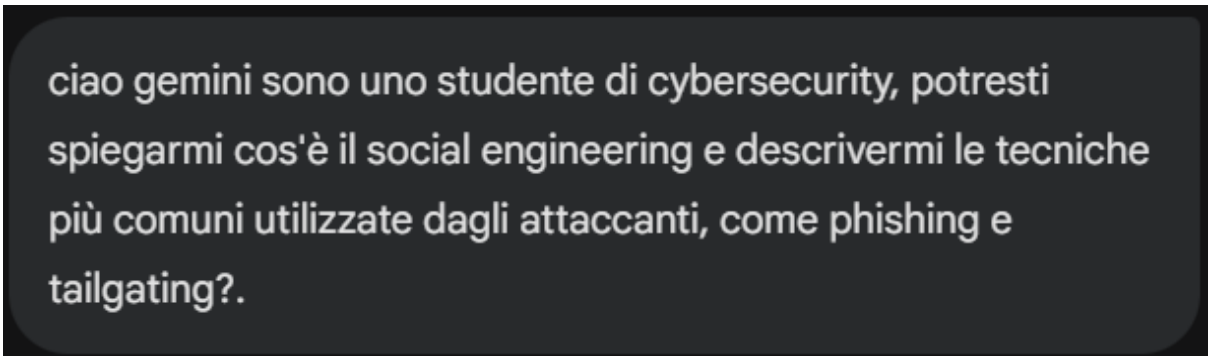
SOCIAL ENGINEERING

Obbiettivo:

Conoscere e scoprire le tecniche di **social engineering** e imparare come difendersi da questi tipi di attacchi. Questo esercizio ci aiuterà a comprendere quali tipi di minacce ci sono e come difendervi da esse.



Spiegazione:

Il social engineering è l'arte di manipolazione psicologica delle persone (come la paura, il senso di urgenza o il desiderio di aiutare) per indurre a rivelare informazioni riservate o a compiere azioni che compromettono la sicurezza.
Invece a differenza di attacchi informatici "**tecnici**" che sfruttano le vulnerabilità dei software o dell'hardware, il social engineering va a colpire la parte più debole della catena di sicurezza ovvero **"l'essere umano".**
L'attaccante va a "**hackerare**" in senso figurato la mente della vittima:
-Fiducia: Fingersi una persona della quale ci si può fidare (un agente di polizia, un tecnico, ecc).
-**Curiosità**: Offrire qualcosa di allettante (un premio, una macchina, un telefono, ecc)
-**Urgenza** e paura: Indurre la vittima alla fretta e non a ragionare lucidamente (il tuo account sta per essere eliminato, i tuoi dati bancari sono visibili a tutti, ecc)

Tecniche più diffuse:

Phishing:

È la tecnica più diffusa e si basa sull'invio di messaggi ingannevoli per rubare dati sensibili.
-**Phishing standard**: Mandare email in massa.
-**Smishing e Vishing**: Variante che usa SMS o chiamate Telefonice.

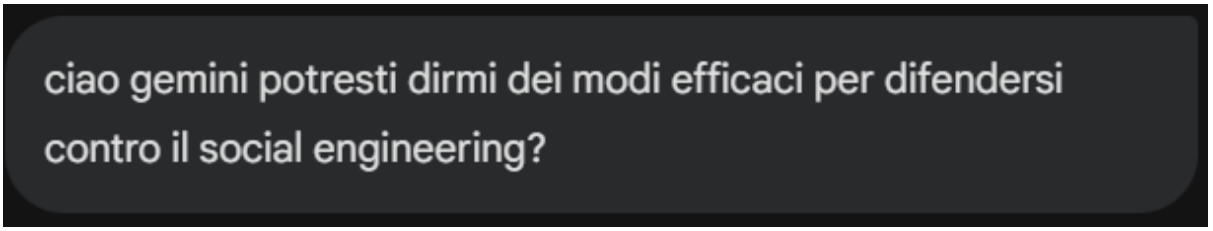
Tailgating:

Questa è una tecnica di sicurezza fisica. L'attaccante segue una persona autorizzata all'interno di un'area riservata (ad esempio un ufficio o un data center) prima che la porta si chiuda.
Esempio: L'attaccante arriva alla porta con le mani occupate da scatole pesanti, contando sulla cortesia del dipendente che gli terrà aperta la porta senza chiedergli di strisciare il badge.

Pretexting:
L'attaccante crea uno scenario inventato (un "**pretesto**") per indurre la vittima a fornire dati.
Esempio: Un hacker telefona a un dipendente spacciandosi per un tecnico dell'IT che deve "verificare un problema sull'account" e richiede la password per risolvere il guasto.

Baiting:
Si basa sulla curiosità o sull'avidità della vittima.
Esempio: Lasciare una chiavetta USB infetta in un parcheggio aziendale con un'etichetta intrigante come **"Aumenti Salari 2025"**. Se un dipendente la inserisce nel PC per curiosità, il malware viene installato automaticamente.

Come difendersi:

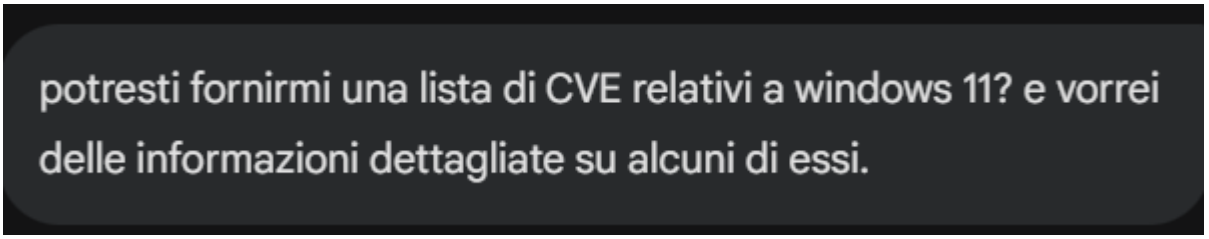


Difendersi dal social engineering è una sfida continua perché, come hai imparato, l'obiettivo non è un computer ma la psiche umana. Essendo nel 2026, le tecniche sono diventate ancora più sofisticate grazie all'uso di intelligenze artificiali che creano "**deepfake**" audio e video quasi indistinguibili dalla realtà.

La difesa è la tua attitudine mentale.
-Rallenta (Slow Down): Gli attaccanti creano un senso di **urgenza** o **paura** per impedirti di pensare logicamente. Se un messaggio ti mette fretta, è un segnale d'allarme.
-Verifica l'identità (Out-of-Band Verification): Se ricevi una richiesta sospetta da un collega o dalla tua banca, non rispondere direttamente. Contattami tu usando un canale ufficiale diverso (es. chiama il numero sul retro della carta o usa l'app ufficiale).
-Diffida dei Deepfake: Nel 2026, una voce familiare al telefono o un viso in videochiamata non garantiscono più l'identità. Se la richiesta riguarda dati sensibili o bonifici, usa una "parola d'ordine" concordata precedentemente o fai domande personali a cui solo la vera persona saprebbe rispondere.

Conclusione:
L'analisi condotta evidenzia come nessuna infrastruttura possa dirsi sicura se non accompagnata da rigorose policy di gestione del fattore umano. Tecniche come il **phishing** e il **pretexting** dimostrano che l'inganno psicologico è spesso più efficace di un attacco **brute-force**. Per mitigare questi rischi, le organizzazioni devono adottare un approccio **Multi-Layered**, combinando l'autenticazione a più fattori (**MFA**) con programmi di formazione continua. Solo attraverso la costante vigilanza e l'adozione di un modello **Zero Trust** è possibile ridurre drasticamente la superficie di attacco esposta alle manipolazioni dei social engineer.

CVE cosa sono:



CVE sta per **Common Vulnerabilities and Exposures** (Vulnerabilità ed Esposizioni Comuni). È un elenco pubblico di falle di sicurezza informatica note, che funge da "dizionario standard" per l'intero settore.
Prima della nascita del sistema **CVE** (creato da **MITRE Corporation** nel 1999), ogni azienda dava un nome diverso alla stessa vulnerabilità. Questo creava confusione. Il **CVE** risolve il problema assegnando un **identificativo univoco** a ogni falla, permettendo a diversi strumenti di sicurezza, database e ricercatori di "parlare la stessa lingua".

Esempi di CVE:

CVE-2025-21298: Windows OLE RCE (Zero-Click)
Questa è stata una delle vulnerabilità più pericolose dell'inizio del 2025
-Dettagli Tecnici: La falla risiede nella libreria ole32.dll, specificamente nella funzione che gestisce i documenti RTF. È un attacco **zero-click**: la vittima non deve nemmeno aprire l'allegato; basta che il client email (come Outlook) visualizzi l'anteprima del messaggio per innescare l'exploit.
-**Impatto**: Permette all'attaccante di eseguire codice arbitrario con i privilegi dell'utente corrente, portando al controllo completo del sistema.

CVE-2025-62215: Windows Kernel Privilege Escalation
Scoperta a fine 2025, questa vulnerabilità è stata sfruttata attivamente "**in the wild**".
-**Dettagli Tecnici:** Si tratta di una **Race Condition** nel kernel di Windows. Un attaccante locale con privilegi bassi può eseguire un'applicazione appositamente creata che manipola la memoria di sistema, innescando un errore di sincronizzazione (double-free).
-**Impatto:** Permette di passare da un utente standard a privilegi di livello **SYSTEM**, garantendo il controllo totale del dispositivo. Spesso viene usata "**in catena**" dopo un accesso iniziale ottenuto via **phishing.**