# Social Engineering e Tecniche di Difesa

## Obiettivo:

Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi. Questo esercizio vi guiderà attraverso la comprensione delle varie forme di social engineering, esempi reali di attacchi e strategie di difesa efficaci.

**Prompt utilizzato:**
Definisci il termine "social engineering", poi descrivi le tecniche piu' comuni usate dagli attaccanti. includi tra queste il phishing e il tailgating.

## Elaborazione della risposta:

Il social engineering e' una tecnica di manipolazione psicologica usata dagli attaccanti per indurre le persone a compiere azioni o a rivelare informazioni riservate, come password, dati personali o accessi a sistemi.

**Tecniche comuni di social engineering:**

1. **Phishing**
   Attacco in cui la vittima riceve un messaggio che sembra provenire da una fonte fidata, con l'obiettivo di:
   - convincerla a cliccare su un link malevolo,
   - inserire credenziali in un sito fasullo,
   - scaricare allegati infetti.

   ***Esempio*:** un'email della "banca" che dice "Abbiamo bloccato il tuo conto. Accedi subito".

   **Come difendersi?**
   Leggere con attenzione il messaggio ricevuto.
   Controllare che il mittente sia chi dice di essere.
   Contattare direttamente il mittente prima di proseguire per chiedere chiarimenti e assicurazioni.

2. **Spear phishing**
   Variante più mirata del phishing. Il messaggio è personalizzato sulla base delle informazioni pubbliche della vittima (social network, azienda, ecc.), aumentando la credibilità dell'inganno.

   **Come difendersi?**
   Come detto prima, bisogna accertarsi del mittente e controllare se ci sono o no errori sospetti nella stesura del messaggio.
   Se il messaggio ricevuto fa nascere dubbi, contattare subito chi e' di competenza prima di fare qualsiasi altra cosa.

3. **Pretexting**
   L’attaccante inventa una falsa identità o situazione per ottenere informazioni o accesso.

   ***Esempio:***
   finge di essere un tecnico IT che ha bisogno della tua password per “risolvere un problema”.

   **Come difendersi?**
   Nessuno chiederà mai la tua password per “risolvere un problema”, nella maggior parte dei casi, potrebbe trattarsi di un tentativo di truffa. Non bisognerebbe mai lasciare le proprie informazioni sensibili quando non si è sicuri di chi stia dall’altra parte.
   Anche in questo caso, contattare subito chi di competenza prima di fare azioni che comprometterebbero la propria sicurezza e quella dell’azienda.

4. **Baiting**
   L’uso di un'esca per attirare la vittima. Spesso si basa sulla curiosità o sul desiderio di ottenere qualcosa gratuitamente.

   ***Esempio:***
   Una chiavetta USB “dimenticata” in un luogo pubblico contenente malware, oppure un sito che promette di farti scaricare la versione craccata del tuo gioco preferito.

   **Come difendersi?**
   Non e’ oro tutto ciò che luccica, a volte e’ un tentativo di truffa.
   Conoscere bene le fonti da dove si prendono risorse o informazioni e’ essenziale per non essere vittime di hacker malevoli.
   Per testare un contenuto “sospetto” si possono usare macchine virtuali, ambienti isolati e antivirus.

5. **Tailgating (o piggybacking)**
   l’attaccante si introduce in un’area riservata seguendo una persona autorizzata, approfittando della cortesia (es. qualcuno tiene aperta la porta).

   ***Esempio:***
   un finto corriere che “si infila” in un edificio protetto quando un impiegato apre la porta.

   **Come difendersi?**
   Kevin D. Mitnick spiega in uno dei suoi libri come difendersi da questo tipo di attaccante: Non bisognerebbe fidarsi troppo di una faccia sconosciuta solo perche’ e’ stato cortese, la raccomandazione migliore e’ quella di chiedere sempre di mostrare un badge o un cartellino.
   Nello stesso libro spiega pero’ perche’ vedere un cartellino aziendale non e’ sufficiente ad assicurarsi della benevolenza del soggetto, bisogna accertarsi dei motivi e dell’identita’ della persona in caso non rispecchi chi dice di essere.

6. **Quid Pro Quo**
   L’attaccante offre un beneficio (supporto tecnico, un regalo, ecc.) in cambio di informazioni o accesso.

   ***Esempio*:**
   Finge di essere dell'assistenza IT e ti chiede la password per "aiutarti".

   **Come difendersi?**
   Rifiuta qualsiasi aiuto tecnico o offerta se ti chiedono in cambio password, accessi o dati riservati: è quasi sempre un inganno.