PRATICA 31 OTTOBRE 2024

Prompt per ChatGPT  
  
Obiettivo: Dovrete scrivere un prompt per ChatGPT che vi permetta di ottenere informazioni dettagliate sulle tecniche di social engineering. Analizzate gli esempi forniti e sviluppate una serie di raccomandazioni per prevenire tali attacchi. Infine, create una presentazione o un documento che riassuma le vostre scoperte e raccomandazioni.

Domanda 1

Scrivendo a ChatGPT di spiegarci cos’è il social engineering come se fosse un docente che spiega la lezione, ci ha risposto così:  
  
“Il *social engineering* è una tecnica di manipolazione psicologica che mira a ottenere informazioni o accesso a risorse riservate, senza l’uso diretto di strumenti tecnologici o software sofisticati. In pratica, chi utilizza il social engineering cerca di convincere una persona a fare qualcosa, a rivelare informazioni private o a comportarsi in modo rischioso, sfruttando la fiducia, la curiosità o la mancanza di attenzione.

Immagina questo scenario: un impostore chiama un dipendente di un’azienda fingendosi un collega del reparto IT. Con tono amichevole, spiega che sta risolvendo un problema urgente e ha bisogno della password del dipendente per “risolvere il problema al più presto”. Se il dipendente non sospetta nulla, può rivelare la password, permettendo all’impostore di accedere a informazioni riservate o di fare danni.

Ecco alcuni esempi comuni di social engineering:

1. **Phishing**: Quando si ricevono e-mail o messaggi che sembrano provenire da fonti affidabili (come banche o colleghi) ma in realtà sono trappole per ottenere informazioni personali.
2. **Vishing** (voice phishing): Quando il malintenzionato chiama direttamente la vittima per estorcere informazioni sensibili, come nel caso dell’impostore che finge di essere del reparto IT.
3. **Pretexting**: In cui il malintenzionato inventa una storia (o *pretesto*) per convincere la vittima a rivelare dati riservati.
4. **Tailgating o piggybacking**: In cui il malintenzionato si infiltra fisicamente in una zona riservata, magari chiedendo a una persona di tenergli aperta la porta fingendo di aver dimenticato il badge.

In sintesi, il social engineering sfrutta i punti deboli delle persone per ottenere ciò che un attacco informatico diretto a volte non riesce a fare.”

Domanda 2

Chiedendo a ChatGPT di spiegarci come ci si difende efficacemente dagli attacchi di social engineering, ci viene data questa risposta:

“Difendersi dagli attacchi di social engineering richiede principalmente consapevolezza e attenzione, perché si tratta di attacchi che mirano a manipolare le persone e non solo a sfruttare le vulnerabilità tecniche. Ecco alcune strategie efficaci per proteggersi:

**1. Formazione e Consapevolezza**

La prima difesa è educare le persone sui rischi e sui metodi di social engineering. Conoscere le tecniche più comuni, come phishing, vishing o pretexting, permette di riconoscere situazioni sospette e reagire di conseguenza.

**2. Verifica delle Informazioni**

Prima di fornire informazioni sensibili, è importante verificare l'identità di chi le richiede:

* Se ricevi una chiamata o un’e-mail da un contatto che ti sembra sospetto, verifica la richiesta attraverso canali ufficiali.
* Non cliccare link o non aprire allegati da fonti non verificate, anche se sembrano provenire da persone fidate.

**3. Politiche di Sicurezza Aziendale**

Le aziende dovrebbero stabilire regole chiare per la gestione di informazioni sensibili, come:

* Non condividere mai password o altre credenziali tramite e-mail o al telefono.
* Utilizzare metodi di autenticazione a più fattori (MFA) per rendere più difficile l’accesso ai dati, anche se qualcuno dovesse ottenere una password.
* Limitare l’accesso fisico e digitale ai soli dipendenti autorizzati e controllare che l’accesso sia legato alle effettive necessità lavorative.

**4. Uso di Password Sicure e Autenticazione a Più Fattori (MFA)**

Le password devono essere robuste e cambiate periodicamente, evitando di usare la stessa password su più servizi. L’autenticazione a due fattori (ad esempio, un codice inviato al telefono oltre alla password) rende più difficile l’accesso per i malintenzionati.

**5. Segnalazione di Attività Sospette**

Chiunque noti comportamenti sospetti o richieste insolite deve segnalarlo subito al reparto IT o al proprio superiore. Una buona cultura aziendale dovrebbe incentivare la segnalazione rapida senza paura di ritorsioni.

**6. Fiducia Limitata e Controlli di Accesso Fisico**

Nei luoghi di lavoro, chiudere sempre a chiave stanze o uffici con accesso riservato e non permettere l’accesso a sconosciuti o a persone senza badge identificativo. Bisogna stare attenti anche a richieste di favori banali, come “tenere aperta una porta” o “passare un badge per un collega”.

**7. Simulazioni di Attacchi**

Molte aziende organizzano simulazioni di attacchi di social engineering (come tentativi di phishing) per verificare il livello di attenzione dei dipendenti e insegnare a identificare e gestire situazioni di rischio.

In definitiva, proteggersi dagli attacchi di social engineering significa sviluppare un atteggiamento critico e dubitare delle richieste inconsuete, ricordando che chi intende manipolare spesso cerca di sfruttare la nostra fiducia o le nostre emozioni.”

BONUS

Chiedendo a ChatGPT di riportarci delle vulnerabilità su Windows Vista, ecco il risultato:  
  
  
“Ecco una lista di alcune delle principali vulnerabilità di Windows Vista con dettagli e soluzioni consigliate:

1. **CVE-2016-7255**: Questa vulnerabilità sfrutta un'escalation dei privilegi attraverso il kernel di Windows. Gli attaccanti possono ottenere privilegi elevati sul sistema tramite exploit specifici. Microsoft ha rilasciato aggiornamenti di sicurezza per risolvere questo problema, e si consiglia di aggiornare Windows Vista all'ultima versione disponibile e attivare firewall e antivirus​

[NVD](https://nvd.nist.gov/vuln/detail/CVE-2016-7255)

.

1. **CVE-2015-2474** (SMB Memory Corruption): Questa vulnerabilità consente a un utente malintenzionato con credenziali valide di eseguire codice remoto tramite una corruzione della memoria nella gestione dei log di SMB. Disabilitare il protocollo SMBv1 può prevenire l'exploit di questa vulnerabilità. Microsoft ha rilasciato aggiornamenti per correggere il problema; applicare l'aggiornamento KB3073921 su Vista è raccomandato per la protezione​

[Microsoft Learn](https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-063)

​

[Microsoft Learn](https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-083)

.

1. **MS09-063** (WSDAPI Remote Code Execution): Un'altra vulnerabilità critica di esecuzione di codice remoto legata all'API WSD, che permette a un attaccante di prendere il controllo del sistema tramite un messaggio WSD opportunamente formattato. Questo problema può essere mitigato assicurandosi che il firewall blocchi le porte TCP 5357 e 5358 o evitando l'uso dell'API WSD​

[Microsoft Learn](https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-063)

.

In generale, il supporto per Windows Vista è terminato, quindi non riceverà più aggiornamenti di sicurezza da Microsoft. È consigliabile aggiornare a un sistema operativo supportato per migliorare la protezione e ridurre i rischi di exploit legati a queste e altre vulnerabilità non risolvibili.

“