

Creare un prompt per ChatGPT in cui si chiede cos'è il social engineering e quali tipi di attacchi utilizza

Il prompt utilizzato per ChatGPT è stato il seguente:

spiegami in parole semplici cos'è il social engineering e quali tecniche di attacco utilizza

Di seguito la risposta che ha fornito:

Il social engineering è un insieme di tecniche che i malintenzionati usano per manipolare psicologicamente le persone e convincerle a fornire informazioni sensibili o a compiere azioni che compromettono la sicurezza. In parole semplici, è un modo per "ingannare" le persone affinché rivelino dati riservati come password, dettagli bancari o altre informazioni personali.

Come funziona?

Il social engineering sfrutta la fiducia, l'ignoranza, la paura o l'urgenza delle vittime per indurle a fare qualcosa che altrimenti non farebbero. Spesso si basa più sulla psicologia umana che sulle competenze tecniche.

Tecniche comuni di attacco:

Phishing: Email o messaggi falsi che sembrano provenire da una fonte affidabile, come una banca o un'azienda, e chiedono di cliccare su un link o inserire dati personali.

Spear Phishing: Una versione più mirata del phishing, in cui l'attaccante si rivolge a una persona specifica con informazioni personalizzate, rendendo l'inganno più credibile.

Vishing (Voice Phishing): Simile al phishing ma attraverso chiamate vocali. Gli attaccanti fingono di essere operatori bancari o tecnici di supporto per ottenere informazioni riservate.

Pretexting: L'attaccante si inventa una storia o un ruolo falso per convincere la vittima a rivelare informazioni. Ad esempio, potrebbe fingersi un addetto IT che deve verificare l'accesso al sistema.

Baiting: Offrire un'esca, come un dispositivo USB infetto lasciato in un luogo pubblico, sperando che qualcuno lo raccolga e lo inserisca nel proprio computer, compromettendolo.

Tailgating (o Piggybacking): L'attaccante si introduce fisicamente in un luogo protetto seguendo qualcuno autorizzato. Ad esempio, entra in un edificio dicendo di aver dimenticato il badge.

Quid Pro Quo: Promettere un vantaggio o un premio in cambio di informazioni personali o dell'accesso a risorse aziendali.

Perché funziona?

Funziona perché fa leva sulle emozioni umane, come l'altruismo, la curiosità o il timore di subire conseguenze negative. Le persone tendono a fidarsi o ad agire velocemente sotto pressione, e gli attaccanti sfruttano proprio questi comportamenti per ottenere ciò che vogliono.

Capire il social engineering è importante per proteggersi. È essenziale mantenere un atteggiamento critico, diffidare di richieste non richieste e verificare sempre l'identità delle persone con cui si comunica, specialmente quando si tratta di informazioni riservate.

Il prompt utilizzato per la seconda richiesta dell' esercizio è stato il seguente:

come posso difendermi da questa tipologia di attacchi?

Questa la risposta di ChatGPT con le best practice da seguire:

Difendersi dagli attacchi di social engineering richiede una combinazione di buone pratiche, consapevolezza e un approccio prudente alla condivisione di informazioni. Ecco alcune misure chiave per proteggerti:

1. Diffida delle comunicazioni non richieste

Se ricevi email, messaggi o chiamate da sconosciuti o da fonti sospette che ti chiedono di fornire informazioni personali o cliccare su link, verifica sempre l'autenticità prima di rispondere. Contatta direttamente l'azienda o la persona che ti avrebbe contattato usando numeri di telefono o email ufficiali (non quelli forniti nel messaggio ricevuto).

2. Non cliccare su link sospetti

Evita di cliccare su link o scaricare allegati in email o messaggi non richiesti, anche se sembrano provenire da una fonte affidabile.

Passa il cursore sui link (senza cliccare) per vedere l'URL reale e verificare che sia legittimo.

3. Proteggi le tue informazioni personali

Limita la quantità di informazioni personali condivise sui social media. Gli attaccanti possono usare questi dati per rendere le truffe più credibili (ad esempio, conoscendo il tuo datore di lavoro o i tuoi amici).

Non rivelare mai dati sensibili come password, PIN o numeri di conto tramite telefono o email.

4. Usa password forti e univoche

Utilizza password complesse e diverse per ciascun account, e cambia regolarmente le password.

Considera l'uso di un password manager per generare e memorizzare password sicure.

5. Abilita l'autenticazione a due fattori (2FA)

Attiva la 2FA sui tuoi account quando possibile. Questo richiede un ulteriore passaggio di verifica per accedere, rendendo più difficile per un attaccante accedere al tuo account anche se ha la tua password.

6. Formazione e consapevolezza

Se lavori in un'azienda, partecipa a programmi di formazione sulla sicurezza informatica per imparare a riconoscere i segnali di attacchi di social engineering.

Mantieniti informato sulle nuove tecniche di attacco e sulle tendenze del social engineering.

7. Verifica sempre l'identità

Se qualcuno ti contatta affermando di essere un rappresentante di un'azienda o un dipartimento IT, chiedi prove della sua identità. Le aziende rispettabili non chiederanno mai dettagli sensibili senza adeguate verifiche.

Evita di lasciarti influenzare da pressioni di urgenza: gli attaccanti spesso cercano di far agire le persone velocemente, usando minacce o promesse allettanti.

8. Protezione dei dispositivi

Assicurati che il tuo software antivirus e il sistema operativo siano sempre aggiornati per proteggerti da malware e altre minacce.

Non collegare dispositivi USB sconosciuti al computer, poiché potrebbero essere infettati con malware.

9. Controlla la fonte delle richieste

Verifica le richieste insolite o inaspettate con un collega o un amico di fiducia. Anche se un messaggio sembra provenire da un contatto noto, potrebbe essere stato inviato da un attaccante che ha compromesso l'account.

10. Segnala tentativi di phishing

Se ricevi tentativi di phishing o sospetti di essere vittima di un attacco di social engineering, segnalalo al dipartimento IT della tua azienda o al provider di servizi interessato. Questo aiuta a prevenire attacchi futuri.

Adottando queste pratiche, puoi ridurre significativamente il rischio di cadere vittima degli attacchi di social engineering e proteggere le tue informazioni personali e aziendali.