INGENIERÍA SOCIAL MODERNA

**Ciberataques más comunes de ingeniería social para estar prevenidos y cuidados**

*¿Alguna vez recibió un correo electrónico sospechoso o una llamada telefónica de un número desconocido solicitando información? ¿O hizo clic en ese enlace que prometía ofertas de descuento pero terminó ingresando información confidencial? Lo más probable es que haya sido víctima de un ataque de ingeniería social.*

**Por Julián M. Zappia.  
Diplomatic Week.**

La ingeniería social es una técnica de manipulación utilizada por los atacantes para extraer información o acceder a las personas.

El Informe de investigaciones de violación de datos de la empresa Verizon de 2022 encontró que la ingeniería social fue un factor importante que abarcó el 32% de todas las violaciones de datos.

El índice de inteligencia de amenazas X-Force de IBM del año pasado, descubrió que el “phishing” era el tipo de ataque más común y representaba más de un tercio de todos los ataques.

**¿Qué son los ataques de ingeniería social?**

Los ataques de ingeniería social son manipulaciones o tácticas engañosas que se utilizan para obtener el control de los sistemas informáticos, los datos o la información confidencial.

Los ataques de ingeniería social han evolucionado drásticamente. Los nuevos métodos, como las falsificaciones profundas, son una preocupación creciente para las personas y las empresas.

Los ciberdelincuentes conocen sus objetivos y la ingeniería social se utiliza para aprovechar las debilidades humanas. Los errores de ciberseguridad como este pueden costar a las empresas enormes sumas de dinero.

A modo de referencia, el costo promedio de una violación de datos de una empresa al día de hoy rondaría los 4,2 millones de dólares.

Protegerse frente a la ingeniería social se ha convertido en un tema apremiante, y defenderse de estos ataques es fundamental para evitar ser víctima.

Los atacantes cibernéticos desarrollan constantemente nuevos métodos para explotar las tendencias tecnológicas, lo que da como resultado técnicas eficientes de ingeniería social.

**¿Cómo funcionan?**

Los ataques de ingeniería social pueden ocurrir en varias formas. Una vez que un ciberdelincuente obtiene acceso a sus sistemas de seguridad o información privada, el daño puede ser costoso.

Los ataques de ingeniería social representan una amenaza para varias plataformas, incluidos los sistemas iOS (Apple), Android y computadoras personales.

**Las cuatro fases principales en la ingeniería social.**

* Descubrimiento e investigación: el atacante busca información sobre su objetivo a través de plataformas de redes sociales, foros de la web oscura (o “dark web”) u otras fuentes públicas de información.
* Engaño y atracción: una vez que el atacante ha recopilado suficiente información, intentará establecer confianza con su objetivo mediante el engaño. Lo hacen a través de correos electrónicos de “phishing” o contactando al objetivo utilizando técnicas de suplantación de identidad.
* Ataque: si el atacante tiene éxito, intentará obtener acceso a su sistema o información. Lo hacen a través de software malicioso, adivinación de contraseñas y otros métodos.
* Retirada: después de que el atacante haya accedido con éxito al sistema o la información de destino, comenzará a cubrir sus huellas eliminando cualquier evidencia de su ataque.

El tiempo promedio para detectar un ataque cibernético o una violación de datos es de aproximadamente 250 días, por lo que la víctima ni siquiera sabrá lo que sucedió hasta que se hayan retirado los ciberdelincuentes.

**Tipos de ataques de ingeniería social.**

Ahora que conocemos las generalidades de los ataques de ingeniería social y lo costosos en lo personal y económico que pueden resultar, veremos los diez tipos más comunes de ataques de ingeniería social.

**Suplantación de identidad (“Phishing”).**

Los ataques de phishing son el tipo más común de ataques de ingeniería social. Implican el envío de correos electrónicos fraudulentos a un número de personas que hacen parecer que el correo electrónico proviene de una fuente legítima, como un banco o una agencia gubernamental.

El correo electrónico generalmente contendrá un enlace que conduce a un sitio web malicioso diseñado para robar información personal.

Un caso no tan reciente pero sí de gravedad fue, en 2017, un ataque de pretexto dirigido a los usuarios de Netflix. Los atacantes enviaron correos electrónicos que parecían ser de Netflix, pidiendo a los destinatarios que actualizaran su información de pago.

Si lo hicieran, serían redirigidos a un sitio web falso que robaría sus credenciales de inicio de sesión y el número de su tarjeta de crédito.

Los ataques de phishing selectivo son como ataques de phishing, pero están dirigidos a personas u organizaciones específicas. El atacante personalizará el correo electrónico con información sobre su objetivo, lo que dificultará que detecte el fraude.

Una nueva versión del phishing selectivo se conoce como phishing de pescador. Esto ocurre cuando los estafadores se hacen pasar por cuentas de servicio al cliente en las redes sociales. Su objetivo es obtener acceso a su información de inicio de sesión con promesas de ayuda.

**Smishing y vishing.**

Smishing es un tipo de ataque de phishing en donde los ciberdelincuentes utilizan mensajes de texto al celular, o WhatsApp. El atacante enviará un mensaje que parece ser de una organización legítima, pidiéndole que haga clic en un enlace o que llame a un número de teléfono.

Vishing es como el smishing, pero el atacante usará llamadas de voz en lugar de mensajes de texto. Pueden falsificar el identificador de llamadas para que parezca que están llamando de una fuente legítima o incluso de un amigo.

Como referencia reciente, en 2019, hubo una campaña masiva de vishing dirigida a clientes de los principales bancos de EE. UU. Los atacantes llamaban a las víctimas y pretendían ser del departamento de fraudes del banco. Luego intentarían que la víctima les diera su información de inicio de sesión o número de tarjeta de crédito.

**Piggybacking / Tailgating.**

Piggybacking se refiere a un ataque en el que el atacante obtiene acceso a un área segura siguiendo a alguien que tiene acceso legítimo. Tailgating es similar a piggybacking, pero el atacante intentará obtener acceso pidiéndole a alguien su identificación. Ambas, son poco comunes por la escasa efectividad que logran los atacantes.

**Ataques de “cebo”.**

En los ataques de cebo utilizan medios físicos. Esto incluye unidades USB o DVD -entre otros medios- a efectos de atraer a las víctimas para que infecten sus propias computadoras. El atacante dejará el medio infectado en un lugar público y esperará a que alguien lo tome y lo conecte a su computadora.

En 2017, hubo un ataque de hostigamiento dirigido al personal del Servicio Nacional de Salud (NHS) del Reino Unido. El atacante dejó memorias USB en hospitales y clínicas que parecían contener información sobre la atención de los pacientes. Cuando eran conectados por los usuarios, los dispositivos en realidad instalarían malware que podría dar acceso al atacante a datos confidenciales del paciente.

**Compromiso de correo electrónico comercial (BEC).**

El compromiso de correo electrónico comercial (BEC, por sus siglas en inglés) es un tipo de ataque de ingeniería social en el que el atacante obtiene acceso a una cuenta de correo electrónico comercial y la utiliza para enviar correos electrónicos fraudulentos.

El tipo más común de ataque BEC se conoce como fraude de facturas. Esto es cuando el atacante envía un correo electrónico que parece ser de un proveedor conocido y le pide al destinatario que pague una factura. El pago irá a la cuenta del atacante en lugar del proveedor legítimo.

**Ataques Quid Pro Quo.**

En los ataques quid pro quo, el atacante ofrece algo a la víctima a cambio de información personal o acceso a un sistema; casi como una exorsión.

Por ejemplo, un atacante puede llamar a alguien que pretende ser un profesional de informática, y se ofrecen a ayudar a solucionar los problemas de su computadora si proporcionan sus credenciales de inicio de sesión.

**Trampas de miel (“Honey Trap”).**

El término "trampa de miel" se refiere a un ataque de ingeniería social, en el que se utiliza una persona atractiva para atraer a los objetivos.

La trampa de miel implica el uso de un individuo atractivo para seducir y manipular a un objetivo para que revele información confidencial o comprometa su posición (puede llegar a lo que se conoce como “sextorsión”). El atacante utiliza a una persona atractiva para atraer a la víctima para que revele información personal o cometa un delito.

También es una táctica de espionaje común que ha sido utilizada por varias agencias de inteligencia de todo el mundo.

Este tipo de ataque, ayuda a extraer información confidencial de personas en posiciones de poder. Ha habido algunos casos de alto perfil de supuestas “capturas de miel” que involucran a personas asociadas, incluso con el ejército.

**Espantapájaros (“Scareware”).**

El “scareware” es un tipo de ataque de ingeniería social en el que el atacante usa el miedo para engañar a la víctima para que realice una acción. Esto incluye hacer clic en un enlace, descargar malware o realizar una compra en línea.

Por ejemplo, como atacante, puede enviar un correo electrónico que parece ser de una empresa legítima como Microsoft, o un banco conocido, entre tantas opciones. Luego advertirá al destinatario que su computadora ha sido infectada con un virus. Luego, el correo electrónico les diría que hicieran clic en un enlace para descargar un "software antivirus", que eventualmente sería malware.

En 2021, hubo un ataque de “scareware” dirigido a usuarios de Android. Los atacantes crearon aplicaciones antivirus falsas y las anunciaron en línea. Cuando las víctimas instalaban las aplicaciones, mostraban advertencias de virus falsas y pedían al usuario que comprara la "versión completa" de la aplicación para eliminar el malware.

**Cómo protegerse de la ingeniería social.**

La mejor manera de protegerse de los ataques de ingeniería social es estar al tanto de ellos para que sean posibles de reconocer cuándo nos está ocurriendo.

Los ciberdelincuentes idean nuevas formas de atacar objetivos y es importante mantenerse actualizado sobre las últimas amenazas.

**Consejos de verificación rápida.**

* Revise cuidadosamente los correos electrónicos, incluidos los nombres, las direcciones y las copias. Esté atento a las características inusuales o desconocidas que no se observen bien.
* Tenga cuidado con los archivos adjuntos inesperados.
* Reconozca las líneas de asunto comunes de los correos electrónicos de phishing ("se requiere una acción urgente", "la cuenta ha sido comprometida", etc.).
* Verifique la identidad de cualquier persona que no conozca personalmente.
* Tenga mucho cuidado con las redes sociales.
* Nunca pague un rescate y denuncie el ransomware a las autoridades pertinentes.
* Utilice siempre autenticación de dos o múltiples factores (2FA/MFA, conocida como “autenticación de dos pasos”).
* Utilice todo mecanismo de control parental que esté a su alcance para con los menores.

**Cómo proteger su empresa de la ingeniería social.**

Así es como podemos proteger a las empresas de los ataques de ingeniería social:

* Educar y capacitar a los empleados sobre los ataques de ingeniería social.
* Crear y aplicar políticas de seguridad sólidas.
* Instalar protecciones técnicas como antivirus y firewalls.
* Realizar un seguimiento de actividad y registros de auditoría.
* Implementar políticas de contraseñas seguras y autenticación multifactor (MFA).
* Restringir el acceso a la información sensible utilizando el Principio de Mínimo Privilegio (no conceder acceso total a archivos o carpetas de importancia).
* Realizar un seguimiento de la actividad de los empleados con una solución SIEM (aplicaciones para generación y lectura de archivos de actividades de los sistemas, con la correspondiente preservación de datos personales, llamados “logs”.).

**Conclusión.**

A medida que los ataques de ingeniería social se vuelven más avanzados, es esencial estar al tanto de cómo los piratas informáticos intentan manipularlo a usted, a su negocio y a su familia.

La mayoría de los ataques de ingeniería social se pueden reconocer, controlar y mitigar.

Es crucial que tomemos en serio los ataques de ingeniería social. Al emplear las estrategias defensivas adecuadas, podemos protegernos contra todas sus formas.

Un buen antivirus y cortafuegos pueden ayudar, pero es más importante mantenerse actualizado, alerta, no publicar información personal en redes sociales, no publicar fotos que puedan permitir identificar dónde se encuentra (interiores de la casa, exteriores, viajes, vacaciones), no publique fotos familiares (mucho menos de niños), no mostrar datos personales o de empresa sensibles, entre otras acciones.

No se olvide que su vida pública y privada puede transformarse en globalmente pública con las tecnologías de hoy en día.