

# INTELLIGENZA ARTIFICIALE

Usando dei prompt andremo ad interrogare chat gpt su alcuni quesiti ovvero:

- Social Engineering
- Difese contro il Social Engineering

In fine lo interrogheremo sulle vulnerabilità di un sistema operativo.

## Social Engineering

Usando il seguente prompt andremo a interrogare gpt sul **SOCIAL ENGINEERING**. Il prompt è “ChatGPT, potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?”

La sua risposta sarà:

Certo! Il social engineering è una pratica in cui gli attaccanti manipolano le persone per ottenere informazioni sensibili o accesso a sistemi protetti. A differenza di attacchi tecnici, come quelli informatici, il social engineering si basa sulla manipolazione psicologica.

Ecco alcune delle tecniche più comuni:

1. **Phishing:** Questa tecnica coinvolge l'invio di email o messaggi falsi che sembrano provenire da fonti affidabili. Gli attaccanti cercano di indurre le vittime a rivelare informazioni personali, come password o dati bancari, cliccando su link malevoli o aprendo allegati infetti.
2. **Spear Phishing:** Simile al phishing, ma più mirato. Gli attaccanti personalizzano i messaggi per ingannare specifiche vittime, utilizzando informazioni raccolte su di loro per rendere l'attacco più credibile.
3. **Pretexting:** In questo caso, l'attaccante crea una falsa identità o scenario (pretesto) per ottenere informazioni. Ad esempio, può spacciarsi per un dipendente di una compagnia telefonica e chiedere dati sensibili.
4. **Baiting:** Gli attaccanti offrono qualcosa di allettante (come un file gratuito) per indurre le vittime a scaricare malware o a rivelare informazioni.
5. **Tailgating:** Questa tecnica implica seguire una persona autorizzata in un'area protetta, sfruttando la cortesia della vittima. Ad esempio, un attaccante potrebbe chiedere di entrare in un edificio mentre qualcuno tiene aperta la porta.

6. **Quizzing:** Qui, l'attaccante pone domande che sembrano innocue per raccogliere informazioni utili. Può avvenire in contesti informali o formali.

Queste tecniche si basano sulla fiducia e sulla vulnerabilità umana, rendendo essenziale la formazione e la consapevolezza per prevenire tali attacchi.

## Difese contro il Social Engineering

Usando il seguente prompt interroghiamo Chat gpt sulle **difese contro il Social Engineering**. “ChatGPT, potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering?”

La sua risposta sarà:

Certo! Ecco alcune strategie efficaci per difendersi dagli attacchi di social engineering:

1. **Formazione e consapevolezza:** Educa te stesso e il tuo team sulle tecniche di social engineering. Conoscere i vari tipi di attacchi aiuta a riconoscerli e a non cadere nelle trappole.
2. **Verifica delle informazioni:** Quando ricevi richieste di informazioni sensibili, verifica sempre l'identità della persona che richiede tali dati. Usa canali ufficiali per contattare l'ente o la persona.
3. **Utilizzo di autenticazione a più fattori (MFA):** Implementare l'MFA rende più difficile per un attaccante accedere ai tuoi account, anche se riesce a ottenere la tua password.
4. **Attenzione ai dettagli:** Sii cauto con email o messaggi che contengono errori grammaticali, link sospetti o richieste urgenti. Questi possono essere segnali di un attacco di phishing.
5. **Protezione fisica:** Adotta misure di sicurezza fisica, come badge di accesso e controlli di ingresso. Monitora le aree sensibili e fai attenzione a persone che cercano di entrare senza autorizzazione.
6. **Uso di software di sicurezza:** Installa e aggiorna regolarmente software antivirus e firewall. Questi strumenti possono aiutare a rilevare e prevenire attacchi informatici.
7. **Politiche aziendali chiare:** Stabilisci politiche chiare riguardo alla gestione delle informazioni sensibili. Assicurati che tutti i dipendenti conoscano le procedure da seguire in caso di richieste sospette.

8. **Controllo degli accessi:** Limita l'accesso alle informazioni sensibili solo a chi ne ha realmente bisogno. Questo riduce il rischio che un attaccante possa raccogliere dati sensibili.
9. **Sviluppo di una cultura della sicurezza:** Promuovi un ambiente in cui i dipendenti si sentano sicuri nel segnalare comportamenti sospetti senza timore di ripercussioni.
10. **Simulazioni di attacchi:** Conduci esercitazioni di simulazione di attacchi di social engineering per testare la prontezza del personale e migliorare le loro capacità di riconoscimento e risposta.

Adottando queste strategie, puoi ridurre significativamente il rischio di cadere vittima di attacchi di social engineering.

## Vulnerabilità di un sistema operativo

Quando interroghiamo chat gpt più siamo specifici e attenti nel formulare le domande e più lui ci darà informazioni, con questo prompt gli chiederemo le vulnerabilità di un sistema operativo windows 11. Il prompt è “chat gpt potresti fornirmi una lista dei CVE relativi a windows 11? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi dettagli delle vulnerabilità e le soluzioni consigliate”

La risposta sarà:

Certo! Ecco una lista di alcuni CVE (Common Vulnerabilities and Exposures) rilevanti per Windows 11, insieme a dettagli su alcune di queste vulnerabilità e le soluzioni consigliate.

### Esempi di CVE per Windows 11

1. **CVE-2021-34527 (PrintNightmare)**
  - a. **Dettagli:** Questa vulnerabilità consente l'esecuzione di codice remoto tramite il servizio di spooler di stampa. Gli attaccanti possono sfruttarla per installare programmi, visualizzare, modificare o eliminare dati.
  - b. **Soluzione:** Microsoft ha rilasciato aggiornamenti di sicurezza per mitigare questa vulnerabilità. Si consiglia di aggiornare il sistema operativo e disabilitare il servizio di spooler di stampa se non necessario.
2. **CVE-2021-36948**
  - a. **Dettagli:** Una vulnerabilità che può consentire l'esecuzione di codice remoto a causa di una gestione inadeguata degli oggetti in memoria. Può colpire applicazioni che utilizzano determinate librerie.

- b. **Soluzione:** È fondamentale installare gli aggiornamenti di sicurezza rilasciati da Microsoft per mitigare il rischio.

### 3. CVE-2022-21907

- a. **Dettagli:** Vulnerabilità di elevazione dei privilegi nel componente Windows Kernel. Un attaccante può sfruttarla per ottenere diritti elevati.
- b. **Soluzione:** Microsoft ha pubblicato patch di sicurezza. È consigliabile mantenere il sistema aggiornato.

### 4. CVE-2022-30134

- a. **Dettagli:** Vulnerabilità che consente l'esecuzione di codice remoto nel protocollo HTTP. Gli attaccanti possono sfruttare questa vulnerabilità per attaccare il sistema.
- b. **Soluzione:** Aggiornamenti di sicurezza sono disponibili; assicurati di applicarli.

### 5. CVE-2023-21716

- a. **Dettagli:** Vulnerabilità di sicurezza che può consentire l'elevazione dei privilegi nel driver di Windows. Può essere sfruttata da un attaccante locale.
- b. **Soluzione:** Microsoft ha rilasciato aggiornamenti per correggere questa vulnerabilità. Si raccomanda di applicare gli aggiornamenti.

## Raccomandazioni Generali

- **Aggiornamenti Regolari:** Mantieni Windows 11 aggiornato applicando regolarmente gli aggiornamenti di sicurezza forniti da Microsoft.
- **Software di Sicurezza:** Usa un software antivirus affidabile e assicurati che sia sempre aggiornato.
- **Backup dei Dati:** Esegui backup regolari dei dati per proteggerti da eventuali attacchi ransomware.
- **Formazione:** Educa gli utenti su come riconoscere potenziali minacce e come comportarsi in caso di attacco.

Per una lista più dettagliata e aggiornata dei CVE, puoi visitare il [NVD \(National Vulnerability Database\)](#) o il sito di Microsoft dedicato alla sicurezza.

Come possiamo vedere chat gpt è uno strumento molto potente che nelle mani di un mal intenzionato può essere dannoso. Mentre è uno strumento molto utile per le azioni quotidiane.