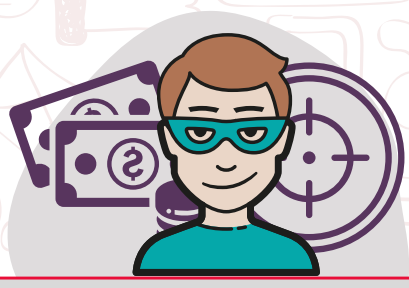
TÉCNICAS DE INGENIERÍA SOCIAL

¿Cómo logran engañarnos?

PRETEXTING

Base de cualquier ataque de ingeniería social.

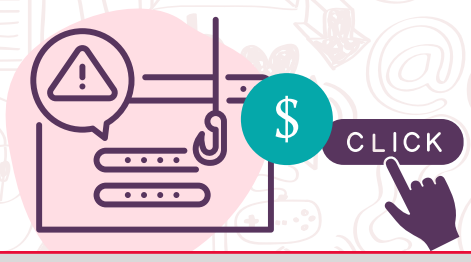
Consiste en elaborar un escenario/historia ficticia, donde el atacante tratará de que la víctima comparta información que, en circunstancias normales, no revelaría.



SEXTORSIÓN

Chantaje donde amenazan a la víctima

Buscan distribuir supuestamente contenido comprometido de ella a sus contactos (aunque no exista dicho contenido), si no accede a las peticiones del ciberdelincuente, generalmente a realizar un pago.



PHISHING

Busca "pescar" víctimas.

Generalmente se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas con el objetivo de tomar el control de sus equipos y robarles información confidencial.

BAITING

Emplea un cebo con software malicioso

A la vista de sus víctimas para que ellos mismos infecten sus dispositivos.

SMISHING

Se trata de una variante del "phishing" pero que se difunde a través de SMS.

Se pide al usuario que llame a un número en especial o que acceda a un enlace de una web falsa.

VISHING

Llamadas telefónicas

Donde el atacante se hace pasar por una organización/persona de confianza para que la víctima revele información privada.

SHOULDER SURFING

Consiste en mirar por "encima del hombro".

Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil.

QUID PRO QUO

Prometen un beneficio a cambio de información Personal

suelen ser compensaciones en formato regalo (merchandising, dinero o acceso gratuito a programas de pago).

DUMPSTER DIVING

Se refiere al acto de "husmear en la basura"

Se realiza con el fin de obtener documentos con información personal o financiera.

REDES SOCIALES

Las técnicas de engaño más comunes son mediante:

Cupones descuento, juegos y concursos, donde crees que puedes ganar algo.