

Social Engineering e Tecniche di Difesa

Obiettivo 1:

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.

Prompt utilizzato:

Definisci il termine "social engineering", poi descrivi le tecniche più comuni usate dagli attaccanti. includi tra queste il phishing e il tailgating.

Elaborazione della risposta:

Il social engineering è una tecnica di manipolazione psicologica usata dagli attaccanti per indurre le persone a compiere azioni o a rivelare informazioni riservate, come password, dati personali o accessi a sistemi.

Tecniche comuni di social engineering:

1. Phishing

Attacco in cui la vittima riceve un messaggio che sembra provenire da una fonte fidata, con l'obiettivo di:

- convincerla a cliccare su un link malevolo,
- inserire credenziali in un sito fasullo,
- scaricare allegati infetti.

Esempio: un'email della "banca" che dice "Abbiamo bloccato il tuo conto. Accedi subito".

Come difendersi?

Leggere con attenzione il messaggio ricevuto.

Controllare che il mittente sia chi dice di essere.

Contattare direttamente il mittente prima di proseguire per chiedere chiarimenti e assicurazioni.

2. Spear phishing

Variante più mirata del phishing. Il messaggio è personalizzato sulla base delle informazioni pubbliche della vittima (social network, azienda, ecc.), aumentando la credibilità dell'inganno.

Come difendersi?

Come detto prima, bisogna accertarsi del mittente e controllare se ci sono o no errori sospetti nella stesura del messaggio.

Se il messaggio ricevuto fa nascere dubbi, contattare subito chi è di competenza prima di fare qualsiasi altra cosa.

3. Pretexting

L'attaccante inventa una falsa identità o situazione per ottenere informazioni o accesso.

Esempio:

finge di essere un tecnico IT che ha bisogno della tua password per “risolvere un problema”.

Come difendersi?

Nessuno chiederà mai la tua password per “risolvere un problema”, nella maggior parte dei casi, potrebbe trattarsi di un tentativo di truffa. Non bisognerebbe mai lasciare le proprie informazioni sensibili quando non si è sicuri di chi stia dall'altra parte.

Anche in questo caso, contattare subito chi di competenza prima di fare azioni che comprometterebbero la propria sicurezza e quella dell'azienda.

4. Baiting

L'uso di un'esca per attirare la vittima. Spesso si basa sulla curiosità o sul desiderio di ottenere qualcosa gratuitamente.

Esempio:

Una chiavetta USB “dimenticata” in un luogo pubblico contenente malware, oppure un sito che promette di farti scaricare la versione craccata del tuo gioco preferito.

Come difendersi?

Non è oro tutto ciò che luccica, a volte è un tentativo di truffa.

Conoscere bene le fonti da dove si prendono risorse o informazioni è essenziale per non essere vittime di hacker malevoli.

Per testare un contenuto “sospetto” si possono usare macchine virtuali, ambienti isolati e antivirus.

5. Tailgating (o piggybacking)

l'attaccante si introduce in un'area riservata seguendo una persona autorizzata, approfittando della cortesia (es. qualcuno tiene aperta la porta).

Esempio:

un finto corriere che “si infila” in un edificio protetto quando un impiegato apre la porta.

Come difendersi?

Kevin D. Mitnick spiega in uno dei suoi libri come difendersi da questo tipo di attaccante: Non bisognerebbe fidarsi troppo di una faccia sconosciuta solo perché è stato cortese, la raccomandazione migliore è quella di chiedere sempre di mostrare un badge o un cartellino.

Nello stesso libro spiega però perché vedere un cartellino aziendale non è sufficiente ad assicurarsi della benevolenza del soggetto, bisogna accertarsi dei motivi e dell'identità della persona in caso non rispecchi chi dice di essere.

6. Quid Pro Quo

L'attaccante offre un beneficio (supporto tecnico, un regalo, ecc.) in cambio di informazioni o accesso.

Esempio:

Finge di essere dell'assistenza IT e ti chiede la password per "aiutarti".

Come difendersi?

Rifiuta qualsiasi aiuto tecnico o offerta se ti chiedono in cambio password, accessi o dati riservati: è quasi sempre un inganno.

Tecniche di difesa al social engineering

Obiettivo 2:

Chiedere a ChatGPT di suggerire strategie e migliori pratiche per difendersi dagli attacchi di social engineering. Prendere nota delle tecniche di difesa più efficaci.

Prompt utilizzato:

Elenca e spiega alcune delle strategie più efficaci per difendersi dal social engineering.

Elaborazione della risposta:

1. Formazione e consapevolezza continua

Perché è utile: La maggior parte degli attacchi riesce perché la vittima non conosce le tecniche usate.

Come attuarla:

- Partecipa a corsi di sicurezza informatica (anche brevi).
- Simula attacchi (es. finti phishing) in ambito aziendale per allenare il personale.
- Tieni aggiornate le conoscenze sulle nuove truffe circolanti.

2. Verifica sempre l'identità

Perché è utile: Gli attaccanti si fingono tecnici, colleghi, manager o fornitori.

Come attuarla:

- Non fornire mai informazioni riservate via email o telefono senza conferma.
- Se qualcuno si presenta di persona, chiedi badge e verifica con l'ufficio competente.
- Usa canali ufficiali per richiamare o ricontattare chi fa richieste sospette.

3. Non condividere mai password o codici di accesso

Perché è utile: Una volta ottenute, le credenziali permettono accessi completi.

Come attuarla:

- Nessun servizio legittimo ti chiederà mai la tua password.
- Usa password diverse per ogni servizio e cambia quelle sospette.

4. Diffida di urgenze o pressioni

Perché è utile: Gli attaccanti spesso creano senso di fretta o panico per ridurre la tua capacità di giudizio.

Come attuarla:

- Se ti dicono “devi agire subito”, fermati e rifletti.
- Prenditi sempre qualche minuto per analizzare la situazione.

5. Implementa il principio del minimo privilegio

Perché è utile: Limita i danni se un account viene compromesso.

Come attuarla:

- Ogni utente deve avere solo gli accessi strettamente necessari.
- Evita account “onnipotenti” usati per routine quotidiane.

6. Aggiorna software e sistemi regolarmente

Perché è utile: Alcuni attacchi social portano l'utente a scaricare malware.

Come attuarla:

- Mantieni antivirus, browser e OS aggiornati.
- Usa firewall e sistemi di rilevamento intrusioni.

7. Segnala subito i tentativi sospetti

Perché è utile: Rende l'organizzazione più resiliente e può prevenire danni.

Come attuarla:

- Se ricevi un messaggio o una telefonata sospetta, avvisa l'IT o il responsabile della sicurezza.
- Anche un tentativo fallito può fornire indizi utili.

Tecnica	Descrizione	Esempio	Come Difendersi
Phishing	Messaggi (email, SMS...) che sembrano legittimi e spingono l'utente a compiere azioni pericolose.	Email dalla "banca" che chiede di accedere urgentemente al conto.	Controllare mittente, leggere con attenzione, non cliccare subito: contattare direttamente chi sembra aver inviato il messaggio.
Spear Phishing	Variante mirata del phishing, basata su informazioni personali o aziendali per sembrare più credibile.	Email personalizzata che sembra provenire dal proprio capo o collega.	Verificare l'identità del mittente, cercare errori sospetti, contattare direttamente la persona se si hanno dubbi.
Pretexting	L'attaccante si finge qualcun altro per ottenere informazioni o accesso.	Un falso tecnico IT chiede la tua password per "risolvere un problema".	Nessuno dovrebbe mai chiedere password. Se non si è sicuri, non fornire dati e contattare chi di competenza.
Baiting	Uso di un'esca per invogliare la vittima ad agire, spesso con malware o link compromessi.	Chiavetta USB "dimenticata" in un luogo pubblico; sito che offre software craccato.	Diffidare delle "offerte" gratuite, usare antivirus e ambienti isolati per testare risorse sospette.
Tailgating	Accesso fisico non autorizzato ottenuto seguendo da vicino una persona legittimata.	Finto corriere entra in azienda quando un dipendente apre la porta.	Come suggerito da Kevin Mitnick: chiedere sempre badge e verificare identità e motivazioni della persona sconosciuta.
Quid Pro Quo	L'attaccante offre qualcosa (supporto tecnico, regali, vantaggi) in cambio di informazioni sensibili.	Un falso tecnico propone assistenza in cambio della password.	Rifiutare richieste che implicano la consegna di dati sensibili in cambio di aiuto o premi: è un classico trucco da social engineering.