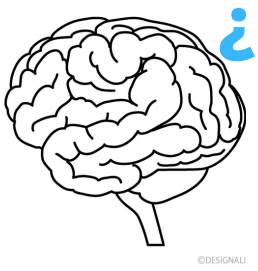
Peter.
Business

Ingeniería social

Técnicas utilizadas por los ciberdelincuentes



¿Qué es la ingenieria social?

Es la práctica de obtener información confidencial **a través de la manipulación** de usuarios legítimos, basado en su comportamiento "es mas fácil manejar a las personas que a las máquinas"

Formas frecuentes de propagación: Llamadas telefónicas, e-mail, apps de mensajería, redes sociales, etc.

Dos tipos de ataques

Hunting

Busca afectar al mayor número de usuarios realizando únicamente una comunicación

Ejemplos: campañas de *phising* contra entidades (bancarias, de gobierno,etc) o campañas de infección por *malware*

Farming

Realizan varias comunicaciones con las víctimas hasta conseguir su objetivo o la mayor cantidad de información posible.

Ejemplos: extorsión con videos privados o futuros ataques contra la empresa. En otros suplantan a algún miembro de la empresa.

Técnicas utilizadas

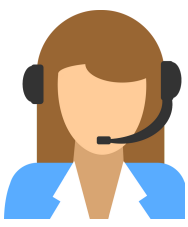
Respeto a la autoridad

Utilizando dominios de entidades de gobierno para intimidar el cumplimiento a regulaciones. Usualmente es usado vía e-mail.

Sentido de ayuda

Puede hacerse pasar por un falso empleado.
Ofrecer ayuda para instalar herramientas informáticas no autorizadas.

Temor a perder un servicio



Utilizando el argumento de accesos repetidos no autorizados a aplicaciones por lo general bancarias, se fuerza a la víctima a acceder a una web/app fraudulenta donde roban información confidencial.

Respeto social

Miedo a ser socialmente juzgado o a perder reputación. Utilizado mayormente en los correos de extorsión sexual.

Obsequios

Ofrecen un producto o servicio gratis a cambio de información privada. Suele ser frecuente en sitios poco legítimos, redes sociales o aplicaciones de mensajería.

Peter.
Business