**INGENIERIA SOCIAL**

Es un conjunto de técnicas estratégicas para engañar a la gente de manera psicológica para obtener información valiosa. Cualquier acto que incluye sobre una persona para tomar una acción que puede ser o no de interés. Se puede influir de manera psicológica, fisiológica y tecnológica sobre una persona. Los mismos principios que son utilizados de forma positiva se pueden usar de forma malintencionada.

**Importancia de la ingeniería social en la ciberseguridad**

La importancia de la ingeniería social en ciberseguridad radica en varios aspectos clave:

* **Ataques altamente efectivos:** los ataques de ingeniería social, bien ejecutados, tienen tasas de éxito significativamente altas.
* **Amenazas internas:** la mayoría de los incidentes de seguridad provienen de amenazas internas.
* **Adaptabilidad:** los ciberdelincuentes se adaptan constantemente y perfeccionan sus técnicas de ingeniería social.
* **Protección de la marca y la reputación:** los atacantes de ingeniería social pueden socavar la confianza del público en una organización.

**¿Qué tan grave es?**

90% de las personas a las que se les pregunta su nombre no solo deletrean su nombre sino también su dirección de correo electrónico sin confirmar la identidad de quien pregunta.

67% de personas que les pregunta dan su número de seguro social, fecha de nacimiento o número de empleado.

La pandemia ha tenido un impacto significativo en la forma en que las personas trabajan, se comunican y utilizan la tecnología, y los ciberdelincuentes han aprovechado esta situación para perfeccionar sus técnicas de ingeniería social.

Tendencias y cambios en el panorama de la Ingeniería Social después del COVID-19:

* Aprovechamiento de la incertidumbre
* Salud y bienestar en línea
* Ciberseguridad consciente
* Estafas y donaciones de caridad
* Mayor satisfacción

Se refiere a la incertidumbre de las personas para obtener la información o accesos que comprometan la seguridad de un individuo o de una organización.

**Basada en persona:** cuando la interaccione s directa entre el atacante y la victima ya sea una conversación cara a cara o via telefónica. Ejemplos: prueba del sistema, tailgating o también piggybacking, shoulder surfing.

**Basada en computadora:** se hace uso de estafas electronicas para engañar a las personas y lograr el objetivo del atacante. Ejemplos: phishing, keyloggers, screenloggers, spyware.

**4 ciclos de ataque de la ingeniería social**

**Investigación**

Recopila la máxima información posible de su víctima.

**Infiltración**

Utiliza la información conseguida para ganarse su confianza.

**Explotación**

Crear una fuerte relación y continuar el dialogo para explotar esa relación y obtener la información deseada sin que la víctima sospeche, confianza.

**Desconexión**

Salir de la escena del ataque o detener la comunicación crear sospechas.

**La ingeniería social activa**

Técnica sofisticada que los atacantes utilizan para manipular a las personas y obtener acceso no autorizado a sistemas, información confidencial o recursos.

**Phishing sofisticado:** los atacantes utilizan correos electrónicos, mensajes de texto o llamadas telefónicas para crear una sensación de urgencia o medio en la victimas.

**Engaño por voz (vishing):** los atacantes utilizan la voz y la comunicación telefónica para persuadir a las victimas.

**Ataques en persona:** los atacantes pueden infiltrarse en las instalaciones físicas de una organización haciéndose pasar por personal autorizado o contratistas.

**Redes sociales y perfiles falsos:** los atacantes pueden crear perfiles falsos en redes sociales para establecer relaciones de confianza con las victimas.

**Suplantación de identidad y pretextos convincentes:**

**La ingeniería social pasiva**