Técnicas de Ingeniería Social

Phishing

engaño/fraude para obtener información usando "cebos".

Subtipos:
a) Smishing. Phishing por SMS
b) Vishing (Phishing por voz / llamada)
c) Spear phishing (ataques dirigidos)
d) Whaling (dirigido a ejecutivos de alto nivel)

Spam

- Mensajes no solicitados, envío masivo.
- Contiene posibles enlaces maliciosos o desinformación.
- Subtipo: SPIM — spam por mensajería instantánea (WhatsApp, Telegram, DM de redes sociales, etc.

Invoice Scams

- Envío de facturas falsas para engañar y obtener pagos.
- Uso del miedo o urgencia ("si no pagas...") para presionar.

Dumpster Diving

- Buscar en la basura documentos que contienen información útil para ataques futuros.
- Contramedida sugerida: destruir los documentos confidenciales antes de desecharlos.

Identity Fraud

Usurpación de identidad para conseguir beneficios o cometer actos en nombre de otra persona.

Shoulder Surfing

- Observar lo que alguien escribe o ve en pantalla (por encima del hombro) para obtener datos sensibles.
- Prevención: asegurarse de privacidad visual, espacios adecuados para trabajar con datos confidenciales.

Prepending

- Incluir el nombre de la víctima al inicio de mensajes para generar cercanía ("rapport").
- Aumenta la probabilidad de que la víctima baje la guardia.

Pharming

- Redireccionamiento malicioso hacia sitio web falso que se hace pasar por uno legítimo.
- Usualmente involucra manipulación de DNS.

Eliciting information

Obtener datos sin preguntar directamente, usando técnicas de conversación: escucha activa, preguntas reflexivas, afirmaciones falsas para que la víctima corrija.

Tailgating

- Seguir a alguien para entrar con él en zonas restringidas (por cortesía, engaño, etc.).
- Uso de barreras físicas (turnos, accesos controlados) como prevención.

Técnicas de Ingeniería Social

Credential Harvesting

- Técnicas para recopilar contraseñas u otros credenciales.
- Importancia de la verificación en dos pasos (2FA) como medida de mitigación.

Reconnaissance

Recolección de información previa sobre la víctima/objetivo para personalizar ataques.

Hoax

- Engaños o bulos que buscan manipular para que la víctima realice acciones (por miedo, urgencia, difusión del mensaje).
- Tres partes: gancho, advertencia, petición.

Impersonation

Hacerse pasar por otra persona o fingir un rol/puesto para obtener confianza y ventajas.

Watering Hole Attack

Infectar un sitio de terceros frecuentado por la víctima; al visitarlo, la víctima también se infecta.

Typo Squatting

Crear dominios parecidos al legítimo con errores tipográficos; engañar para que la víctima crea estar en el sitio correcto.