

Prompt utilizzato per ChatGPT: "Forniscimi un'analisi approfondita delle principali tecniche di social engineering, includendo esempi reali per ogni tecnica. Descrivi i metodi utilizzati dagli attaccanti, i loro obiettivi e i segnali che possono aiutare a identificarli. Inoltre, fornisci raccomandazioni dettagliate per prevenire ciascun tipo di attacco sia a livello individuale che aziendale."

## **Titolo: Tecniche di Social Engineering e Strategie di Prevenzione**

**1. Introduzione** Il social engineering rappresenta una delle minacce più insidiose per la sicurezza informatica e aziendale. Piuttosto che attaccare i sistemi direttamente, i criminali sfruttano la psicologia umana per ottenere accesso a dati sensibili, sistemi e strutture. Comprendere le tecniche utilizzate e adottare misure preventive è fondamentale per proteggere individui e organizzazioni.

## **2. Principali Tecniche di Social Engineering**

### **2.1 Phishing**

Email o messaggi fraudolenti progettati per sembrare legittimi, con l'obiettivo di spingere l'utente a rivelare informazioni riservate.

*Esempio:* Email che simula una comunicazione bancaria, richiedendo l'accesso a un sito falso.

*Prevenzione:* Verificare sempre il mittente, non cliccare su link sospetti, utilizzare autenticazione a due fattori.

### **2.2 Spear Phishing**

Versione mirata del phishing che utilizza informazioni specifiche sull'individuo per aumentare la credibilità.

*Esempio:* Email indirizzata a un dipendente con dettagli del progetto in corso.

*Prevenzione:* Formazione continua del personale, verifica interna delle richieste, autenticazione a più livelli.

### **2.3 Pretexting**

L'attaccante costruisce un falso pretesto per convincere la vittima a fornire informazioni.

*Esempio:* Fingere di essere un tecnico IT per ottenere le credenziali.

*Prevenzione:* Politiche di verifica dell'identità, sensibilizzazione ai ruoli e responsabilità.

### **2.4 Baiting**

L'utente è attirato con un'esca (es. dispositivo USB infetto) per indurlo a eseguire azioni rischiose.

*Esempio:* USB lasciata intenzionalmente nei pressi dell'ufficio.

*Prevenzione:* Non utilizzare dispositivi sconosciuti, controlli antivirus regolari, politica di sicurezza fisica.

## 2.5 Tailgating

Accesso non autorizzato a strutture protette seguendo un dipendente autorizzato.

*Esempio:* Un individuo entra senza badge approfittando della cortesia di chi apre la porta.

*Prevenzione:* Controlli fisici, badge obbligatori, formazione sulla sicurezza aziendale.

## 2.6 Vishing (Voice Phishing)

Telefonate ingannevoli per raccogliere informazioni personali o aziendali.

*Esempio:* Chiamata da finto operatore tecnico che richiede dati bancari.

*Prevenzione:* Non fornire dati al telefono, richiamare tramite numeri ufficiali, formazione per il riconoscimento delle frodi.

## 3. Raccomandazioni Generali di Prevenzione

- **Formazione continua:** sensibilizzare dipendenti e utenti sui rischi e sulle tecniche comuni.
- **Verifica dell'identità:** introdurre protocolli per confermare l'identità di chi richiede informazioni.
- **Controlli tecnici:** implementare strumenti di sicurezza come firewall, antivirus e autenticazione multifattoriale.
- **Politiche aziendali:** sviluppare procedure interne chiare per la gestione di informazioni sensibili.
- **Monitoraggio e auditing:** tenere traccia delle attività sospette e condurre controlli regolari.

**4. Conclusione** Il social engineering sfrutta debolezze umane più che tecnologiche. Per questo, la prevenzione richiede una combinazione di consapevolezza, tecnologia e procedure rigorose. Investire nella formazione e nella cultura della sicurezza è la chiave per ridurre significativamente i rischi.

Prompt per tecniche di Difesa:

"Quali sono le strategie e le migliori pratiche per difendersi dagli attacchi di social engineering? Fornisci tecniche di difesa efficaci a livello individuale e organizzativo, includendo esempi concreti di buone pratiche e consigli su come implementarle."

---

**Risposta riassuntiva basata su questo prompt:**

**Strategie di Difesa Efficaci:**

1. **Formazione e sensibilizzazione degli utenti**

- *Obiettivo:* Educare su cosa sia il social engineering e come si presenta.
- *Tecniche:* Corsi regolari, simulazioni di phishing, test periodici.

## **2. Verifica dell'identità prima di condividere informazioni**

- *Buona pratica:* Chiamare direttamente un collega o usare canali ufficiali prima di rispondere a richieste sospette.

## **3. Autenticazione a più fattori (MFA)**

- *Efficacia:* Anche se una password viene rubata, l'accesso non è concesso senza il secondo fattore.

## **4. Politiche di sicurezza aziendale chiare e condivise**

- *Esempio:* Linee guida su come gestire richieste telefoniche, e-mail sospette e accessi fisici.

## **5. Controllo degli accessi fisici e digitali**

- *Pratica:* Badge individuali, blocco automatico dei PC, gestione dei ruoli utente.

## **6. Backup regolari e piani di risposta agli incidenti**

- *Scopo:* Minimizzare i danni in caso di attacco riuscito.

## **7. Segnalazione facile e incentivata dei comportamenti sospetti**

- *Strumento:* Pulsanti “Segnala phishing” nelle e-mail o canali dedicati interni.

Esercizio Bonus:

Prompt fornito a chatgpt: "Forniscimi una lista dei CVE (Common Vulnerabilities and Exposures) rilevanti per Google Chrome , specificando l'ID del CVE, una breve descrizione della vulnerabilità, la sua gravità (CVSS score), e la data di pubblicazione. Includi sia vulnerabilità client che lato server, se disponibili. Approfondisci poi le vulnerabilità più critiche con dettagli tecnici, impatto potenziale, e misure di mitigazione."



## **Elenco delle vulnerabilità CVE critiche per Google Chrome**

CVE ID	Descrizione	Gravità (CVSS)	Data di pubblicazione	Versioni affette
CVE-2025-2783	Bypass della sandbox tramite malware sofisticato diffuso via phishing (Operation ForumTroll)	Critica	Marzo 2025	Versioni precedenti all'aggiornamento di marzo 2025
CVE-2024-4671	Use-after-free in Visuals, potenziale fuga dalla sandbox	9.6	Maggio 2024	< 124.0.6367.201
CVE-2024-8638	Type confusion nel motore V8, esecuzione di codice arbitrario	8.8	Febbraio 2024	< 128.0.6613.137
CVE-2024-12382	Use-after-free nel componente Translate, rischio di heap corruption	Alta	Dicembre 2024	< 131.0.6778.140
CVE-2023-5217	Heap buffer overflow in libvpx (VP8), esecuzione di codice remoto	Critica	Settembre 2023	< 117.0.5938.132
CVE-2023-4863	Heap buffer overflow in libwebp, esecuzione di codice remoto	Critica	Agosto 2023	< 116.0.5845.188
CVE-2023-6345	Integer overflow in Skia, esecuzione di codice arbitrario	Alta	Novembre 2023	< 119.0.6045.200
CVE-2023-5187	Use-after-free nelle estensioni, potenziale corruzione della memoria	Alta	Settembre 2023	< 117.0.5938.132

## Approfondimento delle vulnerabilità più critiche

### CVE-2025-2783 – Bypass della sandbox tramite malware sofisticato

- **Descrizione tecnica:** Questa vulnerabilità zero-day consente a un malware, distribuito tramite link di phishing, di bypassare la sandbox di Chrome senza ulteriori interazioni da parte dell'utente.

- **Impatto:** Compromissione completa del sistema, con accesso a dati sensibili e possibilità di esecuzione di codice arbitrario.
- **Mitigazione:** Aggiornare immediatamente Chrome all'ultima versione disponibile e evitare di cliccare su link sospetti ricevuti via email. [New York Post+1ORDR+1](#)

#### CVE-2024-4671 – Use-after-free in Visuals

- **Descrizione tecnica:** Un errore di gestione della memoria nel componente Visuals può essere sfruttato per eseguire codice arbitrario o eludere la sandbox di Chrome.
- **Impatto:** Esecuzione di codice non autorizzato, potenzialmente con privilegi elevati.
- **Mitigazione:** Aggiornare Chrome alla versione 124.0.6367.201 o successiva. [ORDR](#)

#### CVE-2023-4863 – Heap buffer overflow in libwebp

- **Descrizione tecnica:** Una vulnerabilità nella libreria libwebp utilizzata per la gestione delle immagini WebP può essere sfruttata per eseguire codice arbitrario.
- **Impatto:** Compromissione del sistema tramite la visualizzazione di immagini WebP malevole.
- **Mitigazione:** Aggiornare Chrome alla versione 116.0.5845.188 o successiva. [CERT-EU+5CERT-EU+5stack.watch+5](#)

---

#### Raccomandazioni generali di sicurezza

- **Aggiornamenti regolari:** Assicurarsi che Chrome sia sempre aggiornato all'ultima versione disponibile.
- **Cautela con i link:** Evitare di cliccare su link sospetti o provenienti da fonti non verificate.
- **Gestione delle estensioni:** Installare solo estensioni da fonti affidabili e rimuovere quelle non necessarie.
- **Utilizzo di strumenti di sicurezza:** Implementare soluzioni antivirus e firewall aggiornate per una protezione aggiuntiva.

Risultato: Offrendo a chatpgt un prompt ben configurato e con le giuste informazioni e specifiche si riescono ad avere informazioni veramente utili in pochissimo tempo.