Il **SOCIAL ENGINEERING** (ingegneria sociale) è una tecnica usata dagli hacker per **ingannare le persone** e ottenere **informazioni riservate**, **accessi** o **azioni** che normalmente non concederebbero.

In pratica, **l'attaccante non buca i sistemi, ma le persone**, sfruttando la fiducia, la disattenzione o la paura.

Esempio semplice

Ti chiama qualcuno fingendo di essere del reparto IT e ti chiede la password "per un controllo urgente": se gliela dai, l'attacco ha avuto successo. Non ha forzato il computer, ha convinto te.

Tecniche comuni di social engineering

1. **Phishing**
   Email o messaggi falsi che imitano banche, aziende o servizi noti.
   ➤ Scopo: farti cliccare su un link malevolo o inserire dati sensibili.
2. **Spear Phishing**
   Variante del phishing, ma **mirata a una persona specifica**, spesso con informazioni raccolte da social o LinkedIn.
   ➤ Più credibile e pericoloso.
3. **Pretexting (pretesto)**
   L'attaccante si inventa un ruolo (es. tecnico, collega, autorità) per convincerti a dare dati.
   ➤ "Ho bisogno del tuo numero di badge per aggiornare il sistema."
4. **Baiting (esca)**
   Lasciare un oggetto (es. una chiavetta USB infetta) in un luogo pubblico sperando che qualcuno lo usi.
   ➤ Attiva malware nel sistema.
5. **Tailgating (scroccone)**
   Seguire fisicamente una persona autorizzata in un'area riservata, senza badge.
   ➤ Tipico negli edifici aziendali.
6. **Vishing** (Voice phishing)
   Stesso principio del phishing, ma via telefono.
   ➤ Esempio: "Sono della banca, c'è un problema sul tuo conto, mi confermi i dati?"

Raccomandazioni generali contro il Social Engineering

1. **Formazione continua del personale**
2. ➤ Corsi periodici su phishing, pretexting, vishing, ecc.
3. ➤ Simulazioni pratiche per testare la reazione dei dipendenti.
4. **Politica del "Zero Trust" umano**
   ➤ Non fidarti di richieste non verificate, anche se sembrano legittime.
   ➤ Verifica sempre l'identità del mittente o del chiamante.
5. **Canali ufficiali per richieste sensibili**
   ➤ Le password, PIN o dati sensibili **non vanno mai condivisi via email o telefono**.

Contro il Phishing / Spear Phishing

- **Controllare l'indirizzo email del mittente** (sospetto se simile ma non identico a quello reale).
- **Non cliccare link o allegati** da fonti sconosciute o inattese.
- **Attivare filtri antispam e antivirus aggiornati**.
- **Utilizzare l'autenticazione a due fattori (2FA)** per email e accessi aziendali.

Contro il Pretexting

- **Verificare ogni richiesta fuori standard** tramite un canale secondario (es. telefono diretto dell'ufficio IT).
- **Mai dare informazioni personali o aziendali a chi non si è identificato correttamente**.
- **Standardizzare le richieste tecniche con moduli o ticket ufficiali**.

Contro il Baiting (es. USB infette)

- **Politica di divieto di uso di dispositivi USB esterni non autorizzati**.
- **Educare il personale a non usare chiavette trovate**.
- **Bloccare l'auto-esecuzione delle USB nei computer aziendali**.

Contro il Tailgating

- **Controllo fisico degli accessi** (badge individuali, porte con tornello o codice).
- **Divieto di far entrare estranei o "colleghi" sconosciuti senza badge**.
- **Formazione su comportamento sospetto nei locali aziendali**.

Contro il Vishing (chiamate ingannevoli)

- **Mai fornire dati riservati via telefono**, soprattutto se la chiamata è non richiesta.
- **Verifica dell'identità tramite richiamata su numero ufficiale**.
- **Registrazione e monitoraggio delle chiamate sospette**.

Strumenti e buone pratiche aziendali

- **Simulazioni regolari di attacchi** (phishing test, tentativi di tailgating, ecc.).
- **Politiche di sicurezza chiare e condivise** con i dipendenti.
- **Segnalazione facilitata di tentativi sospetti** (email/report con un click).

In generale per difendersi si consiglia di:

- Non condividere mai password o dati sensibili, nemmeno se chi chiede sembra affidabile.
- Controlla l'identità di chi ti contatta.
- Non cliccare link sospetti.
- Forma i dipendenti su queste minacce.