INGENIERÍA SOCIAL

ATAQUES DE INGENIERÍA SOCIAL

Los ataques de ingeniería social se basan en la manipulación de las emociones y la psicología humana. Los atacantes engañan a las víctimas haciéndolas creer que estan interactuando con una entidad legítima.

ENGAÑO Y SUPLANTACIÓN DE IDENTIDAD

Los atacantes pueden hacerse pasar por una persona o entidad de confianza, para obtener información o acceso. Esto puede involucrar el uso de correos electrónicos, llamadas telefónicas o perfiles de redes falsos.

RECOPILACIÓN DE INFORMACIÓN CONFIDENCIAL

El objetivo principal de los ataques de ingeniería social es obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales.

COMO IDENTIFICAR UN ATAQUE DE INGENIERIA SOCIAL

Normalmente solicitan se haga un tipo de accion de forma inmediata, con una amenaza de por medio. Se reciben llamadas, correos o mensajes solicitando ingresar claves o usuarios de acceso.

FORMAS DE ATAQUE VARIADAS

Duplican las cuentas de nuestras familias o amigos y utilizan la extorsión. Dejan abandonados dispositivos USB infectados con malaware para al usarlos, comprometer esa computadora.

En resumen, los ataques de ingeniería social son tacticas de manipulación psicológica utilizadas por los ciberdelincuentes para obtener información confidencial o acceso no autorizado a sistemas y datos. La conciencia y la educación sobre estos ataques son esenciales para prevenirlos y protegerse contra ellos.

CIBERSEGURIDAD
PERSONAL Y FAMILIAR
BRILART