

Report Utilizzo Prompt Gemini

Preparazione Ambiente ed Introduzione

Per i seguente report ed esercizio ci serviremo di un'intelligenza artificiale per studiare le tecniche di Social Engineering e i suggerimenti da utilizzare per migliorare questo aspetto della sicurezza.

Prompt 1: Social Engineering e significato

Ciao gemini sono uno studente di cybersecurity e sto studiando le tecniche di social engeneering ma non le ho comprese a fondo, potresti elencarmele con spiegazione ed esempi pratici?

Di seguito il primo prompt che in cui si chiedono informazioni riguardo la materia:

Risposta:

- ◆ Ciao! È un piacere aiutarti. Come studente di cybersecurity, capirai presto che l'anello debole della catena non è quasi mai un firewall configurato male, ma l'essere umano.
Il **Social Engineering** si basa sulla manipolazione psicologica. Il ragionamento di fondo è semplice: è molto più facile convincere qualcuno a darti la sua password che cercare di craccarla con un attacco brute-force.
Ecco le tecniche principali spiegate nel dettaglio:

1. Phishing (e varianti)
È il "grande classico". Consiste nell'invio di messaggi fraudolenti per rubare dati sensibili o installare malware.
 - **Ragionamento:** Sfrutta il **senso di urgenza** o l'**autorità**. L'attaccante punta sulla reazione impulsiva dell'utente davanti a un problema improvviso.
 - **Esempio pratico:** Ricevi una mail che sembra provenire dal dipartimento IT della tua università: "Aggiornamento sicurezza obbligatorio: clicca qui entro 2 ore o il tuo account verrà sospeso". Il link porta a una pagina di login identica a quella vera, ma controllata dall'hacker.
2. Pretexting
Qui l'attaccante crea uno scenario inventato (un pretesto) per ottenere informazioni.
 - **Ragionamento:** Si basa sulla **costruzione di fiducia**. A differenza del phishing generico, qui c'è una storia studiata per farti abbassare le difese.
 - **Esempio pratico:** Un malintenzionato ti chiama fingendosi un operatore della tua banca. Ti dice che c'è un "tentativo di frode" in corso sul tuo conto. Per "fermarlo", ti chiede di confermare la tua identità leggendo il codice che ti è appena arrivato via SMS (che in realtà è il codice per autorizzare un suo bonifico).

Di seguito quindi viene illustrato come il Social Engineering una delle tecniche più semplici ma a volte più efficaci per penetrare la sicurezza di un'azienda che all'apparenza sembra impenetrabile. Quest'ultima quindi diventa "bucabile" a causa dell'errore umano. Vengono individuati poi i vari metodi per mettere in pratica questa tecnica.

3. Baiting (L'esca)

Come suggerisce il nome, si offre qualcosa di allettante per indurre la vittima in errore.

- **Ragionamento:** Sfrutta la **curiosità** o l'**avidità**.
- **Esempio pratico:** Un hacker abbandona una chiavetta USB nel parcheggio di un'azienda con un'etichetta scritta a mano: "Conti aziendali e Bonus 2025". Un dipendente curioso la raccoglie e la inserisce nel PC per vedere cosa c'è dentro, attivando un malware autorun che infetta la rete.

4. Quid Pro Quo

Significa "qualcosa in cambio di qualcos'altro". L'attaccante offre un servizio in cambio di informazioni.

- **Ragionamento:** Sfrutta il principio di **reciprocità**. Se qualcuno ci aiuta, ci sentiamo in dovere di ricambiare o di fidarci.
- **Esempio pratico:** Un attaccante chiama a tappeto i numeri di un'azienda fingendosi il supporto tecnico Microsoft: "Salve, abbiamo rilevato dei rallentamenti sulla sua linea, posso aiutarla a velocizzare il PC?". Se l'utente sta davvero avendo problemi, sarà ben felice di dare l'accesso remoto al "tecnico".

5. Tailgating (e Piggybacking)

Questa è una tecnica di ingegneria sociale "fisica".

- **Ragionamento:** Sfrutta la **cortesia comune** e il desiderio di evitare conflitti sociali.
- **Esempio pratico:** L'attaccante si presenta all'ingresso riservato di un ufficio con le mani occupate da scatole di pizza o caffè. Aspetta che un dipendente apra la porta con il badge e, con un sorriso, si fa tenere la porta aperta. Il dipendente, per educazione, lo lascia passare senza controllare se abbia il permesso.

Tabella Riassuntiva dei Trigger Psicologici

Tecnica	Leva Psicologica Principale	Obiettivo
Phishing	Paura / Urgenza	Credenziali, Dati bancari
Pretexting	Fiducia / Autorità	Informazioni riservate
Baiting	Curiosità / Avidità	Accesso al sistema (Malware)
Quid Pro Quo	Reciprocità	Accesso remoto, Password
Tailgating	Educazione / Desiderio di aiutare	Accesso fisico ai locali

 Esporta in Fogli



Consiglio da "collega": Nello studio della cybersecurity, ricorda che queste tecniche spesso vengono combinate (es. un Pretexting che prepara il terreno per un Phishing mirato).

Ti piacerebbe analizzare un caso reale di attacco famoso per vedere come queste tecniche sono state applicate in scala reale?

fammi un'esempio di attacchi reali famosi

Dopo aver elencato tutte le tecniche di Social Engineering Gemini in questo caso pone l'accento sul fatto che quest'ultime possono essere combinate. Dunque ho acconsentito alla sua richiesta di mostrarmi casi conclamati realmente accaduti.

◆ Certamente! Analizzare casi reali è il modo migliore per capire quanto queste tecniche siano efficaci, anche contro giganti della tecnologia che spendono milioni in sicurezza.

Ecco tre degli esempi più famosi e didattici nella storia della cybersecurity:

1. L'attacco a Twitter (2020) – "Il Grande Hack"

Questo è uno dei casi più eclatanti di **Vishing** (Voice Phishing).

- **Cosa è successo:** Un gruppo di hacker è riuscito a prendere il controllo di account famosi come quelli di **Elon Musk, Barack Obama, Bill Gates e Apple**, usandoli per promuovere una truffa legata ai Bitcoin.
- **La tecnica:** Gli hacker non hanno bucato il server di Twitter. Hanno chiamato alcuni dipendenti dell'assistenza fingendosi tecnici dell'IT interno. Hanno convinto i dipendenti che c'erano problemi con la VPN aziendale e li hanno guidati su un sito di login falso, dove i dipendenti hanno inserito le loro credenziali.
- **Il risultato:** Ottenendo le credenziali dei dipendenti, gli hacker sono entrati nel pannello di amministrazione interno di Twitter, avendo potere assoluto su qualsiasi account della piattaforma.

Tra i casi citati in particolare ho preso in esame l'attacco a Twitter effettuato nel 2020. Questo a dimostrare quanto bisogna essere preparati anche solo ad una semplice chiamata proveniente dall'esterno dell'azienda.

Prompt 2: Soluzioni alle tecniche di Social Engineering

Di seguito il prompt per chiedere probabili strategie per difendersi da questi attacchi:

quali sono quindi le migliori strategie per difendersi da tali attacchi?

Risposta:

- ◆ Ottima domanda. Come avrai intuito dagli esempi precedenti, la difesa non può essere solo tecnologica perché l'attaccante punta all'errore umano. Una strategia di difesa efficace deve essere **multilivello**, agendo sia sulla tecnologia che sulla cultura aziendale.

Ecco le migliori strategie divise per tipologia:

1. Difesa Tecnologica (Hardening)

Anche se il social engineering colpisce l'uomo, la tecnologia può limitare i danni o bloccare il tentativo sul nascere.

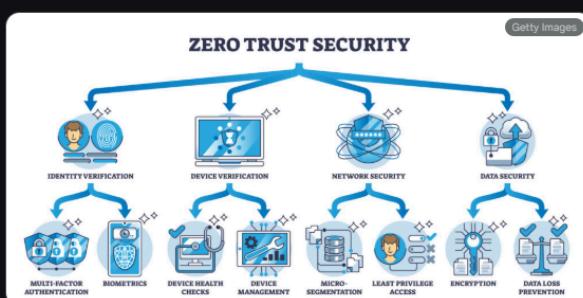
- **Multi-Factor Authentication (MFA) Robusta:** Non usare solo gli SMS (vulnerabili al SIM swapping), ma preferire app di autenticazione (Google Authenticator) o chiavi fisiche (YubiKey).
- **Filtri Anti-Phishing e DMARC:** Configurare protocolli come SPF, DKIM e DMARC per validare le email in arrivo e impedire che hacker possano "spoofare" (imitare) l'indirizzo email di un dirigente.
- **Endpoint Detection and Response (EDR):** Se un dipendente clicca su un link e scarica un malware (Baiting), un buon EDR può bloccare l'esecuzione del processo malevolo prima che si diffonda nella rete.

2. Difesa Organizzativa e Procedurale

Bisogna creare processi che rendano difficile l'esecuzione dell'attacco.

- **Princípio del Minimo Privilegio (PoLP):** Un dipendente dovrebbe avere accesso solo ai dati strettamente necessari per il suo lavoro. Se viene hackerato, l'attaccante avrà un raggio d'azione limitato.
- **Verifica "Fuori Canale" (Out-of-Band):** È la difesa più efficace contro il Pretexting. Se ricevi una richiesta insolita via email (es. "cambia l'IBAN per questo pagamento"), devi confermare la richiesta chiamando il mittente su un numero ufficiale già noto, non quello fornito nell'email.

- **Separazione dei compiti (Segregation of Duties):** Per operazioni critiche (come bonifici di grandi somme), dovrebbero essere necessarie l'approvazione di almeno due persone diverse.



3. Difesa Culturale (Security Awareness)

Questa è la parte più difficile ma fondamentale: trasformare i dipendenti da "vulnerabilità" a "sensori".

- **Simulazioni di Phishing:** Inviare email finte di test per vedere chi clicca. Chi sbaglia non viene punito, ma riceve una formazione immediata. Questo abitua l'occhio a riconoscere i segnali di allarme.
- **Cultura del "No Blame":** Se un dipendente clicca su un link sospetto, deve sentirsi libero di segnalarlo subito all'IT senza paura di ripercussioni. La velocità di segnalazione è critica per contenere i danni.
- **Formazione Psicologica:** Insegnare alle persone a riconoscere i trigger (urgenza, autorità, paura). Se qualcuno ti mette fretta, è il primo segnale che potrebbe essere un attacco.

Riassunto della Strategia di Difesa

Tipo di Attacco	Strategia di Difesa Primaria
Phishing	MFA, Filtri email, Awareness
Pretexting	Verifica fuori canale (chiamata di conferma)
Baiting	Disabilitazione porte USB, Policy "clean desk"
Tailgating	Badge obbligatori, tornelli, cultura della sicurezza fisica
MFA Fatigue	Utilizzo di chiavi FIDO2 (fisiche) anziché notifiche push

 Esporta in Fogli 

Il mio ragionamento

La difesa perfetta non esiste, ma l'obiettivo della cybersecurity è **alzare il costo dell'attacco**.

Se un hacker deve superare un filtro email, convincere un dipendente formato, aggirare una chiave fisica e poi scontrarsi con un processo di doppia approvazione, probabilmente cercherà una vittima più facile.

Ti andrebbe di provare a simulare un breve scenario? Io proverò a "manipolarti" con una tecnica di social engineering e tu dovrà dirmi come mi scopriresti o come ti difenderesti. Che ne dici?



Gemini in questo caso quindi consiglia delle strategie per difendersi da queste pratiche, come ad esempio l'utilizzo di autenticatori di accesso come Google Authenticator, utilizzare filtri antiphishing ecc. ma soprattutto formare il personale interno "ignorante" in modo da prima di tutto evitare o quanto meno evitare danni gravi avvisando immediatamente il team di IT.

Conclusioni

A conclusione del report possiamo assumere che per quanto possa essere impenetrabile la sicurezza, l'errore umano è uno dei fattori più sottovalutati ma più efficaci e che ognuno di noi ha dei punti deboli che possono essere sfruttati.