# **SOCIAL ENGINEERING E TECNICHE COMUNI**

**PROMPT:** sto seguendo un corso di cybersecurity. elencami con una spiegazione dettagliata le tecniche di social engineering più utilizzate che conosci ed includi per ognuna una spiegazione sulle strategie di difese più efficaci

**RISPOSTA:** Ecco un elenco delle tecniche di social engineering più utilizzate, con una spiegazione dettagliata e strategie di difesa per ciascuna:

### **1. Phishing**

**Descrizione:**Consiste nell'invio di messaggi fraudolenti (email, SMS o social media) che imitano comunicazioni ufficiali per indurre le vittime a fornire informazioni sensibili (es. credenziali di accesso, dati finanziari) o a cliccare su link dannosi.

**Strategie di difesa:**

* **Educazione e consapevolezza:** Formare gli utenti per riconoscere email sospette, controllare gli URL e non cliccare su link non verificati.
* **Autenticazione a più fattori (MFA):** Riduce l'efficacia del phishing impedendo accessi non autorizzati.
* **Filtri anti-phishing:** Utilizzare software che blocchino email fraudolente.
* **Politiche di verifica:** Non inviare mai dati sensibili tramite email o SMS.

### **2. Pretexting**

**Descrizione:**L'attaccante inventa uno scenario credibile (pretesto) per ottenere informazioni confidenziali, come fingere di essere un tecnico IT, un cliente o un'autorità.

**Strategie di difesa:**

* **Verifica dell'identità:** Richiedere sempre prove d'identità prima di fornire informazioni sensibili.
* **Formazione del personale:** Insegnare a non fidarsi ciecamente di richieste di informazioni sensibili senza verifiche.
* **Politiche aziendali:** Stabilire che nessuna informazione sensibile venga condivisa senza conferme multiple.

### **3. Baiting**

**Descrizione:**L'attaccante attira la vittima con una "esca" come un dispositivo USB infetto o un link a contenuti apparentemente attraenti per installare malware o rubare informazioni.

**Strategie di difesa:**

* **Non fidarsi di dispositivi sconosciuti:** Vietare l'uso di dispositivi USB trovati o non forniti dall'azienda.
* **Soluzioni endpoint security:** Utilizzare software per rilevare malware su dispositivi connessi.
* **Politiche di sicurezza:** Educare gli utenti a non scaricare file o accedere a contenuti non verificati.

### **4. Tailgating (o piggybacking)**

**Descrizione:**Un attaccante si intrufola in un'area protetta seguendo qualcuno autorizzato (es. entrando dietro a una persona in un edificio con badge di accesso).

**Strategie di difesa:**

* **Controllo degli accessi:** Utilizzare sistemi come porte girevoli o tornelli che permettono il passaggio di una persona alla volta.
* **Formazione:** Educare i dipendenti a non consentire l'accesso a sconosciuti.
* **Badge visibili:** Richiedere ai dipendenti di indossare sempre il badge di identificazione.

### **5. Vishing**

**Descrizione:**L'attaccante utilizza chiamate vocali per ingannare la vittima, spesso fingendo di essere un rappresentante di una banca, un ente governativo o un'azienda.

**Strategie di difesa:**

* **Non condividere informazioni sensibili per telefono:** Richiedere un contatto ufficiale verificato prima di fornire dati.
* **Numero di richiamo:** Chiamare autonomamente il numero ufficiale dell'organizzazione per verificare l'autenticità.
* **Riconoscere pressioni:** Diffidare di richieste urgenti o intimidatorie.

### **6. Spear Phishing**

**Descrizione:**Variante del phishing mirata a un individuo o gruppo specifico, utilizzando informazioni personali per creare messaggi altamente personalizzati e credibili.

**Strategie di difesa:**

* **Formazione specifica:** Educare i dipendenti a verificare anche le email apparentemente legittime.
* **Monitoraggio delle comunicazioni:** Implementare sistemi che analizzino il contenuto delle email per rilevare anomalie.
* **Limitazione delle informazioni pubbliche:** Ridurre la quantità di dati personali disponibili online.

### **7. Dumpster Diving**

**Descrizione:**Consiste nel recuperare informazioni sensibili scartate, come documenti stampati, ricevute o dispositivi elettronici.

**Strategie di difesa:**

* **Distruzione sicura:** Utilizzare distruggi documenti per smaltire documenti sensibili.
* **Gestione dei rifiuti elettronici:** Garantire la cancellazione sicura dei dati da dispositivi prima dello smaltimento.
* **Sorveglianza:** Monitorare le aree di smaltimento per prevenire accessi non autorizzati.

### **8. Shoulder Surfing**

**Descrizione:**L'attaccante osserva fisicamente o attraverso dispositivi (telecamere, binocoli) per carpire informazioni come password o PIN.

**Strategie di difesa:**

* **Privacy screen:** Utilizzare schermi protettivi per impedire la visualizzazione laterale.
* **Protezione fisica:** Essere consapevoli dell'ambiente e coprire la tastiera durante l'inserimento di PIN.
* **Protocolli di lavoro sicuro:** Evitare di lavorare su informazioni sensibili in luoghi pubblici.

### **9. Impersonation**

**Descrizione:**L'attaccante si presenta come una persona di fiducia, come un collega, un fornitore o un'autorità, per ottenere accesso a informazioni o risorse.

**Strategie di difesa:**

* **Doppia verifica:** Confermare l'identità attraverso un canale separato prima di fornire informazioni o accesso.
* **Controlli rigorosi:** Richiedere credenziali ufficiali o referenze per visitatori e richieste.
* **Sensibilizzazione:** Addestrare i dipendenti a riconoscere segnali di impersonazione.

Queste tecniche evidenziano quanto sia cruciale combinare formazione, tecnologia e processi per prevenire attacchi di social engineering. Se ti serve un approfondimento su una tecnica specifica, fammi sapere!

## **ESERCIZIO BONUS: ESPLORAZIONE DEI CVE TRAMITE CHATGPT**

**PROMPT:** ciao chat, scegli un software a tua scelta fra quelli più famosi ed usati in questo momento

**RISPOSTA:** Ciao! Un software famoso e molto utilizzato attualmente è **Microsoft Teams**. È una piattaforma di collaborazione e comunicazione utilizzata da aziende, scuole e team in tutto il mondo per chat, videoconferenze, condivisione di file e integrazione con altre applicazioni.

Se vuoi approfondire questo o un altro software, fammi sapere!

**PROMPT:** forniscimi una lista dei CVE relativi al software che hai scelto. vorrei anche informazioni più dettagliate su alcuni di questi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate

**RISPOSTA:** Ecco alcune vulnerabilità (CVE) relative a Microsoft Teams, con dettagli aggiuntivi e suggerimenti per la mitigazione:

### **CVE rilevanti per Microsoft Teams**

1. **CVE-2024-38197**: Vulnerabilità di spoofing nella versione iOS di Microsoft Teams. Consente a un attaccante remoto di imitare identità all'interno dell'applicazione, aumentando il rischio di phishing.
   * **Soluzione**: Aggiornare all'ultima versione dell'app per iOS e implementare regole di comunicazione più restrittive tra tenant esterni.
2. **CVE-2024-21374**: Problema di divulgazione delle informazioni sulla versione Android di Teams. Un utente potrebbe essere ingannato nell'installare un'applicazione creata ad hoc per accedere a dati sensibili.
   * **Soluzione**: Limitare l'installazione di app da fonti non attendibili e implementare soluzioni di gestione dei dispositivi mobili (MDM) per controllare le app aziendali.
3. **CVE-2023-4863**: Overflow del buffer nella libreria WebP utilizzata da Microsoft Teams. Questa vulnerabilità consente l'esecuzione di codice arbitrario o il crash del sistema.
   * **Soluzione**: Applicare immediatamente la patch fornita da Microsoft e monitorare la presenza di aggiornamenti relativi a librerie di terze parti come WebP.
4. **CVE-2020-10146**: Vulnerabilità di tipo stored cross-site scripting (XSS) nella piattaforma online di Microsoft Teams, sfruttabile per ottenere token di autenticazione o eseguire comandi arbitrari.
   * **Soluzione**: Assicurarsi che le configurazioni di sicurezza siano aggiornate e monitorare costantemente i log di accesso per attività sospette.
5. **CVE-2023-29328 e CVE-2023-29330**: Problemi di esecuzione di codice remoto tramite Teams, in cui un attaccante convince un utente a partecipare a una riunione malevola.
   * **Soluzione**: Educare gli utenti a riconoscere inviti sospetti e attivare strumenti di monitoraggio per individuare attività anomale nelle riunioni.
6. **CVE-2020-17091**: Un attaccante potrebbe eseguire codice arbitrario tramite exploit su Microsoft Teams in specifiche condizioni di configurazione.
   * **Soluzione**: Configurare criteri di sicurezza rigorosi e adottare il principio del privilegio minimo per gli utenti.

### **Best practice generali per mitigare i rischi**

* **Aggiornamenti regolari**: Mantenere sempre aggiornati Microsoft Teams e tutti i software correlati.
* **Limitazioni alla comunicazione esterna**: Ridurre il numero di tenant esterni autorizzati a contattare gli utenti interni.
* **Formazione e consapevolezza**: Sensibilizzare gli utenti sui rischi delle minacce, soprattutto quelle provenienti da piattaforme di collaborazione come Teams.
* **Multi-Factor Authentication (MFA)**: Garantire che tutte le sessioni di accesso richiedano autenticazione multi-fattore per prevenire l'accesso non autorizzato.

Queste vulnerabilità evidenziano l'importanza di una gestione proattiva della sicurezza per strumenti di comunicazione largamente utilizzati. Per ulteriori dettagli, è possibile consultare i database CVE ufficiali, come quello di [MITRE](https://cve.mitre.org)