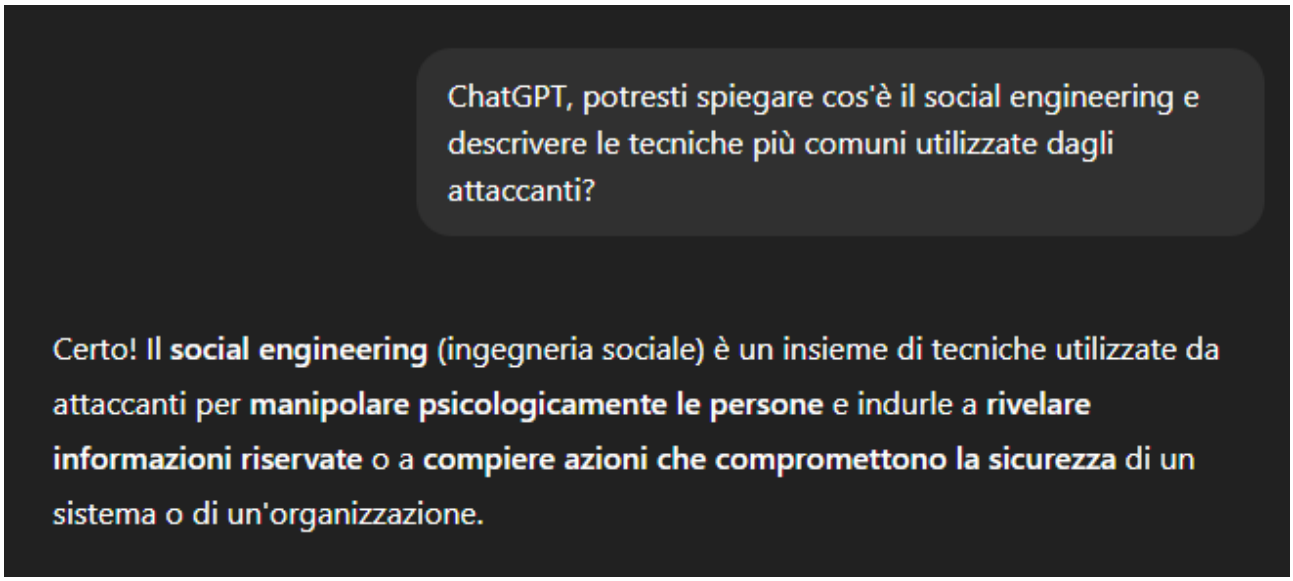
Social engineering e tecniche di difesa

L’esercizio richiede l’utilizzo di ChatGPT come strumento di informazione riguardo il social engineering e le tecniche per difendersi da esso.

Iniziamo inserendo il prompt:



In risposta ci viene spiegato che il social engineering è una tecnica usata dagli attaccanti per manipolare le persone e indurle a rivelare informazioni riservate o compiere azioni che compromettono la sicurezza.

Le tecniche più usate sono:

- Phishing
  Inviare mail o messaggi che sembrano autentici con lo scopo di rubare credenziali o installare malware

- Spear Phishing
  Variante mirata del phishing. L’attaccante personalizza il messaggio per un individuo o un’azienda specifica, per esempio una mail inviata a un reparto contabilità con dettagli reali dell’azienda

- Vishing
  Truffa via telefono, l’attaccante si finge un operatore di banca, un tecnico IT per ottenere dei dati importanti

- Smishing (SMS Phishing)
  Messaggi di testo fraudolenti che contengono link pericolosi o istruzioni ingannevoli.

- Pretexting
  L’attaccante crea un falso pretesto per ottenere informazioni, spesso impersonando una figura autorevole o conosciuta.

- Baiting
  Offerta di un'esca fisica o digitale per indurre la vittima a compiere un’azione.

- Tailgating (o Piggybacking)
  L’attaccante si introduce fisicamente in un'area protetta seguendo una persona autorizzata.

I metodi per difendersi da questo tipo di “attacco” sono:

- Formazione continua sul riconoscimento delle minacce.
  Anche l’utilizzo di software che simulano il phishing

- Diffidare da richieste urgenti o non previste.
  Fornire l’accesso alle informazioni solo a chi ne ha realmente bisogno

- Non condividere credenziali o dati personali, soprattutto via email o telefono.

  Stabilire con delle regole cosa può essere condiviso e cosa no.

- Verificare sempre l'identità di chi richiede informazioni riservate.
  Se qualcuno richiede informazioni sensibili, verifica la sua identità tramite un secondo canale ufficiale

- Usare l’autenticazione a due fattori (2FA) ove possibile.

- Controlli fisici
  Proteggere l’accesso fisico ai locali (es. badge, sorveglianza).
  Istruire il personale a non far entrare sconosciuti senza autorizzazione (contro il tailgating).

CVE Windows 11

CVE-2025-21418 – WinSock Ancillary Function Driver: Escalation di privilegi

- Tipo di vulnerabilità: Privilege escalation che consente a un attaccante di ottenere privilegi SYSTEM da un contesto utente.
- Impatto: accesso completo al sistema, possibile compromissione totale.
- Stato: già sfruttata come zero-day in ambiente reale. Fortemente raccomandata la patch rapida.
- Soluzione: installare l'aggiornamento Microsoft di febbraio 2025. Negli Stati Uniti è stata inserita nel catalogo CISA KEV con scadenza di patch per l'4 marzo 2025.

CVE-2025-21391 – Storage Privilege Escalation

- Tipo di vulnerabilità: escalation di privilegi tramite componente Windows Storage.
- Impatto: potenziale distruzione o cancellazione di file critici con impatto sui servizi.
- Stato: anch'essa attivamente sfruttata e inserita in KEV.
- Soluzione: applicazione urgente degli update di febbraio 2025.

CVE-2025-24983 – Kernel Use-After-Free in Win32 subsystem

- Tipo: escalation privilegi attraverso una race condition kernel.
- Impatto: attacco senza interazione utente, sfruttabile da codice locale.
- Stato: sfruttata in ambienti reali dal marzo 2023 fino alla patch di marzo 2025.
- Soluzione: patch dal Patch Tuesday di marzo 2025; è considerata «Important» da Microsoft.

CVE-2024-38147 – DWM Core Library Elevation of Privilege

- Livello: CVSS ~7.0 – elevazione privilegi possibile tramite Windows Desktop Manager.
- Soluzione: aggiornamenti disponibili per le build 21H2, 22H2, 23H2 e 24H2 (es. KB5041592, KB5041585, KB5041571) .

CVE-2024-21351 – Security Feature Bypass (versione 23H2)

- Tipo: bypass di funzioni di protezione interne, possibile esecuzione arbitraria.
- Soluzione: aggiornamento Microsoft disponibile. Utenti di Windows 11 23H2 devono installarlo tempestivamente.

Tabella riepilogativa:

CVE	Tipo	Versione interessata	Impatto	Soluzione
2025-21418	*Privilege escalation*	WinSock (multi-versione)	SYSTEM access, zero-day	Patch feb 2025 (KB update)
2025-21391	*Storage escalation*	Windows Storage	Cancellazione file critici	Patch feb 2025
2025-24983	*Kernel use-after-free*	Win32 subsystem	Privilegi SYSTEM, exploit locale	Patch mar 2025
2024-38147	*Elevation privilege*	21H2–24H2	Escalation locale	Patch KB5041xxx series
2024-21351	*Security bypass*	23H2	Arbitrary code / bypass	Patch disponibile
2024-21346	*Privilege escalation*	21H2	Escalation da utente	Patch disponibile
2023-35635	*Denial of Service (DoS)*	22H2	Crash o rallentamenti	Patch disponibile
2023-35631	*Privilege escalation*	21H2	Elevazione locale	Patch disponibile

Raccomandazioni generali

Mantieni attivo Windows Update automatico, o esegui patch manuali regolarmente.

Monitora le build attualmente in uso (es. 21H2, 22H2, 23H2, 24H2) e allinea le patch specifiche.

Priorità alta agli aggiornamenti che risolvono zero-day o vulnerabilità attivamente sfruttate (come CVE-2025-21418, CVE-2025-21391, CVE-2025-24983).

Usa strumenti di gestione patch centralizzata (SCCM, WSUS, Intune...) per organizzazioni.

Verifica la corretta installazione delle patch su sistemi endpoint mediante log, Qualys o simili.