

Esercizio UNIT2 S5/L4

OBIETTIVO:

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 riassume le vostre scoperte e raccomandazioni.

“Formulate un prompt per ChatGPT per ottenere una panoramica del social engineering e delle tecniche utilizzate dagli attaccanti.”

ESERCIZIO:

Per lo svolgimento del seguente esercizio ho provato a sperimentare con chat gpt utilizzando uno stesso prompt come richiesta ma su due chat impostate in maniera differente.

La prima chat è stata creata da zero, senza impostazioni aggiunte.

La seconda chat invece ha avuto come prompt iniziale un prompt predefinito che limitasse la simulazione di “emozioni” da parte di chatgpt, l’uso di emoji, risposte che finivano con una domanda finale per allungare la conversazione e altri fattori, per renderla più “asettica” possibile.

il prompt di richiesta è stato il seguente:

“Sto facendo un corso di cyberSecurity e voglio sapere in modo dettagliato una lista di esempi di social engineering che si possono subire e dei metodi di difesa efficaci contro questi ultimi”

differenze:

le prime differenze visibili a occhio nudo sono l’impostazione della risposta per la prima chat, in cui si parla con un tono confidenziale, ci sono differenze di font, e poi vengono descritti

- un esempio di social engineering, la definizione, i segnali e le difese.
- una lista di misure difensive generali (con politiche, formazione, awareness)
- una check list rapida su cosa non dovrebbe fare un target host
- una check list rapida su cosa dovrebbe fare un’organizzazione come difesa
- come difendersi da social engineering Vishing
- e poi cerca di allungare la conversazione proponendo di dover fare un pdf

6) Baiting (esca fisica o digitale)

Cos'è / Scenario: lasciare una chiavetta USB infetta in area comune; qualcuno la inserisce nel PC. Oppure download "gratuito" che contiene malware.

Segnali: dispositivi trovati casualmente, software da fonti non ufficiali.

Difese tecniche: disabilitare autorun, endpoint protection/EDR, controllo device USB (whitelisting), policy "non inserire dispositivi trovati".

Difese comportamentali: training, cartelli e reminder nelle aree comuni.

7) Quid pro quo

Cos'è / Scenario: attaccante offre assistenza tecnica o un servizio in cambio di informazioni (es. "sono dell'helpdesk, dimmi la tua password per aggiornare").

Segnali: offerta di aiuto inaspettata, richiesta di credenziali.

Difese: policy helpdesk (mai chiedere password), procedure di verifica dell'identità, supporto IT che richiede un ticket o verifica out-of-band.

8) Pretexting / Impersonation

Cos'è / Scenario: attaccante crea una falsa identità (fornitore, ispettore, nuovo collega) per ottenere accesso o informazioni.

Segnali: richieste di informazioni non necessarie, persona nuova senza presentazione ufficiale.

Difese: procedure di check-in per visitatori, badge visibili, verifica identità del fornitore con contatti ufficiali, "least privilege" per accessi temporanei.

Esempio di script "out-of-band"/verifica telefonica (puoi includerlo nella policy)

Ricevuta richiesta di pagamento via email dal CFO per €X:

1. "Non eseguire il pagamento."
2. "Chiama il numero ufficiale del CFO registrato nel sistema (non rispondere al numero fornito nell'email)."
3. "Domande di verifica: "Confermi l'IBAN X per la fattura Y e l'importo €X?" — prendi nota della risposta e registra la chiamata se policy lo consente."
4. "Se la persona non risponde sul numero ufficiale o il tono sembra sospetto, escalare al Security Incident Response."

Rilevamento e segnalazione — cosa raccogliere quando segnali un attacco

- Header completi dell'email (From, Received, Message-ID).
- Screenshot del messaggio e del mittente.
- URL sospetti (non cliccarli; copia l'URL come testo).
- Numero chiamante e orario della chiamata.
- Persona coinvolta, eventuali azioni eseguite (ha inserito credenziali? fatto pagamenti?).

Questi elementi velocizzano l'analisi forense.

mentre per la seconda chat:

- la lista è semplificata e più breve della precedente, il responso è più diretto e manca di font differenti.
- La parte finale da dei consigli su misure generali da applicare come difesa a questi problemi e soprattutto manca di richieste sul continuare la conversazione.

Elenco dettagliato di tecniche di social engineering e contromisure efficaci.

1. Phishing via email

- Esempi: email che simulano banche, provider, colleghi o servizi cloud; link a pagine fake per furto credenziali; allegati malevoli (macro, eseguibili nascosti).
- Difese: filtro antiphishing e antispam con analisi URL e sandboxing allegati; autenticazione a due fattori (MFA) obbligatoria; formazione obbligatoria su riconoscimento indicatori (mittente non corrispondente, URL visual vs reale, errori grammaticali); policy che vieta inserimento credenziali dopo click; isolamento di browser per link esterni; disabilitare macro per default; procedure di segnalazione immediata.

2. Spear phishing (targeted phishing)

- Esempi: messaggi personalizzati che citano informazioni reali (nome di progetti, nomi di colleghi) per ottenere trasferimenti di denaro, credenziali o esecuzione di azioni.
- Difese: addestramento avanzato sul riconoscimento di richieste insolite; verifica out-of-band obbligatoria per richieste finanziarie/operazioni critiche (telefono ufficiale, canale verificato); limitare esposizione di informazioni sensibili sui social/profili pubblici; DMARC/DKIM/SPF configurati per dominio.

3. Vishing (voice phishing)

- Esempi: chiamate che si spacciano per IT, banca o fornitore che chiedono password, codici OTP o di installare software remoto.
- Difese: policy che vieta comunicazione di credenziali via telefono; procedura di verifica dell'identità del chiamante (callback su numero ufficiale); formazione specifica: non rivelare OTP o password; uso di canali autenticati per richieste sensibili.

4. Smishing (SMS phishing)

- Esempi: SMS con link a pagine di login false o codice per attivare servizi; link che installano malware mobile.
- Difese: educazione su non cliccare link da numeri sconosciuti; blocco e analisi URL SMS su gateway

Indicatori pratici di possibile attacco sociale da monitorare:

- Email con urgenza ingiustificata, minacce o ricompense.
- Mittente con piccolo cambiamento ortografico nel dominio.
- Richieste non consone al ruolo del richiedente (es. cambio IBAN via email).
- Link che mostrano testo legittimo ma puntano a domini diversi.
- Allegati eseguibili o documenti con macro.
- Richieste out-of-band negate da canali ufficiali.

Azioni immediate post-incidente da imporre:

- Isolare account/endpoint compromessi.
- Resettare credenziali e revocare sessioni attive; forzare MFA reset se necessario.
- Avviare analisi forense log e endpoint per determinare impatto.
- Informare team finance/legale/management secondo playbook.
- Notifica agli utenti e avvio di campagne di mitigazione (scansione password compromesse, forced logout).

Non applicare queste difese è equivalente a lasciare la porta aperta: implementare le misure tecniche + procedure organizzative + formazione obbligatoria, monitorare e testare regolarmente.

risponso prima chat:

Ecco una guida dettagliata — esempi concreti di social engineering e contromisure efficaci

Ottimo argomento per un corso di cybersecurity. Ti do una lista ampia e pratica: per ogni attacco trovi **che cos'è / uno scenario tipico / segnali di allarme e contromisure tecniche e comportamentali** (per singolo utente e per l'organizzazione). Alla fine ti do anche una checklist rapida e uno script di verifica telefonica che puoi usare come policy.

1) Phishing via email

Cos'è / Scenario: email che sembra provenire da servizi legittimi (banche, provider cloud, HR) che invita a cliccare link o inserire credenziali.

Segnali: URL sospetto (non corrisponde al dominio), errori grammaticali, richieste urgenti, allegati eseguibili.

Difese tecniche: filtro antispam/ATP, controllo SPF/DKIM/DMARC, sandboxing allegati, URL rewriting/scan, proxying dei link.

Difese comportamentali: formazione anti-phishing, sospettare richieste urgenti per

informazioni sensibili, usare password manager (compila solo su domini veri), segnalare mail sospette.

2) Spear phishing (targeted)

Cos'è / Scenario: email altamente personalizzata diretta a una persona specifica (es. CFO) usando informazioni raccolte sui social.

Segnali: conoscenza di dettagli personali o aziendali, mittente che sembra un collega/fornitore.

Difese: addestramento specifico per ruoli a rischio (finance, HR, IT), regole di verifica per trasferimenti di denaro, policy "out-of-band" (conferma via telefono su numero noto), MFA obbligatorio.

3) Whaling

Cos'è / Scenario: forma di spear phishing rivolta ai top executive con richieste finanziarie o legali.

Segnali: messaggi che simulano CEO/avvocati/banche, tono autoritario.

Difese: privilegi limitati, approvazioni multiple su pagamenti, awareness per executive, simulazioni di attacco personalizzate.

4) Vishing (voice phishing)

Cos'è / Scenario: chiamate che fingono banche, IT o enti per ottenere password/OTP o trasferimenti.

Segnali: pressione per condividere OTP o password, numero anonimo o mascherato, richieste di eseguire azioni immediatamente.

Difese: policy "mai comunicare password o OTP al telefono", verifica out-of-band chiamando un numero ufficiale, registrazione/monitoring delle chiamate, formazione con role-play.

5) Smishing (SMS phishing)

Cos'è / Scenario: SMS contenenti link malevoli o codici che invitano a inserire dati.

Segnali: link corto, mittente sconosciuto, messaggio che richiede azione urgente.

Difese: blocco/smartfiltering SMS per account aziendali, educazione utenti a non cliccare link da numeri sconosciuti, MFA non basata solo su SMS (usare app autenticatore o chiavi hardware).

6) Baiting (esca fisica o digitale)

Cos'è / Scenario: lasciare una chiavetta USB infetta in area comune; qualcuno la inserisce nel PC. Oppure download "gratuito" che contiene malware.

Segnali: dispositivi trovati casualmente, software da fonti non ufficiali.

Difese tecniche: disabilitare autorun, endpoint protection/EDR, controllo device USB (whitelisting), policy "non inserire dispositivi trovati".

Difese comportamentali: training, cartelli e reminder nelle aree comuni.

7) Quid pro quo

Cos'è / Scenario: attaccante offre assistenza tecnica o un servizio in cambio di informazioni (es. "sono dell'helpdesk, dimmi la tua password per aggiornare").

Segnali: offerta di aiuto inaspettata, richiesta di credenziali.

Difese: policy helpdesk (mai chiedere password), procedure di verifica dell'identità, supporto IT che richiede un ticket o verifica out-of-band.

8) Pretexting / Impersonation

Cos'è / Scenario: attaccante crea una falsa identità (fornitore, ispettore, nuovo collega) per ottenere accesso o informazioni.

Segnali: richieste di informazioni non necessarie, persona nuova senza presentazione ufficiale.

Difese: procedure di check-in per visitatori, badge visibili, verifica identità del fornitore con contatti ufficiali, "least privilege" per accessi temporanei.

9) Tailgating / Piggybacking (accesso fisico)

Cos'è / Scenario: una persona segue un dipendente attraverso una porta a badge fingendo di essere autorizzata.

Segnali: qualcuno che non usa badge o appare nervoso, persone con imballaggi grandi che "dimenticano" il badge.

Difese: policy "non tenere la porta aperta per sconosciuti", tornelli/porte mantrap, badge obbligatori, guardie di sicurezza, telecamere, formazione sul rifiuto cortese.

10) Dumpster diving (raccolta rifiuti)

Cos'è / Scenario: estrazione di documenti confidenziali dalla spazzatura.

Segnali: informazioni sensibili buttate senza taglio.

Difese: distruggidocumenti (shredder) per carta, cancellazione sicura per dispositivi e hard disk, policy per smaltimento sicuro.

11) Watering hole

Cos'è / Scenario: compromissione di siti web frequentati da un gruppo target (es. portale industriale) per infettare visitatori.

Segnali: siti legittimi che iniziano a comportarsi in modo strano, avvisi di sicurezza del browser.

Difese tecniche: network monitoring, aggiornare browser/plugin, EDR, filtraggio web, threat intelligence, segmentazione della rete.

12) Social media reconnaissance / oversharing

Cos'è / Scenario: informazioni personali/post che permettono attacchi mirati (date vacanza, nomi familiari, ruolo aziendale).

Segnali: post pubblici con dettagli su viaggi, ruoli o procedure aziendali.

Difese: policy uso social (guidelines su cosa NON pubblicare), training su privacy, scansione di leakage dei dati, ridurre informazioni pubbliche aziendali.

13) Deepfake voice/video

Cos'è / Scenario: audio o video contraffatti usati per ordinare pagamenti o convincere qualcuno (es. "è il CEO, paga questa fattura").

Segnali: timbro vocale strano, richieste inconsuete, assenza di canali verificabili.

Difese: policy obbligatoria per conferme multiple su pagamenti, procedure out-of-band (incontro/numero ufficiale), formazione su segnali di deepfake, strumenti di rilevamento e analisi forense.

14) Account takeover (ATO) via helpdesk / reset

Cos'è / Scenario: attaccante ottiene reset password dal supporto fingendo di essere il legittimo utente.

Segnali: reset richiesti da IP/paesi insoliti, richieste multiple di reset.

Difese: processi di verifica identity per helpdesk, registri e alert per reset massivi, MFA, limitare privilegi e sessioni attive.

Misure difensive generali (organizzazione + utente)

Tecniche (infrastrutturali)

- **MFA forte** (preferire U2F/chiavi hardware o app autenticatore, non solo SMS).
- **SPF/DKIM/DMARC** e monitoraggio DMARC report.
- **Filtri email avanzati / ATP / sandboxing allegati.**
- **Endpoint Detection & Response (EDR)** e controllo delle applicazioni (application allowlist).
- **Network segmentation** e least-privilege per ridurre danni se compromessi.
- **Data Loss Prevention (DLP)** per prevenire esfiltrazione dati.
- **Patch management** regolare per software e plugin (browser, Office).
- **Controllo device USB** (whitelist o blocco) e disabilitare autorun.
- **Sistemi di logging e SIEM** con regole anti-phishing e analisi comportamentale.

Politiche e processi

- **Policy di conferma out-of-band** per trasferimenti di denaro e richieste sensibili.
- **Procedure helpdesk rigide** (mai resettare password senza verifica).
- **Gestione privilegi** (PAM per account elevati).
- **Incident response playbook** per phishing e ATO (linee chiare su chi contattare, isolamento, forensic).
- **Politiche BYOD e sicurezza mobile** (MDM).
- **Crittografia dei dati sensibili** at-rest e in-transit.
- **Politiche di retention e smaltimento sicuro.**

Formazione e awareness

- **Phishing simulation** regolari (anche mirati per ruoli) con feedback immediato.
 - **Training pratico e role-play** per vishing e skills di verifica.
 - **Campagne di micro-learning** (brevi pillole) su come segnalare.
 - **Test di ingegneria sociale fisica** (tailgating tests) con security team.
 - **Comunicazione chiara per la segnalazione** (come, dove, a chi segnalare mail/chiamate sospette).
-

Checklist rapida per un utente (cosa fare subito)

1. Non cliccare link sospetti; passa il mouse sul link per vedere il dominio.
 2. Non inserire credenziali su una pagina aperta da link email; vai direttamente al sito ufficiale.
 3. Non fornire password/OTP al telefono o via email.
 4. Se ricevi richiesta di pagamento urgente: verifica con una chiamata al contatto ufficiale (numero dal CRM o sito).
 5. Segnala l'email/chiamata sospetta al team di sicurezza (includi header email).
 6. Aggiorna il dispositivo e attiva MFA.
 7. Non inserire chiavette USB trovate: consegnale all'IT/security.
-

Checklist per l'organizzazione (pratico, ordine di priorità)

- Implementare MFA per tutti gli accessi sensibili.
 - Abilitare SPF/DKIM/DMARC e monitorare i report.
 - Deploy di EDR + web/email protection.
 - Policy per trasferimenti di denaro con approvazioni multiple.
 - Eseguire simulazioni di phishing trimestrali e training mirati per i ruoli critici.
 - Procedure di incident response documentate e testate.
Limitare privilegi e usare PAM per account amministrativi.
 - Politiche fisiche di accesso e controlli visitor.
-

Esempio di script “out-of-band”/verifica telefonica (puoi includerlo nella policy)

Ricevuta richiesta di pagamento via email dal CFO per €X:

1. Non eseguire il pagamento.
2. Chiama il **numero ufficiale** del CFO registrato nel sistema (non rispondere al numero fornito nell'email).
3. Domande di verifica: “Confermi l'IBAN X per la fattura Y e l'importo €X?”
— prendi nota della risposta e registra la chiamata se policy lo consente.

4. Se la persona non risponde sul numero ufficiale o il tono sembra sospetto, escalare al Security Incident Response.

Rilevamento e segnalazione — cosa raccogliere quando segnali un attacco

- Header completi dell'email (From, Received, Message-ID).
- Screenshot del messaggio e del mittente.
- URL sospetti (non cliccarli; copia l'URL come testo).
- Numero chiamante e orario della chiamata.
- Persona coinvolta, eventuali azioni eseguite (ha inserito credenziali? fatto pagamenti?).

Questi elementi velocizzano l'analisi forense.

Misure specifiche contro deepfake e AI-enabled social engineering

- Policy di verifica a più fattori per richieste sensibili.
 - Processi obbligatori "conferma fisica" per pagamenti grandi.
 - Awareness su come funzionano i deepfake; sospettare richieste vocali/video impreviste.
 - Strumenti di analisi forense per verificare incongruenze audio/video.
-

Se vuoi, posso subito trasformare questa guida in:

- una **scheda PDF stampabile** per il tuo corso, oppure
- **5 domande di quiz** a tempo (stile esame) con spiegazioni — so che preferisci quiz simulati completi a tempo, te ne preparo uno subito se vuoi.

Dimmi quale delle due opzioni preferisci e te la fornisco subito (PDF o quiz)

risponso seconda chat:

Elenco dettagliato di tecniche di social engineering e contromisure efficaci.

1. Phishing via email
 - Esempi: email che simulano banche, provider, colleghi o servizi cloud; link a pagine fake per furto credenziali; allegati malevoli (macro, eseguibili nascosti).
 - Difese: filtro antiphishing e antispam con analisi URL e sandboxing allegati; autenticazione a due fattori (MFA) obbligatoria; formazione obbligatoria su riconoscimento indicatori (mittente non corrispondente, URL visual vs reale, errori grammaticali); policy che vieta inserimento credenziali dopo click; isolamento di browser per link esterni; disabilitare macro per default; procedure di segnalazione immediata.
2. Spear phishing (targeted phishing)
 - Esempi: messaggi personalizzati che citano informazioni reali (nome di progetti, nomi di colleghi) per ottenere trasferimenti di denaro, credenziali o esecuzione di azioni.
 - Difese: addestramento avanzato sul riconoscimento di richieste insolite; verifica out-of-band obbligatoria per richieste finanziarie/operazioni critiche (telefono ufficiale, canale verificato); limitare esposizione di informazioni sensibili sui social/profil pubblici; DMARC/DKIM/SPF configurati per dominio.
3. Vishing (voice phishing)
 - Esempi: chiamate che si spacciano per IT, banca o fornitore che chiedono password, codici OTP o di installare software remoto.
 - Difese: policy che vieta comunicazione di credenziali via telefono; procedura di verifica dell'identità del chiamante (callback su numero ufficiale); formazione specifica: non rivelare OTP o password; uso di canali autenticati per richieste sensibili.
4. Smishing (SMS phishing)
 - Esempi: SMS con link a pagine di login false o codice per attivare servizi; link che installano malware mobile.
 - Difese: educazione su non cliccare link da numeri sconosciuti; blocco e analisi URL SMS su gateway aziendale; MFA su app/telefono con canali separati.
5. Pretexting (pretesto)
 - Esempi: attaccante si finge tecnico, auditor, fornitore per ottenere informazioni, accesso o cambi di configurazione.
 - Difese: procedure di verifica dell'identità dei fornitori/tecnici; ticketing obbligatorio e autorizzazioni scritte per interventi; principio di minimo privilegio; logging e revisione attività esterne.

6. Baiting (esca fisica)

- Esempi: chiavette USB infette lasciate in parcheggio/ufficio che un dipendente inserisce nella propria macchina; CD con documentazione falsa.
- Difese: divieto di inserire dispositivi sconosciuti; policy di gestione dispositivi rimovibili; blocco di autorun, endpoint protection con controllo dispositivi; campagne di sensibilizzazione.

7. Tailgating / Piggybacking (accesso fisico non autorizzato)

- Esempi: intruso segue un dipendente attraverso una porta con badge lasciata aperta; persona si spaccia per consegna.
- Difese: controllo accessi fisici (turnstiles, porte a doppio varco); policy che vieta tenere porte aperte; badge obbligatorio, controllo visitatori con registrazione e scorta; CCTV e badge reader logging; formazione per rifiutare accesso a estranei.

8. Watering hole

- Esempi: compromissione di siti web usati frequentemente da un gruppo target, inserimento di exploit per infettare i visitatori.
- Difese: aggiornamenti e hardening dei client, whitelisting applicazioni critiche, proxy e filtraggio contenuti, monitoraggio EDR per comportamento anomalo dopo visita, limitare privilegi di navigazione.

9. Quid pro quo

- Esempi: offerta di assistenza tecnica o servizi gratuiti in cambio di informazioni o accesso (telefono che offre assistenza e chiede installazione di tool).
- Difese: policy che vieta l'installazione di software non autorizzato; canali ufficiali per supporto IT; formazione su non accettare offerte "gratuità" o servizi sconosciuti.

10. Social media reconnaissance (OSINT) per attacchi successivi

- Esempi: raccolta di informazioni pubbliche (ruoli aziendali, ferie, struttura progetto) per creare spear phishing credibili.
- Difese: politiche di privacy per account aziendali; linee guida sul contenuto personale condiviso; monitoraggio OSINT per informazioni sensibili pubblicate; minimizzazione di dati esposti nei profili.

11. Business Email Compromise (BEC) / Invoice fraud

- Esempi: richiesta via email di cambio coordinate bancarie da fornitore; direttiva CEO per pagamento urgente.
- Difese: procedure finance con due firme per pagamenti rilevanti; verifica out-of-band obbligatoria per cambi conto; controllo delle modifiche di pagamento tramite portale sicuro; reconciliation e controllo anomalia.

12. Malicious QR codes

- Esempi: QR che punta a pagine di phishing o installa app malevole.
- Difese: non usare scanner non controllati; policy per l'uso dei QR aziendali; verifiche su URL prima di aprire; uso di browser sicuro e sandbox.

13. Shoulder surfing / keylogging fisico

- Esempi: osservazione diretta della digitazione di password; installazione fisica di keylogger.
- Difese: schermature fisiche (privacy filters), posture di lavoro, non scrivere password su carta in aree visibili; ispezioni fisiche workstation.

14. Impersonation on collaboration platforms

- Esempi: account Slack/Teams falsi che chiedono info sensibili o link malevoli.
- Difese: verification badge per account aziendali; canali ufficiali per richieste sensibili; MFA su piattaforme; policy su invio di dati sensibili via chat.

15. Rogue software updates / supply-chain social engineering

- Esempi: messaggi che spingono a installare aggiornamenti da link esterni; attacco alla catena di fornitura.
- Difese: consentire aggiornamenti solo da repository ufficiali; code signing; monitoring integrità; procedure per verifica aggiornamenti.

Linee di difesa tecniche e organizzative, obbligatorie:

- Autenticazione forte: MFA su tutti gli account privilegiati e accessi remote.
- Principle of Least Privilege: conti con privilegi minimi; role-based access control.
- Patch management e hardening: ridurre superficie d'attacco software.
- Protezione endpoint: EDR/AV con rilevamento comportamentale e prevenzione esecuzione per file malevoli.
- Email security avanzata: SPF/DKIM/DMARC, sandboxing allegati, URL rewriting e controllo click.
- Logging centralizzato e SIEM: correlazione eventi di phishing, login anomali, comportamenti sospetti.
- Backup e recovery: backup offline e piani di ripristino testati (mitigano estorsioni/crypto).
- Procedure: double-check per transazioni finanziarie, ticketing obbligatorio per interventi, escalation definita.
- Training periodico e test: esercitazioni phishing simulate, valutazioni, remediation training obbligatorio per chi cade.
- Cultura del reporting: procedura semplice e non punitiva per segnalare tentativi social engineering.

Indicatori pratici di possibile attacco sociale da monitorare:

- Email con urgenza ingiustificata, minacce o ricompense.
- Mittente con piccolo cambiamento ortografico nel dominio.
- Richieste non consone al ruolo del richiedente (es. cambio IBAN via email).
- Link che mostrano testo legittimo ma puntano a domini diversi.
- Allegati eseguibili o documenti con macro.
- Richieste out-of-band negate da canali ufficiali.

Azioni immediate post-incidente da imporre:

- Isolare account/endpoint compromessi.
- Resettare credenziali e revocare sessioni attive; forzare MFA reset se necessario.
- Avviare analisi forense log e endpoint per determinare impatto.
- Informare team finance/legale/management secondo playbook.
- Notifica agli utenti e avvio di campagne di mitigazione (scansione password compromesse, forced logout).

Non applicare queste difese è equivalente a lasciare la porta aperta: implementare le misure tecniche + procedure organizzative + formazione obbligatoria, monitorare e testare regolarmente.

Conclusioni:

Come è possibile evincere facilmente da questo breve esperimento, l'importanza di saper indirizzare bene con dei prompt precisi un IA è **fondamentale** per la buona riuscita di un output.

Lo stesso identico prompt presentato in due contesti differenti ha generato due risposte con delle varietà sia sulla lista di esempi di social engineering, che su i consigli extra proposti, uno più di carattere generale e uno più specifico come consiglio proprio per la difesa aziendale