La **Ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de usuarios.
Más del 90% de los ataques exitosos a compañías involucran estas técnicas.

"..Si usan sistemas seguros puede que sus empleados sean débiles.."
—Mr.Red

Técnicas más usadas en ingeniería social

Pretexting:
El atacante crea un espacio creíble para que la víctima le de acceso a su ordenador, puesto de trabajo o teléfono celular, a manera de robar información, introducir malware, etc.

"No tengo batería, me prestas para cargar, por favor"

Tailgaiting:
Persuadir a la seguridad de una empresa/compañía a través de la manipulación de uno o más empleados.

Dumpster diving:
Conseguir en los botaderos de basura archivos importantes.

Shoulder surfing:
Obtener datos mirando de reojo o por encima el hombro.

Baiting:
Dejar USB/micro SD en lugares específicos para que personas seleccionadas lo inserten en sus ordenadores y así infectarlos.

Phishing:
Montar un escenario online para que la víctima de sus correos y credenciales.

Vishing:
Llamadas telefónicas en la que se desequilibra/sorprende a la víctima y cuando se haya vulnerable se le extraen datos personales o password, haciéndose pasar por banqueros, prestamistas, arrendatarios etc.

Redes sociales:
Todos podemos acceder a información publicada en los perfiles.