

# ChatGPT

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



Certamente! Ecco una panoramica concisa ma dettagliata sul Social Engineering, le tecniche principali e come prevenire gli attacchi.

## Cos'è il Social Engineering

Il Social Engineering è una tecnica di manipolazione psicologica utilizzata per indurre le persone a rivelare informazioni confidenziali o a compiere azioni specifiche, come cliccare su un link malevolo o divulgare credenziali. Gli attaccanti sfruttano la fiducia, la curiosità, la paura o l'urgente bisogno di risolvere un problema per influenzare la vittima.

## Tecniche Comuni di Social Engineering

- **Phishing:** E-mail, SMS o siti web falsi che imitano entità fidate per ottenere informazioni sensibili come username e password.
- **Spear Phishing:** Variante del phishing, altamente mirata su singole persone o organizzazioni. Gli attacchi sono personalizzati con informazioni specifiche della vittima.
- **Pretexting:** L'attaccante si presenta come una figura autorevole o di fiducia (come un agente bancario o un tecnico IT) per ottenere informazioni o convincere la vittima a compiere un'azione.

- **Baiting:** Attira le vittime con promesse o incentivi (es. USB infettate lasciate in luoghi pubblici, o file di download interessanti) per ottenere accesso ai loro dispositivi.
- **Quid Pro Quo:** Gli attaccanti offrono un vantaggio o un servizio in cambio di informazioni o accesso.
- **Tailgating/Piggybacking:** Accesso non autorizzato a un edificio o area sfruttando la cortesia di dipendenti legittimi (es. accodandosi dietro qualcuno che entra con il badge).

## Prevenzione degli Attacchi di Social Engineering

- **Educazione e Formazione:** Formare il personale su riconoscimento e gestione delle tecniche di Social Engineering. Gli aggiornamenti regolari migliorano la consapevolezza.
- **Verifica dell'Identità:** Prima di fornire informazioni o eseguire richieste, verificare sempre l'identità del richiedente attraverso canali ufficiali.
- **Doppia Autenticazione (2FA):** Utilizzare l'autenticazione a due fattori per una sicurezza aggiuntiva, rendendo più difficile per gli attaccanti accedere agli account.
- **Aggiornamenti e Sicurezza IT:** Mantenere software, antivirus e sistemi di sicurezza aggiornati per proteggersi da attacchi che potrebbero sfruttare vulnerabilità.
- **Politiche di Accesso Fisico e Digitale:** Controllare l'accesso agli spazi e ai dati sensibili. Limitare l'accesso ai soli utenti autorizzati e monitorare i log di accesso.

- **Diffidare dalle Richieste di Informazioni Sensibili:** Non condividere informazioni sensibili (password, codici, etc.) via e-mail o telefono, soprattutto se la richiesta sembra sospetta.

## **Conclusione**

Il Social Engineering è tra le minacce più insidiose poiché sfrutta le debolezze umane. Una combinazione di formazione, politiche di sicurezza e pratiche preventive aiuta a proteggere le informazioni e ridurre il rischio di attacchi.

-

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

**Ecco un riepilogo delle vulnerabilità note di Windows 10, incluse alcune soluzioni consigliate per mitigare i rischi:**

- CVE-2021-36934 (SeriousSAM o HiveNightmare)
  - Questa vulnerabilità permette a utenti con privilegi limitati di accedere al file Security Account Manager (SAM), che contiene hash delle password, tramite copie shadow dei file di sistema. Gli attaccanti possono sfruttare questa vulnerabilità per ottenere privilegi elevati.

- Soluzione: limitare i permessi sulla cartella %windir%\system32\config ed eliminare le copie shadow precedenti. Microsoft ha consigliato di eseguire i comandi in PowerShell per mitigare temporaneamente il problema.
- CVE-2024-38063 (Vulnerabilità RCE IPv6)
  - Questa vulnerabilità permette un'escalation dei privilegi tramite una condizione di competizione nell'IPv6. Gli attaccanti potrebbero ottenere il controllo di sistema completo, rendendo questa vulnerabilità una delle più critiche.
  - Soluzione: Microsoft ha già rilasciato una patch; si consiglia di aggiornare il sistema operativo per prevenire possibili exploit.
- CVE-2024-38213 (Bypass del Mark of the Web)
  - Questa vulnerabilità consente di bypassare il filtro SmartScreen, esponendo il sistema a file pericolosi. Richiede che la vittima apra un file compromesso.
  - Soluzione: applicare le patch di sicurezza più recenti e sensibilizzare gli utenti su file e link sospetti.

- CVE-2024-38199 (Remote Code Execution per il servizio LPD)
  - Questa vulnerabilità consente l'esecuzione remota di codice (RCE) attraverso il servizio di stampa Line Printer Daemon (LPD), permettendo potenzialmente agli attaccanti di eseguire comandi malevoli.
  - Soluzione: disattivare il servizio LPD se non necessario e applicare le patch rilasciate da Microsoft.
- CVE-2024-21302 (Elevazione dei privilegi del kernel sicuro)
  - Questa vulnerabilità consente di elevare i privilegi accedendo al kernel in modo non autorizzato.
  - Soluzione: installare le ultime patch di sicurezza e mantenere il sistema operativo aggiornato.

Mantenere Windows 10 aggiornato è essenziale per ridurre il rischio di attacchi tramite vulnerabilità note. Microsoft rilascia aggiornamenti di sicurezza regolarmente per queste e altre vulnerabilità, per cui è consigliato effettuare aggiornamenti automatici e rivedere le politiche di gestione dei permessi su file critici.

**Daniel\_Gabriel\_Costeanu**