

S5E4

Prompt per ChatGPT

Cosa sono i prompt?

Un "prompt" è un input o una richiesta che fornisci a un sistema di intelligenza artificiale per ottenere una risposta o un'azione. Nei modelli di linguaggio, come quelli utilizzati in cybersecurity, un prompt è una frase o una domanda che guida il modello a generare una risposta specifica. I prompt sono davvero importanti perché ci aiutano a ottenere risposte più precise e mirate. È come prendere appunti durante una lezione: ricordando ciò che è stato detto prima, possiamo costruire su quelle informazioni per avere una discussione più approfondita e significativa. Questo è particolarmente vero con IA come ChatGPT, che possono memorizzare ciò che è stato detto in precedenza per offrire risposte più pertinenti e ben contestualizzate. Quindi, sfruttare i prompt correttamente può migliorare notevolmente la qualità delle informazioni che riceviamo e delle risposte che diamo.

Esercizio pratico

Obiettivo: Esplorare le tecniche di social engineering e imparare come difendersi da questi tipi di attacchi. Questo esercizio vi guiderà attraverso la comprensione delle varie forme di social engineering, esempi reali di attacchi e strategie di difesa efficaci.

1. Scrivere un prompt per comprendere al meglio il social engineering

2. Scrivere un prompt che mi possa spiegare come mi proteggo dal social engineering

Prompt1: chat spiegami in maniera dettagliata cos'è il Social Engineering, ho bisogno di sapere nella maniera più approfondita possibile ogni singolo attacco a disposizione.

In questo caso chat ci ha fornito una risposta ricca e dettagliata, volendo possiamo sfruttare la sua memoria e scrivendo prompt come 'riassumi in 10 righe', chat ci andrà a riassumere i concetti chiesti con il prompt precedente.

Risposta chatGPT

Il **Social Engineering** è una forma di manipolazione psicologica usata per ottenere informazioni, accesso o guadagni illeciti. Si basa sulla capacità di sfruttare la fiducia, la curiosità, la paura o altri sentimenti delle persone per manipolarle e indurle a rivelare informazioni o compiere azioni dannose. Questa tecnica viene frequentemente utilizzata in ambito cyber per condurre attacchi informatici, ma può anche essere applicata a situazioni di vita quotidiana.

Come funziona il Social Engineering

L'attaccante cerca di sfruttare la naturale inclinazione delle persone a fidarsi di chi sembra autorevole o a rispondere rapidamente in situazioni percepite come urgenti. Le tecniche di Social Engineering mirano a superare le difese umane piuttosto che quelle tecnologiche, rendendole efficaci anche contro sistemi di sicurezza avanzati.

Tipi di Attacchi di Social Engineering

Di seguito, descriverò in dettaglio le tipologie più comuni di attacchi di Social Engineering.

1. **Phishing**

Il **phishing** è una delle tecniche più diffuse e si basa sull'invio di email, messaggi di testo o link che sembrano provenire da fonti legittime, ma in realtà sono progettati per indurre la vittima a fornire informazioni personali o finanziarie.

- **Esempio:** Un'email che sembra provenire dalla banca della vittima, che la informa di una presunta attività sospetta e la invita a cliccare su un link per verificare il conto. Cliccando, la vittima viene indirizzata a un sito web falso dove inserisce le proprie credenziali di accesso, che vengono rubate.

- **Sottotipi di Phishing:**

- **Spear Phishing:** Versione mirata del phishing che si concentra su una singola persona o un piccolo gruppo, usando informazioni personali per aumentare la credibilità.

- **Whaling:** Mirato a obiettivi di alto profilo, come dirigenti di aziende.

- **Smishing:** Phishing via SMS o messaggi istantanei.

- **Vishing**: Phishing via telefonata, spesso con attori umani o con l'uso di sistemi di risposta automatica.

2. **Pretexting**

Nel **pretexting**, l'attaccante crea uno scenario falso per ottenere informazioni dalla vittima. L'attaccante finge di essere qualcuno di autorevole o fidato e chiede alla vittima informazioni sensibili.

- **Esempio**: L'attaccante chiama un dipendente fingendosi un tecnico IT e sostiene che ci sia un problema con l'account aziendale della vittima, chiedendole di fornire password o dettagli del sistema.

- **Caratteristica distintiva**: L'attaccante costruisce un "pretesto" credibile, utilizzando spesso informazioni personali sulla vittima per risultare convincente e autorevole.

3. **Baiting**

Il **baiting** sfrutta la curiosità umana per spingere la vittima a compiere un'azione che comprometta il proprio sistema o le proprie informazioni.

- **Esempio**: Un attaccante lascia una chiavetta USB infetta in un'area pubblica, come un parcheggio aziendale. Chiunque la trovi potrebbe essere tentato di collegarla al proprio computer per vedere cosa contiene, permettendo all'attaccante di accedere al sistema informatico.

- **Variante digitale**: Link allettanti o falsi download online che promettono contenuti interessanti, come film, musica o software, ma contengono malware.

4. **Tailgating (o Piggybacking)**

Il **tailgating** è una tecnica di Social Engineering fisica che sfrutta la fiducia o la distrazione delle persone per ottenere accesso a spazi fisici protetti.

- **Esempio**: Un attaccante si avvicina a una persona che entra in un edificio con accesso limitato, facendosi tenere la porta aperta senza mostrare il proprio badge, o fingendo di averlo dimenticato.

- **Piggybacking**: Variante in cui la vittima è consapevole dell'attaccante, ma acconsente a farlo entrare. Ad esempio, se qualcuno chiede gentilmente di essere accompagnato all'interno.

5. **Quid Pro Quo**

Nel **quid pro quo**, l'attaccante promette un beneficio o un servizio in cambio di informazioni sensibili o di un'azione da parte della vittima.

- **Esempio**: Un attaccante si spaccia per tecnico di assistenza e chiama diverse persone all'interno di un'azienda, dicendo di dover risolvere un problema informatico. Alcuni dipendenti potrebbero essere disposti a dare informazioni di accesso per "ricevere aiuto".

- **Differenza dal pretexting**: In questo caso, viene offerto uno scambio piuttosto che creare un pretesto elaborato.

6. **Shoulder Surfing**

Il **shoulder surfing** implica osservare direttamente la vittima per ottenere informazioni come PIN, password o altre credenziali. Questo può avvenire sia fisicamente che con strumenti digitali come telecamere nascoste.

- **Esempio**: Un attaccante si posiziona dietro qualcuno in un bar mentre quest'ultimo inserisce la password sul computer, osservando la sequenza di tasti.

- **Tecnica avanzata**: Utilizzo di telecamere o binocoli per osservare da lontano, ad esempio quando la vittima usa un bancomat.

7. **Dumpster Diving**

Nel **dumpster diving**, l'attaccante cerca informazioni riservate tra i rifiuti, come documenti aziendali scartati, appunti con password, lettere o supporti digitali.

- **Esempio**: L'attaccante recupera documenti bancari o file di backup che non sono stati distrutti correttamente.

- ****Prevenzione****: Molte aziende utilizzano trita-documenti o aziende specializzate nello smaltimento sicuro dei documenti per proteggersi.

8. ****Impersonation****

L'****impersonation**** implica che l'attaccante si finge un'altra persona per ottenere informazioni o accesso. È una delle tecniche di Social Engineering più pericolose quando viene combinata con l'uso di identità realistiche.

- ****Esempio****: Un attaccante si finge un impiegato di un'azienda partner e convince un dipendente a dargli l'accesso al sistema aziendale.

- ****Utilizzo frequente****: Questo approccio è comune nelle grandi aziende, dove il flusso di persone rende più difficile verificare l'identità di chiunque.

Come Difendersi dal Social Engineering

Il Social Engineering si basa principalmente sulla vulnerabilità umana, quindi la ****consapevolezza e la formazione**** sono essenziali per ridurre i rischi. Ecco alcuni suggerimenti chiave:

1. ****Educazione e formazione****: Fornire formazione periodica a dipendenti e utenti su come riconoscere tentativi di Social Engineering.
2. ****Verifica dell'identità****: Quando si ricevono richieste di informazioni, è sempre bene verificare l'identità della persona che le richiede.
3. ****Politiche aziendali****: Stabilire e comunicare chiare procedure di sicurezza, come il cambio regolare delle password o la segnalazione di email sospette.
4. ****Sistemi di autenticazione a più fattori (MFA)****: Una protezione aggiuntiva anche nel caso in cui una password venga compromessa.
5. ****Sicurezza fisica****: Migliorare la sicurezza negli edifici per ridurre i rischi di accesso non autorizzato tramite tailgating.

Il Social Engineering è una minaccia che continua ad evolvere, e il miglior modo per difendersi è mantenersi informati e vigili, poiché, come detto, nessun sistema tecnologico è efficace contro una persona inconsapevolmente ingannata.

Come possiamo notare chatGPT ci ha già fornito una piccola base di difesa contro il social engineering, ora sfrutteremo il prompt precedente per richiedere un'ulteriori informazioni più dettagliate dal punto di vista di difesa.

Prompt2: Approfondisci in maniera dettagliata come posso difendermi dal social engineering

Risposta chatGPT:

Difendersi dal ****Social Engineering**** richiede una combinazione di misure tecniche, consapevolezza e pratica costante. Gli attacchi di Social Engineering sono subdoli perché non puntano direttamente a vulnerabilità informatiche, ma sfruttano le debolezze umane, come la fiducia, la fretta e la paura. Per evitare di cadere vittima di questi attacchi, è fondamentale adottare misure preventive su più livelli. Ecco una guida dettagliata su come proteggersi.

1. ****Formazione e Consapevolezza del Personale****

La formazione continua è essenziale per aiutare le persone a riconoscere tentativi di manipolazione e frodi.

- ****Corsi periodici di sicurezza informatica****: Prevedere training specifici su phishing, pretexting, baiting e altri tipi di attacchi di Social Engineering. Utilizzare casi studio reali per aiutare le persone a identificare segnali di allarme.

- ****Simulazioni di attacchi di Social Engineering****: Programmare esercitazioni simulate, ad esempio tramite campagne di phishing interne, per testare la consapevolezza dei dipendenti e rafforzare le capacità di riconoscimento delle truffe.

- ****Creazione di una cultura della sicurezza****: Incoraggiare i dipendenti a non condividere mai informazioni sensibili e a verificare sempre le richieste, anche quelle che sembrano provenire da persone fidate.

2. ****Implementare Politiche e Procedure di Sicurezza****

Avere policy aziendali ben definite e seguite può ridurre notevolmente il rischio.

- ****Procedure di verifica delle richieste****: Stabilire una prassi in cui ogni richiesta di informazioni sensibili o accesso richiede una doppia conferma, soprattutto per le richieste telefoniche o via email.
- ****Separazione dei compiti****: Limitare l'accesso alle informazioni solo a chi ha bisogno di saperle per lavorare. Questa misura previene che un singolo individuo possa essere manipolato per ottenere accesso illimitato.
- ****Uso dell'autenticazione a più fattori (MFA)****: L'MFA protegge le credenziali di accesso anche se le password vengono compromesse, dato che richiede un'ulteriore conferma, come un codice inviato via SMS o tramite un'app autenticatrice.

3. ****Riconoscere i Segnali di Social Engineering****

Identificare e reagire ai tentativi di manipolazione è cruciale per evitare di cadere nella trappola.

- ****Attenzione a richieste urgenti o sospette****: I tentativi di Social Engineering spesso fanno leva sulla fretta. Frasi come “deve essere fatto subito” o “è un'emergenza” sono segnali d'allarme. Abituarsi a verificare sempre le richieste, anche in condizioni di pressione.
- ****Verificare le fonti****: In caso di dubbi, contattare direttamente la persona o l'organizzazione tramite canali ufficiali per verificare la richiesta.
- ****Attenzione a richieste di informazioni non necessarie****: Se viene chiesta una quantità eccessiva di dettagli o informazioni che non sembrano pertinenti, è possibile che sia un tentativo di ottenere dati sensibili in maniera subdola.

4. ****Sicurezza Informatica e Controllo degli Accessi****

Adottare misure di sicurezza informatica per limitare il rischio di accesso non autorizzato ai dati e ai sistemi.

- ****Limitare i privilegi di accesso****: Ridurre l'accesso alle informazioni critiche ai soli individui che ne hanno bisogno per il proprio ruolo. I profili con privilegi amministrativi dovrebbero essere usati solo quando strettamente necessario.
- ****Aggiornamento e sicurezza del software****: Assicurarsi che tutti i software, specialmente quelli che gestiscono la sicurezza (antivirus, firewall), siano aggiornati. Un software obsoleto può essere sfruttato come “cavallo di Troia” se un attaccante riesce a manipolare una vittima per installare un malware.
- ****Protezione fisica dei dispositivi****: Stabilire regole per bloccare i computer quando ci si allontana e per proteggere i dispositivi mobili con password sicure. L'accesso fisico a dispositivi non protetti può permettere a un attaccante di rubare dati o installare malware.

5. ****Protezione Contro il Phishing e Simili****

Gli attacchi di phishing sono una delle forme più comuni di Social Engineering e richiedono misure specifiche.

- ****Utilizzo di filtri anti-phishing****: Installare e mantenere attivi filtri anti-phishing nella posta elettronica per rilevare email sospette.
- ****Controllare attentamente i link e gli allegati****: Evitare di cliccare su link sconosciuti o aprire allegati non richiesti. Passare il cursore sopra i link per vedere dove portano realmente, verificando che corrispondano a indirizzi ufficiali.
- ****Segnalazione delle email sospette****: Se si riceve un'email sospetta, segnalarla immediatamente al team IT o al personale di sicurezza. Non eliminare l'email, poiché può essere utile per proteggere altri dipendenti.

6. ****Protezione Contro Attacchi Fisici e Accessi Non Autorizzati****

Il Social Engineering si estende anche all'accesso fisico ai luoghi e dispositivi.

- ****Implementare badge e autenticazione fisica****: Assicurarsi che l'accesso agli edifici aziendali sia controllato da badge di sicurezza e che i visitatori siano sempre accompagnati.
- ****Politiche contro il tailgating****: Educare i dipendenti a non permettere a sconosciuti di entrare senza autorizzazione. Usare tornelli o porte di sicurezza per evitare che qualcuno possa seguire un dipendente all'interno di un edificio senza autorizzazione.

- ****Distruzione sicura dei dati****: Distruggere adeguatamente tutti i documenti riservati (utilizzando ad esempio trita-documenti) e disporre di un sistema di gestione sicura dei rifiuti per evitare il dumpster diving.

7. ****Gestione delle Password e delle Credenziali****

L'uso appropriato delle password è una delle difese principali contro molti tipi di attacco.

- ****Password forti e uniche****: Assicurarsi che le password siano complesse e diverse per ogni account. Utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli.
- ****Gestione delle password****: Usare un password manager per memorizzare in sicurezza le password e per facilitare la creazione di password uniche per ogni servizio.
- ****Non condividere mai le password****: Evitare di condividere le credenziali via email o telefonicamente. In caso di necessità, usare metodi di condivisione sicura.

8. ****Segnalazione e Registrazione di Attività Sospette****

La documentazione di attività sospette è essenziale per la sicurezza.

- ****Tracciamento delle attività****: Implementare sistemi di log per monitorare chi accede ai dati e quando. Le attività di accesso sospette devono essere registrate e analizzate.
- ****Processo di segnalazione immediata****: Stabilire una politica di segnalazione rapida per tutti i dipendenti, con la possibilità di riportare qualsiasi attività sospetta a un team di sicurezza dedicato.
- ****Audit regolari****: Condurre audit e controlli periodici sulle pratiche di sicurezza per identificare eventuali lacune o rischi.

9. ****Sensibilizzazione Sull'Uso dei Social Media****

Gli attaccanti possono raccogliere molte informazioni sui social media, quindi è necessario educare i dipendenti all'uso consapevole di queste piattaforme.

- ****Limitare le informazioni personali condivise online****: Evitare di pubblicare dettagli specifici sul lavoro, come il titolo esatto, le tecnologie usate o i nomi dei colleghi. Queste informazioni possono essere usate per rendere più credibili gli attacchi.
- ****Rivedere le impostazioni di privacy****: Assicurarsi che solo le persone autorizzate abbiano accesso alle informazioni personali sui social media.
- ****Politiche aziendali sui social media****: Stabilire regole chiare su cosa è appropriato pubblicare riguardo all'azienda e alle proprie attività professionali.

10. ****Cultura della Sicurezza e Continuità della Formazione****

Infine, creare una cultura della sicurezza solida è uno degli strumenti più potenti per combattere il Social Engineering.

- ****Promuovere una mentalità di vigilanza****: Fare in modo che ogni dipendente sia parte attiva della sicurezza aziendale, rendendolo consapevole dei rischi di Social Engineering e promuovendo una comunicazione aperta su eventuali incidenti.
 - ****Aggiornamento continuo delle procedure****: Mantenere aggiornate le politiche di sicurezza e adattare ai nuovi tipi di attacco che emergono con l'evoluzione delle tecniche di Social Engineering.
 - ****Premiare la segnalazione proattiva****: Creare un ambiente in cui segnalare potenziali problemi di sicurezza sia visto come un comportamento positivo e premiato.
- Con l'adozione di queste pratiche, individui e aziende possono migliorare significativamente la loro resistenza agli attacchi di Social Engineering, riducendo le possibilità di successo degli aggressori e rafforzando la sicurezza complessiva dei sistemi.
- Come si può notare con 2 semplici Prompt ChatGPT è stato decisamente dettagliato e in pochissimo tempo ci ha fornito una quantità di informazioni spropositata.
- È importantissimo saper richiedere le informazioni a chat nella giusta maniera.