Ingeniería social

Conozca formas de reconocer y evitar técnicas de manipulación de ingeniería social.

1. ¿Cómo funcionan los ataques de ingeniería social?

La ingeniería social hace referencia a los métodos y las técnicas que usan los estafadores con el objetivo de engañarlo para que haga algo cuestionable, como revelar su información personal o enviar dinero. La ingeniería social ha existido durante siglos y se acaba de adaptar a la era de la Internet.

El objetivo principal de la ingeniería social es manipular a las personas. Así funciona un ataque de ingeniería social:

- El atacante identifica a una víctima y revela información sobre esta.
- Luego, decide qué tipo de técnica de ingeniería social utilizará.
- El atacante involucra a la víctima y usa diferentes técnicas para manipularla.
- El atacante convence a la víctima para que le dé información o dinero.
- El atacante concluye la farsa y desaparece.

2. ¿Cuáles son algunas técnicas comunes de ingeniería social?

En los ataques de ingeniaría social, se intenta manipular a las personas. Estas son algunas tácticas y técnicas habituales:

- **Señuelo:** estos ataques intentan atraer a las víctimas con promesas o cosas falsas, como descargas gratuitas, servicios gratuitos o premios.
- **Scareware:** suele adoptar la forma de anuncios emergentes con mensajes alarmantes que intentan asustarlo para que revele su información o sus datos.
- **Fraudes de suplantación de identidad:** estas formas muy comunes de ingeniería social manipulan sus emociones por mensaje de texto o correo electrónico, e

intentan convencerlo de hacer clic sobre algo o hacer una descarga, o de enviar información o dinero. Los fraudes de suplantación de identidad suelen utilizar la emergencia como detonador, pero también pueden intentar asustarlo, jugar con su simpatía o persuadirlo con un premio.

- **Pretexto:** con esta técnica, el atacante puede hacerse pasar por alguien en quien usted confía o una figura de autoridad para ganar su confianza y lograr que revele su información.
- **Suplantación de identidad de objetivo definido:** este tipo de fraude de suplantación de identidad está dirigido a una persona o a un grupo pequeño de personas, y suele parecer que proviene de alguien que conocen.

Tenga en cuenta que la ingeniería social puede ocurrir fuera de línea a través de llamadas telefónicas fraudulentas o en persona. Por ejemplo, los delincuentes pueden hurgar en la basura para obtener su información personal de la basura, o intentar acceder a un edificio para robar datos o tecnología.

3. ¿Cuáles son las señales de la ingeniería social?

Esté atento a lo siguiente:

- La solicitud o el mensaje son inesperados.
- La solicitud es muy urgente.
- Siente que lo están presionando para que haga algo rápido.
- La oferta parece demasiado buena para ser real.
- Nota errores gramaticales o de ortografía extraños.
- El mensaje parece aterrador y amenazante.

Recuerde que los ingenieros sociales intentan manipularlo y lograr que actúe sin detenerse, reflexionar ni pensar de forma crítica. No ceda ante la presión.

4. ¿Cómo puede evitar la ingeniería social?

- Esté atento a las técnicas que usan estos estafadores.
- Investigue la solicitud y no responda de inmediato ni se involucre directamente.
- Considere su propia respuesta emocional: ¿se siente presionado o amenazado?
- Ponga en práctica la minimización de datos, y sea consciente de lo que publica en la Internet y pone a disposición de otros.
- Emplee contraseñas seguras usando la autenticación multifactor y un administrador de contraseñas.
- No abra archivos adjuntos ni haga clic en enlaces de fuentes desconocidas.
- Gestione la configuración de seguridad de sus cuentas y limpie sus perfiles de redes sociales para asegurarse de que no haya información privada o confidencial expuesta.
- Mantenga actualizados sus dispositivos e instale las últimas actualizaciones de seguridad.
- Destruya los documentos confidenciales.
- Mantenga una copia de seguridad de sus datos en caso de que sufra un hackeo o un ataque de ransomware.

5. Haga un plan

Considere las medidas que puede tomar para asegurar mejor sus cuentas y su información, y evitar caer en un fraude de ingeniería social. Use este espacio para reflexionar: