Esercitazione S5-L4 (da ChatGPT)

Cos'è il Social Engineering?

Il **Social Engineering** (ingegneria sociale) è una tecnica utilizzata dagli attaccanti per manipolare le persone al fine di ottenere informazioni sensibili, accessi non autorizzati o compiere azioni che compromettano la sicurezza di un sistema informatico o di un'organizzazione.

A differenza di attacchi che si basano su vulnerabilità tecniche (come malware o exploit), il social engineering sfrutta **l'errore umano**, facendo leva su fattori psicologici come la fiducia, la paura, l'urgenza o la curiosità. Gli attaccanti mirano a convincere le vittime a rivelare dati riservati, come credenziali, numeri di carte di credito, informazioni personali, o a compiere azioni che compromettono la sicurezza, come cliccare su link malevoli o aprire allegati infetti.

Tecniche più utilizzate nel Social Engineering

1. Phishing

Il **phishing** è una delle forme più comuni di social engineering. Consiste nell'invio di messaggi fraudolenti (spesso via email, SMS o piattaforme di messaggistica) che sembrano provenire da fonti affidabili. Lo scopo è indurre la vittima a:

- Fornire credenziali (username e password),
- Scaricare malware,
- Effettuare pagamenti o trasferimenti di denaro.

Caratteristiche comuni del phishing:

- **Spoofing del mittente:** Gli attaccanti utilizzano email che sembrano provenire da enti legittimi come banche, istituzioni governative o aziende conosciute.
- **Messaggi urgenti:** "La tua password scade oggi!" oppure "Il tuo account è stato bloccato!" sono esempi di messaggi che creano un senso di urgenza.
- **Link ingannevoli:** L'URL sembra legittimo ma, se analizzato, punta a un sito fraudolento.

Varianti di phishing:

- **Spear Phishing:** Attacchi mirati verso una persona specifica o un gruppo ristretto, con messaggi personalizzati basati su informazioni raccolte sull'obiettivo.
- **Whaling:** Variante del phishing che prende di mira alti dirigenti o figure di rilievo in un'azienda.
- **Smishing:** Phishing tramite SMS.
- **Vishing:** Phishing tramite chiamate vocali, spesso utilizzando sistemi automatizzati.

---

2. Tailgating (o piggybacking)

Il **tailgating** è una tecnica fisica di social engineering in cui un attaccante accede a un'area riservata di un edificio (come un ufficio o un data center) **approfittando della fiducia o della distrazione di una persona autorizzata**.

Come funziona:

- L'attaccante segue una persona autorizzata attraverso una porta d'accesso controllata (es. con badge o codice di sicurezza).
- Spesso si presentano come dipendenti, tecnici o fornitori, sfruttando il fatto che molte persone non chiedono verifiche per educazione o fiducia.

Esempio classico:

- Un attaccante con in mano pacchi o attrezzature si avvicina a una porta chiusa e chiede gentilmente a un dipendente di "tenergli la porta aperta", fingendo di essere impossibilitato a usare il badge.

---

3. Pretexting

Il **pretexting** consiste nella creazione di una storia fittizia o di una falsa identità per convincere la vittima a condividere informazioni riservate. L'attaccante potrebbe fingersi, ad esempio:

- Un collega o superiore,
- Un rappresentante di un'azienda (ad esempio dell'help desk),
- Un agente delle forze dell'ordine.

Esempio: un attaccante chiama un dipendente fingendo di essere del reparto IT e lo convince a fornire la password per "risolvere un problema tecnico".

---

4. Baiting

Il **baiting** (letteralmente, "adescamento") sfrutta la curiosità della vittima, inducendola ad accedere a un file o a un dispositivo infetto. Spesso viene usato in forma fisica o digitale.

Esempi:

- L'attaccante lascia una chiavetta USB compromessa in un'area comune, con un'etichetta accattivante come "Salari_2024.doc". La vittima inserisce la chiavetta nel proprio computer, installando malware.
- Pubblicità o link che promettono download gratuiti di software o film, ma che contengono virus.

---

5. Quid Pro Quo

In questo caso, l'attaccante offre un **beneficio in cambio di informazioni riservate** o accesso ai sistemi. Ad esempio:

- Si finge un tecnico IT e chiama le vittime promettendo supporto gratuito per risolvere problemi al computer, chiedendo in cambio credenziali o accesso remoto.
- Un falso sondaggio promette una ricompensa (come un buono sconto o un gadget) in cambio di informazioni sensibili.

---

6. Shoulder Surfing

Lo **shoulder surfing** consiste nell'osservare fisicamente una persona mentre:

- Digita la password o il PIN su un dispositivo,
- Inserisce informazioni riservate.

Questo può avvenire in luoghi pubblici (es. bancomat, aeroporti) o in uffici affollati.

---

7. Dumpster Diving

Gli attaccanti rovistano nei cestini della spazzatura o nei documenti scartati alla ricerca di:

- Informazioni sensibili (es. password scritte, report finanziari, dati aziendali).
- Materiali che possano essere usati per creare attacchi più sofisticati (ad esempio, email aziendali trovate nei rifiuti possono essere usate per il phishing).

Come proteggersi dal Social Engineering

Per il phishing:

- Controllare sempre l'indirizzo del mittente e i link sospetti prima di cliccarci.
- Non fornire mai informazioni personali o credenziali in risposta a email non richieste.
- Utilizzare software di sicurezza per rilevare email fraudolente.

Per il tailgating:

- Non aprire porte a persone sconosciute senza verificarne l'identità.
- Usare sistemi di sicurezza avanzati (es. badge magnetici con registrazione).

Pretexting e altre tecniche:

- Educare i dipendenti sulle tecniche di social engineering.

- Segnalare qualsiasi richiesta sospetta o insolita.
- Implementare procedure di verifica per tutte le richieste di accesso o informazioni.

Ecco alcuni esempi reali di attacchi di **social engineering** avvenuti nel mondo, classificati in base alla tecnica utilizzata. Questi casi dimostrano l'efficacia dell'ingegneria sociale nel bypassare anche le difese tecnologiche più avanzate, sfruttando l'errore umano.

Esempi di Attacchi di Phishing

1. L'attacco a Google e Facebook (2013–2015)

Un truffatore lituano, **Evaldas Rimasauskas**, riuscì a frodare Google e Facebook per una somma complessiva di circa **100 milioni di dollari**.
Come fece:

- Rimasauskas impersonò un fornitore asiatico legittimo, **Quanta Computer**, che lavorava regolarmente con Google e Facebook.
- Creò indirizzi email e documenti falsi che sembravano provenire da Quanta.
- Inviò email ai dipartimenti finanziari delle due aziende richiedendo il pagamento di fatture per servizi forniti.
  Risultato: Entrambe le aziende trasferirono milioni sui conti bancari controllati dall'attaccante.
  Lezione: Questo attacco dimostra come il phishing mirato (spear phishing) può ingannare anche le organizzazioni più grandi.

---

2. Target Corporation (2013)

Un attacco di phishing fu il punto d'ingresso per una delle più grandi violazioni di dati della storia, in cui furono compromessi i dati di oltre **40 milioni di carte di credito**.
Come accadde:

- Gli hacker inviarono email di phishing ai dipendenti di un fornitore terzo di Target, una società che gestiva la manutenzione degli impianti di condizionamento.
- Una volta ottenute le credenziali del fornitore, gli attaccanti accedettero ai sistemi interni di Target.
- Iniettarono malware nei registratori di cassa per raccogliere i dati delle carte di credito in tempo reale.
  Lezione: Anche una terza parte connessa alla rete di un'azienda può rappresentare una vulnerabilità.

---

3. Sony Pictures (2014)

Nel famoso attacco a Sony Pictures, attribuito al gruppo di hacker nordcoreani **"Guardians of Peace"**, fu utilizzata una combinazione di phishing e spear phishing.
Come accadde:

- Gli hacker inviarono email mirate ai dipendenti di Sony, fingendosi colleghi o rappresentanti di enti legittimi.
- Una volta compromessi i computer di alcuni dipendenti, gli attaccanti ottennero accesso a file riservati, email aziendali e script di film.
  Risultato: Furono rubati e pubblicati online numerosi dati sensibili, causando danni reputazionali e finanziari enormi.

Esempi di Tailgating

4. L’attacco al Data Center di RSA (2011)

Un attacco fisico contro il data center di **RSA Security**, un’importante azienda di sicurezza informatica, utilizzò una combinazione di social engineering e tecniche fisiche.
Come accadde:

- Gli attaccanti si presentarono come fornitori di servizi di pulizia o manutenzione, riuscendo a entrare nei locali riservati.
- Approfittando del tailgating, accedettero a stanze con server contenenti dati sensibili, rubando file cruciali legati ai token di sicurezza SecurID. **Risultato:** L'attacco compromise i sistemi di sicurezza utilizzati da milioni di clienti RSA.

---

5. L'attacco di "Kevin Mitnick"

Kevin Mitnick, uno dei più famosi hacker della storia, utilizzava spesso il **tailgating** e il **pretexting** per infiltrarsi fisicamente in edifici aziendali.
Come agiva:

- Fingendosi un tecnico informatico o un nuovo dipendente, Mitnick si avvicinava agli uffici di aziende tecnologiche.
- Seguiva impiegati veri attraverso le porte di sicurezza, approfittando della loro fiducia.
  Risultato: Una volta dentro, accedeva ai sistemi aziendali e rubava dati sensibili.

Esempi di Pretexting

6. L’attacco al CEO di Mattel (2015)

Un truffatore ingannò il CFO di Mattel convincendolo a trasferire **3 milioni di dollari** su un conto bancario cinese.
Come accadde:

- Il truffatore si spacciò per il CEO della compagnia, utilizzando email e tecniche di spoofing per imitare il tono e lo stile del dirigente.
- Approfittando di un momento in cui il vero CEO era in viaggio, l'attaccante richiese al CFO un trasferimento urgente di denaro per una "acquisizione riservata". **Risultato:** I soldi furono trasferiti, ma grazie a un intervento tempestivo, parte della somma fu recuperata.

---

7. Il finto tecnico IT (Clever Social Engineering)

Un attaccante convinse diversi dipendenti di una grande banca fingendosi un tecnico IT.
Come fece:

- L'attaccante chiamava i dipendenti e diceva che c'era un problema con il loro computer.
- Li convinceva a fornire le credenziali di accesso "per risolvere rapidamente il problema".
  Risultato: L'attaccante ottenne accesso al sistema della banca, compromettendo dati finanziari sensibili.

Esempi di Baiting

8. L'attacco tramite chiavette USB (Stuxnet)

Il worm **Stuxnet**, che comprometteva sistemi industriali, fu diffuso anche tramite **chiavette USB lasciate intenzionalmente nei pressi di aziende e impianti industriali**.
Come funzionava:

- Le chiavette, una volta inserite nei computer da dipendenti curiosi, installavano automaticamente il malware.
  Risultato: Furono compromessi diversi sistemi SCADA, inclusi quelli di una centrale nucleare iraniana.

---

9. Netflix Fake Giveaway (2017)

Gli attaccanti crearono pagine web false che offrivano **abbonamenti gratuiti a Netflix**, convincendo gli utenti a inserire dati personali e credenziali.
Come funzionava:

- L'offerta sembrava autentica e pubblicizzata tramite social media.

- Gli utenti, attratti dall'idea di un regalo, fornivano dati sensibili che venivano poi utilizzati per ulteriori attacchi o venduti sul dark web.

Esempi di Dumpster Diving

10. Hack dell’Agenzia di Sicurezza di Londra

Un hacker riuscì a ottenere accesso a documenti riservati di una compagnia di sicurezza britannica semplicemente rovistando nella **spazzatura dell’azienda**.
Come accadde:

- Nei cestini furono trovati documenti con credenziali di accesso, report di sicurezza e schemi di rete.
- Con queste informazioni, l'attaccante pianificò un attacco mirato contro i sistemi dell'azienda.
  Lezione: La gestione sicura dei documenti cartacei è fondamentale, così come la loro distruzione corretta (es. tramite triturazione).

Conclusione

Questi esempi dimostrano quanto sia potente il **social engineering** e quanto possa essere devastante se combinato con attacchi tecnici. La chiave per difendersi da questi attacchi è una **consapevolezza costante** da parte di tutti i dipendenti, combinata con l'adozione di **procedure di sicurezza rigorose**.

. Tecniche per contrastare il Social Engineering

Contrastare gli attacchi di **social engineering** richiede un approccio multilivello che combini **educazione, tecnologia e politiche aziendali rigorose**. Qui di seguito trovi i migliori metodi, suddivisi per categorie, per proteggerti da queste minacce.

1. Formazione e Sensibilizzazione del Personale

A. Corsi di formazione sulla cybersicurezza

- **Obiettivo:** Rendere i dipendenti consapevoli delle tecniche di social engineering, insegnando loro a identificare segnali di pericolo.
- **Contenuti chiave:**
  - Come riconoscere email di phishing e messaggi fraudolenti.
  - Come gestire richieste sospette di informazioni (es. pretexting).

    - Importanza di non condividere mai password, nemmeno con colleghi o “tecnici”.
    - Simulazioni di attacchi (phishing simulato o test di tailgating).

B. Cultura della Sicurezza

- **Incoraggiare segnalazioni:** I dipendenti devono sentirsi liberi di segnalare attività sospette senza timore di ripercussioni.
- **Aggiornamenti regolari:** Organizzare briefing periodici per informare sulle nuove tecniche di social engineering.

---

2. Difese Tecnologiche

A. Protezioni contro il phishing

1. **Filtri antispam avanzati:**
    - Utilizzare soluzioni come **Microsoft Defender for Office 365**, **Proofpoint**, o **SpamTitan** per identificare email fraudolente.
    - Bloccare email con spoofing del mittente e URL sospetti.
2. **Autenticazione DMARC, DKIM e SPF:**
    - Implementare protocolli di autenticazione delle email per ridurre il rischio di spoofing.
3. **Sandbox per allegati:**
    - Allegati sospetti vengono aperti in un ambiente virtuale sicuro prima di raggiungere l'utente.
4. **URL rewriting:**
    - Modifica automatica dei link nelle email per reindirizzare l'utente a un sistema di controllo che verifica la sicurezza del sito.

B. Monitoraggio delle attività

- **Sistemi di monitoraggio del comportamento utente (UEBA):**
    - Identificare attività anomale, come tentativi di accesso insoliti o trasferimenti di file sospetti.
    - Soluzioni popolari: **Splunk**, **Microsoft Sentinel**, **Exabeam**.
- **Intrusion Detection Systems (IDS):**
    - Rilevano e bloccano attività sospette nelle reti aziendali.

C. Autenticazione avanzata

1. **Autenticazione a due fattori (2FA):**
    - Utilizzare 2FA per ogni accesso, preferibilmente con app come **Google Authenticator** o dispositivi hardware come **YubiKey**.
2. **Password Manager:**
    - Strumenti come **LastPass**, **Dashlane** o **Bitwarden** aiutano a creare e gestire password sicure.
    - Riduce la probabilità di riutilizzo delle credenziali.

D. Protezione degli endpoint

- **Soluzioni EDR (Endpoint Detection and Response):**
    - Software come **CrowdStrike**, **Carbon Black** o **SentinelOne** rilevano e bloccano malware o attività sospette sui dispositivi degli utenti.
- **Firewall personale:**
    - Blocco di connessioni non autorizzate o traffico sospetto.

---

3. Politiche e Procedure Aziendali

A. Gestione delle credenziali

- **Mai condividere password:**
    - Nessun dipendente dovrebbe mai fornire password per telefono o email.
- **Politica di rotazione delle password:**
    - Richiedere aggiornamenti periodici delle password (ogni 90 giorni o meno).
- **Accesso minimo necessario:**
    - Fornire a ciascun dipendente solo i privilegi necessari per il proprio ruolo.

B. Gestione degli accessi fisici

1. **Controllo rigoroso degli accessi:**
    - Utilizzare badge, lettori biometrici o PIN unici per limitare l'accesso agli edifici o ai server.
    - Monitorare l’uso dei badge tramite log.

2. **Politica "no tailgating":**
    - Addestrare i dipendenti a non consentire l'accesso a persone senza badge.
    - Installare tornelli o porte a chiusura automatica per prevenire il tailgating.
3. **Supervisione dei visitatori:**
    - Registrazione e accompagnamento obbligatori per ogni visitatore.

C. Distruzione sicura dei documenti

1. **Triturazione obbligatoria:**
    - Distruggere documenti contenenti informazioni sensibili utilizzando distruggi documenti certificati.
2. **Gestione sicura dei dispositivi di archiviazione:**
    - Pulizia sicura dei dati prima di smaltire dischi rigidi, USB e altri dispositivi.

---

4. Difese Psicologiche contro il Social Engineering

A. Verifica delle richieste

- **Regola del doppio controllo:**
    - Verificare ogni richiesta di trasferimento di fondi o accesso a dati sensibili tramite un secondo canale di comunicazione (es. telefonata diretta al richiedente).
- **Domande di sicurezza:**
    - Implementare procedure per verificare l'identità di chi richiede informazioni (es. domande segrete o codici univoci).

B. Gestione delle situazioni di emergenza

1. **Politiche contro l'urgenza:**
    - Addestrare i dipendenti a non cedere a richieste urgenti o pressioni emotive senza verifiche adeguate.
2. **Team dedicato alla sicurezza:**
    - Creare un team interno a cui i dipendenti possono rivolgersi in caso di dubbi su attività sospette.

---

5. Simulazioni e Test di Sicurezza

A. Test di phishing simulati

- **Obiettivo:** Inviare campagne simulate di phishing ai dipendenti per misurare la loro reazione e individuare punti deboli.
- Strumenti consigliati: **KnowBe4**, **PhishMe**, **Barracuda Sentinel**.

B. Audit di sicurezza regolari

- Condurre controlli periodici sui protocolli di sicurezza per identificare vulnerabilità.
- Simulare attacchi fisici (es. tailgating) e sociali (es. pretexting) per testare le procedure aziendali.

---

6. Soluzioni Legali e di Conformità

A. Politiche di non divulgazione (NDA)

- Obbligare dipendenti, fornitori e partner a firmare NDA per garantire la riservatezza delle informazioni sensibili.

B. Conformità normativa

- Assicurarsi che l'azienda rispetti standard di sicurezza come:
    - **GDPR** (protezione dei dati personali in Europa).
    - **ISO/IEC 27001** (gestione della sicurezza delle informazioni).
    - **PCI DSS** (per le aziende che gestiscono carte di credito).

---

7. Protezione Contro Tecniche Specifiche

Ecco un'analisi dettagliata di come contrastare **ogni singolo tipo di attacco di social engineering** descritto in precedenza. La difesa contro questi attacchi richiede una combinazione di **misure preventive**, **procedure aziendali** e **tecnologie avanzate**. Per ogni attacco, indicherò le contromisure specifiche.

1. Phishing

Attacco che tenta di ingannare le persone attraverso email, messaggi o siti web falsi.

Come contrastarlo

A. Tecnologie anti-phishing

- **Filtri antispam avanzati:**

    - Strumenti come **Proofpoint**, **Barracuda** o **Microsoft Defender** bloccano email di phishing.
    - Riconoscono schemi sospetti e segnalano URL o domini fraudolenti.
- **Protezione DNS:**
    - Soluzioni come **Quad9** o **Cloudflare DNS** filtrano i siti web pericolosi.

B. Autenticazione dell'email

- **DMARC, SPF e DKIM:**
    - Questi protocolli verificano che un'email provenga davvero dal dominio che afferma di rappresentare, riducendo attacchi di spoofing.

C. Formazione continua

- Educare il personale su:
    - Verifica degli URL prima di cliccare (es. passare il cursore sopra un link per visualizzare la destinazione).
    - Segnali tipici di phishing (grammatica errata, urgenza, richieste di dati sensibili).
    - Non aprire allegati da mittenti sconosciuti.

D. Simulazioni regolari

- Inviare email di phishing simulate per verificare la prontezza del personale. Soluzioni: **KnowBe4**, **PhishMe**.

---

2. Spear Phishing

Phishing mirato a individui specifici, basato su informazioni personali.

Come contrastarlo

A. Ricerca limitata delle informazioni

- **Minimizzare la presenza sui social media:**
    - Educare i dipendenti a non condividere dettagli personali/professionali che potrebbero essere sfruttati.
    - Implementare controlli sulla privacy dei profili.

B. Doppio controllo delle richieste

- Qualsiasi richiesta di dati sensibili o trasferimenti di denaro deve essere verificata attraverso un **secondo canale** (es. telefonata diretta).

C. Difese tecnologiche

- **Indicatori di compromissione (IOC):**

    - Soluzioni come **SIEM** (es. Splunk, IBM QRadar) analizzano email e documenti per identificare segnali di spear phishing.

---

3. Pretexting

Gli attaccanti si spacciano per figure autorevoli per ottenere informazioni sensibili.

Come contrastarlo

A. Politica di verifica dell'identità

- Implementare procedure obbligatorie per verificare l'identità:
    - Richiedere dettagli aggiuntivi o verificare le richieste attraverso canali interni.
    - Utilizzare **domande di sicurezza** o **codici segreti** per confermare l'identità.

B. Divieto di condivisione immediata

- Formare il personale a non fornire informazioni sensibili, nemmeno a figure che sembrano legittime, senza un’autorizzazione ufficiale.

C. Monitoraggio delle richieste sospette

- Implementare un sistema di tracciamento per tutte le richieste di accesso o modifica dei dati, come:
    - Registri centralizzati delle richieste.
    - Allarme automatico per richieste ripetute o non ordinarie.

---

4. Tailgating

Accedere a un’area riservata sfruttando la fiducia o la distrazione di altri.

Come contrastarlo

A. Controllo degli accessi

1. **Badge elettronici e biometrici:**
    - Utilizzare badge personalizzati con foto e chip RFID.
    - Installare lettori biometrici (impronte digitali, riconoscimento facciale).
2. **Tornelli con accesso singolo:**
    - Tornelli o porte a chiusura automatica che consentono l’accesso a una persona per volta.

B. Politica “No Tailgating”

- Formazione dei dipendenti per:
    - Non permettere l’ingresso a estranei o persone senza badge.
    - Non tenere aperte le porte per altri, anche se sembrano colleghi.

C. Videosorveglianza

- Installare telecamere di sicurezza nelle aree di accesso critiche, con monitoraggio attivo.

---

5. Baiting

Gli attaccanti utilizzano incentivi (es. chiavette USB o premi) per indurre le vittime a compiere azioni pericolose.

Come contrastarlo

A. Protezione degli endpoint

- **Bloccare dispositivi USB non autorizzati:**
    - Disabilitare l’uso delle porte USB sui computer aziendali, a meno che non siano registrate.

B. Formazione sulla curiosità umana

- Insegnare al personale che:
    - Le chiavette USB trovate per strada **non devono mai essere inserite nei computer aziendali**.
    - Qualsiasi premio o offerta “troppo bella per essere vera” potrebbe essere un’esca.

C. Tecnologie di sandboxing

- Utilizzare sandbox virtuali per esaminare file o dispositivi sospetti in un ambiente sicuro.

---

6. Dumpster Diving

Raccogliere informazioni da documenti cartacei o dispositivi scartati.

Come contrastarlo

A. Distruzione sicura dei documenti

1. **Trituratori certificati:**
    - Utilizzare trituratori industriali (standard DIN P-4 o superiori) per documenti sensibili.
2. **Distruzione dei dispositivi digitali:**
    - Smagnetizzazione (degaussing) o distruzione fisica di hard disk, USB e altri dispositivi.

B. Politiche di smaltimento sicuro

- Implementare una politica aziendale per:
    - Archiviazione sicura fino alla distruzione.
    - Ritiro regolare dei rifiuti da fornitori certificati.

---

7. Vishing (Phishing telefonico)

Truffe condotte tramite telefonate.

Come contrastarlo

A. Politica di verifica dell'identità

- Richiedere un **codice univoco di autenticazione** per tutte le chiamate relative a dati sensibili o operazioni.

B. Divieto di condivisione via telefono

- Stabilire che dati sensibili (es. password, credenziali, PIN) **non devono mai essere condivisi telefonicamente**.

C. Registrazione delle chiamate sospette

- Installare sistemi di registrazione per tracciare e verificare le chiamate sospette.

---

8. Smishing (Phishing via SMS)

Gli attaccanti inviano SMS fraudolenti per ottenere informazioni personali o indurre l'utente a cliccare su link pericolosi.

Come contrastarlo

A. Filtraggio SMS

- Utilizzare soluzioni di sicurezza mobile come **Lookout** o **Kaspersky Mobile Security** per identificare messaggi fraudolenti.

B. Consapevolezza degli utenti

- Formare il personale a:
    - Non cliccare su link provenienti da mittenti sconosciuti.
    - Verificare sempre i messaggi di banche, operatori telefonici o enti.

---

9. Watering Hole

Compromettere siti web popolari per infettare specifici target.

Come contrastarlo

A. Navigazione sicura

1. **Estensioni di sicurezza:**
    - Utilizzare strumenti come **Malwarebytes Browser Guard** o **uBlock Origin**.
2. **DNS sicuro:**
    - Soluzioni come **OpenDNS** bloccano siti compromessi.

B. Protezione degli endpoint

- Utilizzare antivirus e EDR (Endpoint Detection and Response) per rilevare attività anomale.

C. Monitoraggio continuo

- Analizzare i siti web visitati dal personale per identificare quelli compromessi.

Conclusione

La difesa contro gli attacchi di **social engineering** dipende da:

1. **Educazione del personale** per ridurre l'errore umano.
2. **Adozione di tecnologie avanzate** come 2FA, EDR e filtri antiphishing.
3. **Implementazione di procedure rigorose** per l'accesso fisico e digitale.