



# S5L4

# Social Engineering

---

## Social Engineering:

Il prompt fornito a ChatGPT per fornirmi una descrizione del social engineering è stato:

Potresti spiegarmi dettagliatamente ma in maniera concisa, cos'è il Social Engineering. E le varie tecniche utilizzate, e ovviamente come prevenire a tali attacchi. Grazie



Il *Social Engineering* è una tecnica di manipolazione psicologica usata per indurre le persone a compiere azioni o rivelare informazioni riservate. Gli attaccanti puntano a sfruttare la fiducia, la curiosità, l'insicurezza o la fretta delle vittime per ottenere dati sensibili come password, informazioni bancarie o altre risorse digitali. Questi attacchi non si basano su vulnerabilità tecniche, ma piuttosto sulle debolezze umane.

Successivamente mi ha descritto le tecniche più utilizzate:

## Principali Tecniche di Social Engineering

1. **Phishing:** Una delle tecniche più comuni, in cui l'attaccante invia email, messaggi o siti web falsi che sembrano autentici, per spingere l'utente a inserire le proprie credenziali o scaricare malware.
2. **Spear Phishing:** Versione mirata del phishing, indirizzata a una specifica persona o azienda. L'attaccante raccoglie informazioni preliminari sulla vittima per rendere l'attacco più credibile.
3. **Pretexting:** L'attaccante finge di essere una persona fidata (come un collega o un fornitore) con un pretesto convincente per ottenere informazioni riservate. Potrebbe fingere di essere un tecnico informatico che chiede le credenziali per "risolvere" un problema.
4. **Baiting:** Si basa sulla curiosità o sull'avidità dell'utente. Gli attaccanti offrono qualcosa di allettante (come un file gratuito o una chiavetta USB trovata "per caso") che, una volta aperto, infetta il dispositivo con malware.
5. **Tailgating:** Tecnica fisica in cui l'attaccante accede a un'area riservata seguendo qualcuno (come un dipendente) senza mostrare credenziali, sfruttando la cortesia della vittima.
6. **Quid Pro Quo:** Simile al baiting, ma offre un "servizio" in cambio di informazioni. Ad esempio, l'attaccante può fingere di essere un tecnico e promettere assistenza gratuita in cambio dell'accesso al computer della vittima.

Ed infine come prevenire a tali attacchi:

## Come Prevenire il Social Engineering

1. **Formazione e Consapevolezza:** Educare i dipendenti sui rischi del social engineering e sulle tecniche usate dagli attaccanti. Formazioni regolari possono ridurre notevolmente i rischi.
2. **Verifica delle Identità:** Non fornire mai informazioni riservate a persone che non hanno verificato la propria identità. Usare protocolli di verifica come l'autenticazione a due fattori.
3. **Politiche di Sicurezza Rigorose:** Implementare politiche aziendali che limitino l'accesso ai dati solo alle persone autorizzate e addestrare i dipendenti a non cliccare su link sospetti o a non inserire credenziali su siti non verificati.
4. **Uso di Antivirus e Firewall:** Strumenti di sicurezza come antivirus e firewall possono bloccare molte minacce che potrebbero derivare da file infetti o siti dannosi.
5. **Simulazioni di Attacco:** Organizzare periodicamente test di phishing e simulazioni di social engineering per testare la preparazione dei dipendenti e migliorare le difese.

Seguendo queste pratiche, è possibile ridurre notevolmente il rischio di cadere vittima di attacchi di social engineering.

Il prompt successivo è stato utile per scoprire quali sono le **CVE** (**C**ommon **V**ulnerabilities **E**xposures) di Windows 10:

Ora mi puoi fornire una lista dei CVE relativo a Windows 10, descrivendoli sinteticamente, fornendomi anche le soluzioni ottimali. Grazie



Ecco cinque vulnerabilità recenti di Windows 10 con descrizioni e soluzioni:

1. **CVE-2024-38063 (TCP/IP Zero-Click RCE)**

- **Descrizione:** Una vulnerabilità in IPv6 permette esecuzione di codice remoto senza interazione.
- **Rimedio:** Installare la patch; in alternativa, disabilitare IPv6 BLEEPINGCOMPUTER BLEEPINGCOMPUTER .

2. **CVE-2024-43468 (Microsoft Configuration Manager)**

- **Descrizione:** Permette attacchi remoti tramite richieste modificate in Configuration Manager.
- **Rimedio:** Aggiornare subito e usare un account di servizio sicuro TENABLE® .

3. **CVE-2024-43533 e CVE-2024-43599 (Remote Desktop Client)**

- **Descrizione:** Vulnerabilità di esecuzione di codice remoto; un server compromesso può eseguire codice su client vulnerabili.
- **Rimedio:** Applicare le patch e disabilitare Remote Desktop quando non necessario TENABLE® BLEEPINGCOMPUTER .

4. **CVE-2024-38247 (Windows Graphics Component)**

- **Descrizione:** Vulnerabilità che consente l'elevazione dei privilegi nei componenti grafici di Windows.
- **Rimedio:** Installare le patch di settembre 2024 BLEEPINGCOMPUTER .

Aggiornare il sistema con le patch ufficiali è essenziale per la protezione da queste vulnerabilità.