



# INGENIERÍA SOCIAL



## ¿CÓMO NOS PUEDE AFECTAR?

Según el objetivo los podemos clasificar en:

**Fraude:** obtener dinero de la víctima, sin usar violencia.

**Infeción:** conseguir infectar el dispositivo con un software malicioso (virus).

**Robo de credenciales:** obtener claves de acceso a determinados servicios, como por ejemplo Correo Electrónico, Cuentas de Banco, etc.

*El sentido común y la precaución son los mejores aliados en la defensa contra la ingeniería social.*

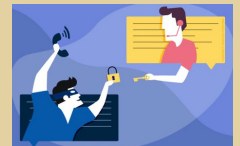


**LAS INSTITUCIONES NUNCA LE SOLICITARÁN DATOS PERSONALES O CREDENCIALES.**



## ¿QUÉ ES ?

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios desprevenidos y así obtener información privada, credenciales de acceso o permisos en sistemas de información que le permitan realizar daño.



## ¿CÓMO LO EVITAMOS?

- Fomentar la cultura de la discreción, educar al personal en la importancia de no divulgar información privada o sensible a desconocidos, en equipos o redes públicas ni en redes sociales.
- No revelar información personal ni datos confidenciales (credenciales de acceso, números de tarjetas de crédito, cuentas bancarias, etc.) por teléfono, email o servicios de mensajería instantánea.
- Verificar los ficheros adjuntos. No descargarlos si se desconoce su origen/contenido, aunque provengan de un contacto conocido.
- Si se contactan con usted por mail, mensaje de texto o teléfono solicitándole información personal o credenciales de cualquier tipo, comuníquese inmediatamente con la institución correspondiente para confirmar la legitimidad del contacto.