sea correcta en los mensajes que envían; 2) la extensión de dominio "xyz" no corresponde a un dominio "com" que es el dominio reservado al sector económico; 3) el mensaje indica que es el intento 2 de 2 para entregar el paquete, dicho mensaje tiene la intención de generar estrés, aunque es poco común que un proveedor mande un mensaje SMS, pues por lo regular hacen una llamada telefónica cuando no encuentran el domicilio. Por otro lado, empresas como Amazon tienen un sistema de logística muy eficiente, por lo que son raros los casos en que el repartidor se tenga que comunicar con el cliente y si lo hace sería vía telefónica.

Importancia de que el empresario conozca el *phishing*

El tiempo promedio que las personas tardan en caer en un *phishing* es menor a 60 segundos. Según el *Data Breach Investigations Report (DBIR)* 2024 de Verizon, 2.6 millones de consumidores fueron defraudados en el año 2023, por un valor de más de 10,000 millones de dólares según informa la Comisión Federal de Comercio (FTC) de los Estados Unidos de América. El phishing fue el ataque primario, con 36% aproximado de todos los incidentes de filtración de datos, según el *Data Breach Investigations Report (DBIR)* 2023 de Verizon. Esto quiere decir que se utiliza inicialmente para convencer a los usuarios de seguir algún enlace o proporcionar información confidencial que permita al atacante realizar un ataque de mayor impacto dentro de la empresa. La cantidad de sitios de *phishing* ha aumentado 50%, aproximadamente, respecto del año anterior, según el reporte *Phishing Activity Trends Report* de APWG.

Si se considera el nivel de riesgo que representan los ataques de tipo *phishing*, exigen de una empresa consciencia, planeación y toma de acciones en materia de ciberseguridad que ayuden a prevenirlos apropiadamente alineado a los intereses y tolerancia al riesgo de la empresa.



Imagen de Mikhail Nilov en Pexels.

¿Cómo identificar un ataque?

Si bien los escenarios y medios pueden variar, existen puntos en común para identificar un ataque:

- Uso de la presión. Presionan a las víctimas para que sientan una sensación de urgencia y en consecuencia actúen rápido y sin pensar. Por ejemplo:

Somos de [su banco]. Nos comunicamos con usted, pues hemos detectado una compra inusual por la cantidad de [cifra considerable]; si usted no la reconoce, deberá confirmar su número de cliente y tarjeta para poder cancelar la transacción, si no ésta será ejecutada en [tiempo determinado].

- Solicitud de dinero o información personal. La intención final del mensaje es que se entregue dinero o información sensible.
- Faltas de ortografía, gramática o un acento extraño en el tono de voz. Las empresas cuidan su comunicación, por lo que identificar una falta en ese aspecto debería ser una alerta; asimismo, en los ataques de *vishing* las llamadas telefónicas ocasionalmente se realizan de países o regiones distintas a nuestra localidad, por lo que identificar un acento distinto podría ser una alerta.
- Contactos externos. En algunos casos, el remitente de la comunicación (correo, llamada o mensaje) no es un contacto reconocido, no está dentro de la lista de contactos o es un contacto externo a la organización.
- Uso de vínculos apócrifos. Se le pide que siga algún enlace que podría aparentar una empresa confiable, pero cambian algunas letras por unas muy parecidas. Ejemplo: *Annazon*, cambian la letra "m" por el uso de dos "n" juntas.



Imagen de energepic.com en Pexels.



Imagen de Christina Morillo en Pexels.

Medidas que puede tomar para protegerse

- Establecer campañas de concientización de seguridad. Lo que incluye, más no limita, temas de *phishing* y sus variantes; dirigidas tanto a los empleados como para las empresas que ofrecen servicios tercerizados e incluso en el nivel personal.
- Realizar simulaciones de *phishing*. Las empresas pueden establecer ejercicios de *phishing* y *spear phishing* hacia todos los niveles de la organización que permitan evaluar periódicamente la efectividad de las medidas que hayan sido implementadas; así como, el nivel de conciencia y madurez de los empleados para prevenir el *phishing*.
- Emplear herramientas de simulación. Herramientas como KnowBe4, Cofense y SANS Security Awareness ofrecen capacitación regular y simulaciones de *phishing* para entrenar a los empleados en la identificación y manejo de ataques de ingeniería social.
- Establecer políticas de seguridad apropiadas para proteger a la organización. Por ejemplo, una política de mínimos privilegios, que consiste en establecer privilegios mínimos al personal para que realice sus funciones donde se establece el tipo de acceso a internet o el envío y recepción de correo externo a la organización.
- Establecer medios de denuncia ágiles y efectivos para reportar anomalías y asegurar la integridad y confidencialidad del denunciante.

Herramientas útiles para la empresa

La selección de las herramientas dependerá de diversos factores, como el tamaño de la empresa, el tipo de negocio, el nivel de riesgo, factores regulatorios, costos de herramientas, ingresos de la empresa, etc. A continuación, se describe cinco herramientas y marcas de proveedores.

Soluciones de filtrado de correo electrónico. Ayudan a filtrar correos electrónicos sospechosos y bloquean intentos de *phishing* antes de que lleguen a la bandeja de entrada de los usuarios (Microsoft Defender for Office 365, Proofpoint, Mimecast).

Protección contra *malware* y *ransomware*. Soluciones que detectan el *malware* y *ransomware* que podría ser distribuido a través de ataques de *phishing*. Ejemplos: Symantec, Broadcom, McAfee, CrowdStrike.

Autenticación Multifactorial (MFA). Añade una capa adicional de seguridad al requerir un factor adicional de autenticación, por ejemplo enviar un código al celular para acceder a actividades críticas. Ejemplos: Google Authenticator, Microsoft Authenticator, Duo Security.

Sistemas de Prevención de Intrusiones (IPS) y Detección de Intrusiones (IDS). Ayudan a monitorizar el tráfico de red y detectar comportamientos anómalos o intrusivos que podrían indicar un ataque de *phishing*. Ejemplos: Snort, Suricata, Splunk.

Gestión de Accesos e Identidades (IAM). Permiten la gestión centralizada de identidades y accesos para garantizar que sólo usuarios autorizados puedan acceder a sistemas y datos críticos. Ejemplo: Okta, Ping Identity, OneLogin.

¿De dónde vendrán los siguientes ataques?

El uso de la Inteligencia Artificial (IA) lleva estos ataques (*phishing*, *spear phishing*, *vishing* y *smishing*) a una evolución que se caracteriza por:

- Permitir a los delincuentes automatizar y personalizar con mayor precisión las campañas de *spear phishing* y *smishing* que imitan con gran exactitud el estilo y tono de una comunicación legítima, lo que complica así su identificación.
- Analizar grandes volúmenes de datos personales para dirigir ataques de spear *phishing* extremadamente específicos y convincentes.
- Utilizar el *vishing* para realizar llamadas automatizadas con un alto grado de realismo, incluso al generar una voz con el mismo tono de alguien conocido y al manipular a las víctimas con técnicas de ingeniería social y respuestas predefinidas basadas en patrones de conversación.
- Combinar *vishing* y *smishing* para generar mensajes de audio con la voz de algún conocido de la víctima para pedir dinero por una supuesta situación de emergencia.

Esta integración de IA en el cibercrimen no sólo aumenta la efectividad de los ataques, sino que también plantea desafíos mayores para las estrategias de defensa y detección, por lo que subraya la necesidad de soluciones de seguridad que combinen tecnología avanzada con formación continua para mitigar los riesgos y estar a la altura de este nuevo desafío.

Referencias

Anti-Phishing Working Group, Inc. (2024, junio 1). Phishing Activity Trends Report. APWG; Anti-Phishing Working Group, Inc. https://apwg.org/trendsreports/

Comisión Federal de Comercio de los Estados Unidos de América (2024, febrero 9). Con pérdidas por fraude en todo el país que en 2023 superaron los $10,000 millones de dólares, la FTC intensifica sus esfuerzos para proteger al público. Comisión Federal de Comercio de EUA. <https://n9.cl/lk5f2>

Verizon (2024, enero). 2024 *Data Breach Investigations Report*. Verizon DBIR; *Verizon Business*. <https://n9.cl/00o6lr>

Mtro. Christian David Pineda Sainz
Licenciatura en Informática
Facultad de Contaduría y Administración, UNAM
profesorpineda22@gmail.com

Mtro. Gabriel Guevara Gutiérrez
Jefe de la Licenciatura en Informática
Facultad de Contaduría y Administración, UNAM
gguevara@fca.unam.mx