Ingeniería social

Es la técnica de manipulación que aprovecha los errores humanos para obtener información privada, accesos u objetos de valor. Estas estafas de “hackeo de humanos” tienden a hacer que los usuarios desprevenidos expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, persona y a través de otras interacciones.

Rasgos de este ataque

- **Intensificación de las emociones:** La manipulación emocional les da a los atacantes la ventaja en cualquier interacción. Las emociones se utilizan en igual medida para convencerlo.
- **Urgencia:** Las oportunidades o solicitudes urgentes son otra herramienta confiable en el arsenal de un atacante, es posible que se siente motivado a comprometerse ante aparentes problemas graves que necesitan atención inmediata.
- **Confianza:** La credibilidad es invaluable y esencial para un ataque de este tipo. En este punto el atacante puede crear un perfil para que la víctima caiga fácilmente.

Tipos de ataques de ingeniería social

- Ataques de phishing (Uso de otra identidad)
- Ataques de cebo (Uso de Intensificación de las emociones)
- Ataques de acceso (Uso de la confianza)
- Ataques que usan pretextos (Uso de la confianza)
- Ataques de “acceso a cuestas” (Uso de la confianza)
- Ataques de reciprocidad (Uso de Intensificación de las emociones)

Emociones que pueden usar

- Miedo
- Entusiasmo
- Curiosidad
- Ira
- Culpa
- Tristeza