Actividad 05. Ataques de ingeniería social

La ingeniería social es un tipo de manipulación que **se basa en engañar al usuario a través de diferentes actividades maliciosas para proporcionar en secreto información privada** (como contraseñas e información de cuentas bancarias), **o para acceder a su dispositivo e instalar malware** (software malicioso).

Estos ataques suelen producirse en línea, en persona y a través de otras interacciones.

Las estafas basadas en la ingeniería social se construyen en torno a la forma de pensar y comportarse de las personas.

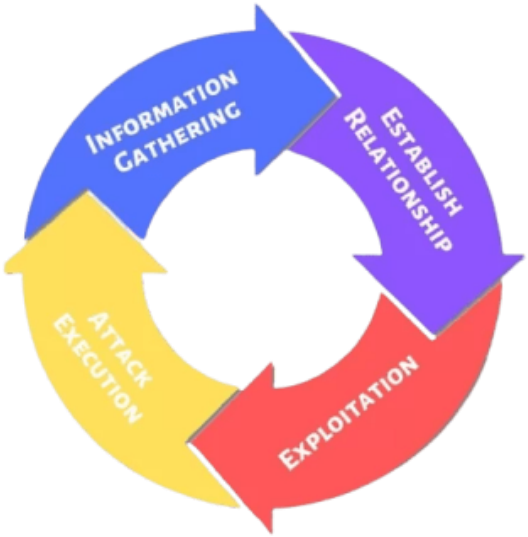
Por lo tanto, **los ataques de ingeniería social son útiles para manipular el comportamiento del usuario**. Una vez que el atacante conoce la motivación del comportamiento del usuario, puede engañarlo y manipularlo eficazmente.

Por ejemplo, es mucho más fácil engañar a alguien para que dé sus contraseñas que intentar hackear su contraseña (a menos que la contraseña sea realmente débil).

¿Cuáles son los pasos de un ataque de ingeniería social?

Los ataques de ingeniería social suelen producirse en uno o varios pasos. Un atacante sigue, en la mayoría de los casos, los siguientes pasos:

1. **Preparar el terreno para el ataque**
   - Identificar a la víctima (o a las víctimas)
   - obtener información de fondo
   - Decidir qué método(s) de ataque utilizar
2. **Engañar a la víctima**
   - Atacar el objetivo
   - Inventar una historia
   - Tomar el control de la interacción
3. **Obtener acceso a la información durante un período de tiempo**
   - Ampliar la posición
   - Realizar el ataque
   - Destruir el negocio o/y desviar los datos
4. **Cerrar la interacción sin despertar sospechas**
   - Eliminar cualquier rastro de malware
   - Cubrir las huellas
   - Terminar el ataque de forma natural



Este proceso puede realizarse en un solo correo electrónico o a lo largo de meses tras varias charlas en las redes sociales. O, como hemos dicho, incluso podría ocurrir en la interacción cara a cara. Finalmente, concluye con una acción que realiza la propia víctima, como entregar su información personal o exponerse a un malware.

¿Cómo reconocer los ataques de ingeniería social?

1. Correo electrónico de un *amigo*

Si los delincuentes consiguen descifrar o aplicar ingeniería social a la contraseña del correo electrónico de una persona, pueden acceder a la lista de contactos de esa persona, y como la mayoría de la gente utiliza una contraseña en todas partes, también pueden tener acceso a los contactos de las redes sociales de esa persona.

Una vez que el actor de la amenaza toma el control de la cuenta de correo electrónico, enviará correos electrónicos a todos los contactos de la persona o dejará un mensaje en todas las páginas de las redes sociales de sus amigos, o también puede dejar un mensaje en la página de los amigos de la persona.

Para aprovechar su confianza y curiosidad, estos mensajes contendrán en su mayoría lo siguiente:

- **Contienen un enlace**: que sólo tiene que comprobar porque el enlace viene de un amigo y usted está interesado en él. Al final, al hacer clic en el enlace, se infectará con un malware para que el delincuente pueda controlar su dispositivo y recopilar la información de sus contactos para engañar a otros
- **Contienen un archivo adjunto para descargar**: pueden ser imágenes, películas, música, un documento, etc. Pero estos archivos adjuntos incluyen un software malicioso. Ahora, el hacker ha accedido a su dispositivo. cuentas de redes sociales y contactos, cuenta de correo electrónico, y el ataque se extiende a todos los que usted conoce sin parar.

¿Cómo reconocer los ataques de ingeniería social?

2.Correo electrónico de otra persona de confianza

Los ataques de phishing forman parte de una estrategia de ingeniería social que imita a una persona de confianza y presenta un escenario aparentemente lógico para entregar las credenciales de acceso u otros datos personales sensibles. Según la investigación anual de Verizon sobre brechas de datos, los ataques de ingeniería social son responsables del 93% de las brechas de datos que tienen éxito.

Posibles escenarios y mensajes que puede recibir:

- ***Pidiendo urgentemente su ayuda***: a su «amigo» le han robado, ha tenido un accidente o está en el hospital y necesita que le envíe dinero inmediatamente. Además, le indican cómo enviar el dinero al estafador.
- ***Intentos de phishing con una apariencia legítima:*** básicamente, un phisher envía un correo electrónico, un mensaje instantáneo, un comentario o un mensaje de texto que parece proceder de un banco, una escuela, una empresa popular o una institución legítimos.
- ***Pedir un donativo para una recaudación de fondos benéficos***: lo más probable es que recibas instrucciones sobre cómo enviar el dinero al delincuente. Confiando en su amabilidad y generosidad, estos hackers piden ayuda o apoyo para cualquier desastre, campaña política o de caridad.
- ***Presentar un problema que le pide que «verifique» sus datos pulsando un enlace específico***: la ubicación del enlace parece muy legítima, con todos los logotipos y contenidos correctos (tal vez incluso copiados con el formato exacto de la página original). Ante ello, el usuario confía en el correo electrónico y en la falsa página web y proporciona cualquier información que el hacker le pida. Además, este tipo de estafas de phishing incluyen una advertencia de lo que ocurrirá si no se actúa pronto (manipulando al usuario para «actuar antes de pensar»).

Tipos de ataques de ingeniería social

1. Ataques de phishing

- Los atacantes de phishing se presentan como una empresa o individuo legítimo y de confianza que intenta persuadirle para que comparta sus datos personales y otros elementos de valor.
- Puede ocurrir de una o dos maneras, respectivamente, el **spam phishing** (ataque generalizado dirigido a muchos usuarios) y el **spear-phishing** (por extensión whaling, que utiliza información personalizada para dirigirse a usuarios específicos, como celebridades, altos directivos y altos funcionarios del gobierno).

2. Ataques con cebo

- El cebo abusa de su curiosidad natural para persuadirle de que se exponga a un atacante. La manipulación que se utiliza para explotarte suele ser la posibilidad de obtener algo exclusivo o gratuito. Este tipo de abuso implica normalmente infectar su dispositivo con malware.
- Los métodos de cebo más populares son: Unidades USB dejadas en espacios públicos y archivos adjuntos de correo electrónico que incluyen detalles sobre una oferta gratuita, o software gratuito fraudulento.

3. Ataques basados en la brecha física

- Este tipo de ataque consiste en que los hackers se presenten en persona, haciéndose pasar por alguien legítimo para acceder a áreas o datos restringidos.
- Estos ataques son más comunes en entornos empresariales, como negocios, gobiernos u otras organizaciones. Por lo tanto, los atacantes se presentan como representantes de una empresa de confianza. De hecho, algunos de los atacantes podrían ser incluso empleados recientemente despedidos que quieren vengarse.
- Logran que su identidad sea desconocida pero lo suficientemente creíble como para evitar más preguntas. Esto requiere un poco de investigación para el atacante y también implica un alto riesgo.

4. **Ataques de pretexto**

El pretexto utiliza identidades engañosas como «excusa» para generar confianza, por ejemplo, suplantando directamente a un proveedor o empleado de una instalación. Este método requiere que el atacante interactúe con la víctima de forma más activa. Una vez que la convencen de que son legítimos, seguirán explotándola.

5. Ataques de tipo «acceso a la cola»

Tailgating (o **piggybacking**) es el acto «colarse», de seguir a un empleado autorizado en un área de acceso restringido.

Básicamente, los atacantes intentan convencerle de que ellos también están autorizados a estar en la zona. De hecho, el pretexto también puede desempeñar un papel en este caso.

6. **Ataques quid pro quo**

- Esto significa literalmente «**un favor por un favor**», que en el contexto del phishing significa un intercambio de su información personal por alguna recompensa o compensación. Lo más habitual sería que los regalos o las ofertas para participar en estudios de investigación le expongan a este tipo de ataques.
- La explotación proviene del entusiasmo por conseguir algo valioso con una baja inversión. Sin embargo, al final, el atacante se limita a recopilar los datos sin recompensa alguna para usted.

7. **Ataques de falsificación de DNS y contaminación de la caché**

- La falsificación de **DNS** manipula su navegador y los servidores web para redirigirle a sitios web maliciosos cuando introduce una **URL** legítima. Una vez infectado, el redireccionamiento continuará a menos que se borren los datos de la ruta errónea en los sistemas implicados.
- Por otro lado, los ataques de contaminación de la caché de **DNS** infectan particularmente su dispositivo con instrucciones de rutas para la **URL** legítima o múltiples **URLs** para conectarse a sitios web sospechosos.

8. **Ataques de tipo «scareware».**

- El **scareware** es un tipo de malware que se utiliza para asustar al usuario para que realice una acción. Este malware engañoso utiliza avisos alarmantes que informan de falsas infecciones de malware o afirman que una de sus cuentas ha sido comprometida.
- Como efecto, el scareware le presiona para que compre software de ciberseguridad fraudulento, o revele información privada como las credenciales de su cuenta.

9. **Ataques de tipo «watering hole» (pozo de agua)**

- Estos ataques infectan páginas web conocidas con malware que puede afectar a muchos usuarios a la vez. Requiere una cuidadosa planificación por parte del atacante para encontrar vulnerabilidades en sitios específicos. Buscan debilidades existentes que no son conocidas ni parcheadas (estas vulnerabilidades se consideran exploits de día cero)
- Por lo tanto, pueden descubrir que un sitio web no ha actualizado su infraestructura para parchear los problemas conocidos. Los propietarios de sitios web suelen optar por retrasar las actualizaciones de software para mantener las versiones que saben que son estables. Pasarán a la nueva versión una vez que se haya demostrado la estabilidad del sistema.
- Por lo tanto, los hackers abusan de este comportamiento para dirigirse a las debilidades recientemente parcheadas.

10. **Métodos inusuales de ingeniería social**

- ***Phishing por fax***: cuando un cliente de un banco recibe un falso correo electrónico que dice ser del banco, pidiéndole que confirme su código de acceso, el método de confirmación no era por la vía habitual del correo electrónico o de Internet. En cambio, se pedía a los clientes que imprimieran el formulario del correo electrónico, rellenaran sus datos y enviaran el formulario por fax al número de teléfono del atacante.
- ***Distribución de malware por correo tradicional***: en Japón, los ciberatacantes utilizaron un servicio de entrega a domicilio para compartir CDs infectados con un troyano espía. Los discos se entregaron a los clientes de un

banco japonés. Por ello, las direcciones de los clientes habían sido robadas previamente de la base de datos del banco.

Reflexiones finales

La prevención de los ataques de ingeniería social comienza con la formación. Si todos los usuarios son conscientes de estas amenazas, nuestra seguridad como sociedad colectiva mejorará. Por lo tanto, asegúrese de concienciar sobre estos riesgos compartiendo lo que ha aprendido con sus empleados, compañeros, amigos y familiares.

En los siguientes artículos se habla sobre Ingeniería social:

- ¿Qué es la ingeniería social?
- Tipos de ataques de ingeniería social y cómo evitarlos
- ¿Qué es la ingeniería social?

En los siguientes vídeos se habla sobre Ingeniería social y se ven algunos ejemplos:

- ¿Sabes qué es INGENIERÍA SOCIAL?
- Qué es la ingeniería social
- Ingenieria Social (Parte 1): Componentes Psicológicos
- Ingeniería Social (Parte 2): Técnicas
- Ingeniería social Mr Robot
- Datos e información y aplicación de ingenieria social-ATRAPAME SI PUEDES
- Ingeniería Social por teléfono
- Ingeniería social parte 1
- Ingeniería social parte 2
- Ejemplo de fraude telefónico (Ingeniería Social)
- Demostracion de un ciberataque - © Deloitte Company

Se pide:

1. Describe con tus propias palabras qué es la ingeniería social, los tipos y técnicas existentes
2. Busca ejemplos de ingeniería social
3. Explica, con tus propias palabras, que medidas has de realizar en una organización para evitar los ataques de ingeniería social