RELAZIONE S5 - L4 - Social Engineering e tecniche di difesa

Passo 1 — Comprendere il Social Engineering.

- **Prompt 1 — Spiegazione + tecniche + esempi**

Agisci da docente di Cybersecurity (livello base, chiaro).
1) Spiegami cos'è il Social Engineering e perché funziona (fattore umano).
2) Descrivi le tecniche più comuni, con definizione + esempio breve per ciascuna:

- Phishing
- Spear phishing
- Whaling
- Pretexting
- Baiting (es. USB drop)
- Tailgating/Piggybacking
- Vishing
- Smishing
- Deepfake voice/video

3) Elenca i segnali di allarme per riconoscere un tentativo di Social Engineering (almeno 10).

Social Engineering (Ingegneria Sociale)

Cos'è
Il *Social Engineering* è un insieme di tecniche con cui un attaccante **manipola le persone** per ottenere informazioni, accessi o compiere azioni dannose. Non colpisce i sistemi, ma **sfrutta il fattore umano** (fiducia, paura, urgenza, autorità).

Perché funziona

- Le persone sono abituate a **fidarsi** (email, telefonate, procedure).
- Le emozioni (urgenza, curiosità, timore) **riduccono il pensiero critico**.
- I controlli tecnici possono essere aggirati se l'utente **collabora inconsapevolmente**.

Tecniche più comuni (definizione + esempio)

1) Phishing

Definizione: messaggi (email/SMS/chat) che imitano fonti legittime per rubare credenziali o indurre azioni.
Esempio: “La tua password scade oggi, clicca qui per aggiornarla”.

Varianti

- **Spear phishing:** mirato a una persona/ruolo specifico.
  Esempio: email al reparto IT con riferimenti reali al progetto in corso.
- **Whaling:** mirato a dirigenti o figure apicali.
  Esempio: finto messaggio del CEO che chiede un bonifico urgente.

---

2) Pretexting

Definizione: creazione di un **pretesto credibile** (storia/ruolo) per ottenere dati.
Esempio: “Sono dell’helpdesk, devo verificare il tuo account: mi confermi username e codice?”

---

3) Baiting (es. USB drop)

Definizione: sfrutta **curiosità o convenienza** offrendo un’esca.
Esempio: chiavetta USB “Stipendi 2026” lasciata in ufficio; collegandola, installa malware.

---

4) Tailgating / Piggybacking

Definizione: accesso fisico non autorizzato seguendo qualcuno autorizzato.
Esempio: una persona entra dietro a un dipendente dicendo “Ho dimenticato il badge”.

---

5) Vishing e Deepfake Voice

Definizione: truffe telefoniche; con **deepfake vocali** si imita la voce di persone reali.
Esempio: chiamata che replica la voce del responsabile e chiede dati o pagamenti urgenti.

Segnali tipici di allarme (red flags)

- **Urgenza o pressione** (“subito”, “entro 10 minuti”).
- **Richieste insolite** di credenziali, codici MFA, bonifici.
- **Errori o incoerenze** (indirizzi email simili, link strani).
- **Autorità improvvisa** (“Sono il CEO/IT/fornitore”).
- **Offerte troppo vantaggiose** o file inattesi.
- **Canali non abituali** (CEO che scrive via SMS/WhatsApp).
- **Richiesta di segretezza** (“Non dirlo a nessuno”).

Buona pratica chiave: verifica sempre su **un canale alternativo** (telefonata interna, ticket ufficiale, contatto noto) prima di agire.

- # Prompt 2 — Difese + best practice + checklist finale

Agisci da responsabile Security in azienda.
Fammi una guida alle strategie di difesa e migliori pratiche.

Includi obbligatoriamente:

1) Formazione e sensibilizzazione (training + simulazioni)
2) Policy e procedure (verifica richieste sensibili su canale separato)
3) Tecnologie (filtri email, antivirus/EDR, MFA/2FA, DMARC/SPF/DKIM)
4) Gestione accessi (least privilege, logging, monitoraggio)

Per ogni punto scrivi:
- cosa fare (pratico)
- perché funziona
- esempio concreto

Chiudi con:
- una checklist “anti social engineering” di 10 regole per i dipendenti
- 5 raccomandazioni finali sintetiche per l’azienda

Formato: titoli + elenco puntato.

Strategie di difesa contro il Social Engineering

1) Formazione e sensibilizzazione

(training continuo + simulazioni pratiche)

Cosa fare (pratico)

- Erogare **formazione periodica obbligatoria** (almeno annuale) su phishing, vishing, pretexting, deepfake.
- Organizzare **simulazioni di phishing** interne (email false ma controllate).
- Prevedere **micro-training** brevi (5–10 minuti) dopo ogni simulazione fallita.
- Aggiornare il training in base alle **nuove minacce** (AI voice, QR phishing).

Perché funziona

- Il social engineering sfrutta **l'errore umano**, non le vulnerabilità tecniche.
- La ripetizione crea **memoria comportamentale**: il dipendente riconosce il pattern.
- Le simulazioni riducono il panico e aumentano la capacità di reazione reale.

Esempio concreto

Un dipendente riceve una mail che simula un "reset password urgente".
Avendo già visto lo stesso schema durante una simulazione, **non clicca**, segnala l'email al SOC e evita la compromissione dell'account.

---

2) Policy e procedure

(regole chiare, verifiche su canale separato)

Cosa fare (pratico)

- Definire policy scritte per:
    - richieste di **pagamenti**
    - reset credenziali
    - condivisione di dati sensibili
- Introdurre l'obbligo di **verifica su canale separato** (telefono, Teams, di persona).

- Formalizzare la regola: *“Nessuna urgenza giustifica una deroga”*.
- Rendere le procedure **semplici e accessibili** a tutti.

Perché funziona

- Il social engineering fa leva su **autorità + urgenza**.
- Il canale separato rompe lo schema dell’attaccante.
- Le policy tolgono responsabilità individuale e riducono decisioni impulsive.

Esempio concreto

Un’email sembra arrivare dal CFO e chiede un bonifico urgente.
La procedura impone la **conferma telefonica** → il CFO nega → tentativo bloccato.

---

3) Tecnologie di sicurezza
(difesa multilivello)

Cosa fare (pratico)

- **Email Security**: filtri antiphishing, sandbox allegati, analisi link.
- **Autenticazione forte**: MFA/2FA su email, VPN, cloud, account admin.
- **Endpoint Protection**: antivirus + EDR su tutti i dispositivi.
- **Protezione dominio email**: configurare SPF, DKIM e DMARC (policy reject).
- Bloccare macro e allegati eseguibili non necessari.

Perché funziona

- Riduce drasticamente la **superficie di attacco**.
- Anche se l’utente sbaglia, la tecnologia **contiene il danno**.
- MFA rende inutili molte credenziali rubate.

Esempio concreto

Un utente inserisce le credenziali su un sito di phishing.
L’attaccante tenta l’accesso, ma senza il secondo fattore **l’account resta protetto**.

---

4) Gestione degli accessi

(least privilege + monitoraggio)

Cosa fare (pratico)

- Applicare il principio del **least privilege** (solo accessi necessari).
- Separare account utente e account amministrativi.
- Abilitare **logging centralizzato** (login, accessi, azioni critiche).
- Monitorare eventi anomali (orari insoliti, IP esteri, accessi massivi).
- Revocare immediatamente accessi non più necessari.

Perché funziona

- Limita l'impatto di un account compromesso.
- Permette **individuazione rapida** di un attacco in corso.
- Supporta analisi forense e incident response.

Esempio concreto

Un account HR viene compromesso, ma non ha accesso ai sistemi finanziari.
Il danno è **contenuto** e l'accesso anomalo viene rilevato dai log.

Checklist "Anti Social Engineering" – 10 regole per i dipendenti

1. Diffida sempre di **urgenze improvvise**.
2. Controlla con attenzione **mittente e dominio email**.
3. Non cliccare link o allegati inattesi.
4. Verifica richieste sensibili su **canale separato**.
5. Nessuno è autorizzato a chiedere password o codici MFA.
6. Errori grammaticali o toni insoliti sono un campanello d'allarme.
7. Le email "troppo belle per essere vere" lo sono.
8. Segnala subito messaggi sospetti al team IT/Security.
9. Non farti intimidire da presunta autorità.
10. Quando hai dubbi, **fermati e chiedi**.

Raccomandazioni finali per l’azienda (sintesi)

1. Il social engineering è un **rischio di business**, non solo IT.
2. La formazione continua è la **prima linea di difesa**.
3. Le policy devono essere chiare, semplici e applicabili.
4. Tecnologia e persone devono lavorare insieme.
5. Misura, simula, migliora: la sicurezza è un **processo continuo**.