Esercitazione sulle metodologie di ingegneria sociale

Scopo didattico ed etico

L'obiettivo dell'esercitazione odierna è creare uno scenario di **pretexting** (costruzione di un pretesto credibile), scegliendo un contesto di preferenza, con l'intendo di **sensibilizzare** gli utenti su questa pratica utilizzata da malintenzionati per raccogliere informazioni sensibili tramite ingegneria sociale.

Avviso

Questo elaborato **non intende insegnare a truffare**, ma a riconoscere e neutralizzare le tecniche di social engineering.

Scenario creativo: "La verifica del supporto tecnico"

Nello scenario che ho scelto per oggi, un'ipotetica azienda di software, "**TechVision Solutions**", fornisce supporto tecnico ai propri clienti tramite telefono e email.

L'attaccante sfrutta la fiducia nel supporto ufficiale, fingendo di essere un **tecnico IT autorizzato** che contatta l'utente per motivi legittimi (aggiornamento software, verifica di licenza, indagine su anomalie di accesso).

L'attaccante sfrutta le vulnerabilità emotive del destinatario: dopo aver confermato dettagli aziendali reali (recuperati da LinkedIn, siti ufficiali o OSINT), la persona acquisisce fiducia e diviene disponibile a condividere informazioni che in altri contesti rifiuterebbe.

L'obiettivo dell'attaccante è sottrarre:

- **Credenziali di accesso** (username/password)
- **Token di autenticazione** o link di reset password
- **Dettagli della rete aziendale** (IP, nomi server, software installato)
- **Numeri di identificazione** (codice cliente, numero dipendente, badge ID)

Profili bersaglio e leve psicologiche

Abbiamo diverse categorie di persone a cui si vuole rivolgere l'attacco. Di seguito ne elenco un paio:

Persona A – Impiegato IT junior (22-35 anni): possiede accesso ai sistemi, scarsa esperienza → leva: **autorità** ("sono dal team di sicurezza centrale") e **curiosità tecnica** ("abbiamo rilevato anomalie sul tuo account").

Persona B – Responsabile amministrativo (40-60 anni): gestisce risorse aziendali, alta fiducia nell'autorità → leva: **urgenza** ("situazione critica") e **conformità** ("è richiesto per compliance").

Cognitive triggers:

- Urgenza ("entro oggi")
- Autorità ("sono dal reparto Sicurezza IT")
- Reciprocità ("ti aiutiamo, aiuta anche tu")
- Coerenza ("è una procedura standard")
- Simpatia ("abbiamo lavorato insieme prima")
- Scarsità ("accesso limitato a questa finestra")

Catena d'attacco e mappatura

Di seguito definisco i passaggi della catena di attacco:

Ricerca preliminare (OSINT) – raccogliere nomi, numeri telefonici, struttura IT tramite LinkedIn, siti aziendali, comunicati stampa.

Preparazione – creare email "spoofata" con dominio look-alike (`techvision-support[.]it` invece di `techvision.it`); procurarsi numero telefonico simile.

Contatto iniziale – email o telefonata: "Ciao, sono Marco del team Sicurezza, abbiamo rilevato una possibile violazione sul tuo account".

Costruzione della fiducia – menzionare dettagli reali (nome azienda, ultimi progetti, nomi di colleghi); stabilire rapporto amichevole.

Estrazione dati – chiedere credenziali con pretesto di "verifica", link malevoli di "reset password", accesso remoto tramite TeamViewer/AnyDesk.

Abuso – utilizzo credenziali per accesso laterale, installazione backdoor, exfiltrazione dati.

Perché la comunicazione risulta (apparentemente) credibile

Capiremo quali sono gli elementi che rendono credibile il contatto:

Linguaggio tecnico ma accessibile – uso di terminologia IT (token, SSO, anomalia di login) senza eccessiva complessità.

Dettagli contestuali specifici – riferimenti a progetti aziendali reali, nomi di colleghi, struttura del reparto IT.

Urgenza motivata – "abbiamo rilevato un accesso da IP sconosciuto ieri alle 18:42", dati precisi che sembrano estratti da log reali.

Identificazione strutturata – badge virtuale (numero ticket, codice caso, firma formale con recapiti interni).

Coerenza multicanale – contatto via email e poi telefonata, oppure link che rimanda a portale "interno" con branding aziendale.

Appello all'orgoglio professionale – "so che sei esperto di sicurezza, potremmo usare il tuo aiuto per verificare qualcosa".

Campanelli d'allarme

Vediamo quali potrebbero essere i campanelli d'allarme su cui concentrarsi per non cedere alla truffa:

Mittente email non coincide con dominio ufficiale

- Email: `m.rossi@techvision-support[.]it` (dominio secondario sospetto)
- È importante verificare il **dominio esatto** negli header email. Contattare sempre il numero ufficiale in azienda, non quello fornito dall'email.

Richiesta di credenziali via email o telefono

- Nessun team legittimo di IT chiede password via email, chat o telefonata.
- Le aziende serie utilizzano **portali di reset autenticati** o MFA.

Pressione temporale e minacce

- "Devo fare questa verifica entro 2 ore" oppure "il tuo account sarà disabilitato domani".
- Gli attaccanti creano urgenza per bypassare il pensiero critico.

Link abbreviati o domini look-alike

- Link come `hxxps://techvision-support[.]it/verify/login` (simile ma non identico a `techvision.it`).
- Usare un tool come **VirusTotal** (`https://www.virustotal.com`) per verificare URL sospetti.

Mancanza di verifica a doppio canale

- Se ricevi email di IT, contatta direttamente il numero della compagnia (non quello in email).
- Chiedi il numero di caso o ticket e verifica tramite canale ufficiale (Intranet, email ufficiale).

Errori linguistici o stilistici

- Errori grammaticali, formattazione incoerente, font strani.
- Le comunicazioni aziendali serie mantengono standard stilistici uniformi.

Richiesta di accesso remoto

- Offerte di "condividere lo schermo" tramite TeamViewer, AnyDesk o strumenti non approvati.
- Aziende serie usano strumenti MDM e agent ufficiali, non sharing temporanei.

Informazioni generiche spaciate per specifiche

- "Ultimi accessi: ieri" (generico) vs. "Ultimi accessi: ieri 14:23 da IP 192.168.1.100 con Windows 11" (specifico ma comunque verificabile).
- Chiedere sempre dettagli che solo tu conosci per confermare identità.

Esempio di Email

Contenuto:

```
**Oggetto:** [AZIONE RICHIESTA] Verifica urgente del profilo aziendale

**Da:** "TechVision Support" <support@techvision-secure-check.com>

**A:** <nome.cognome@azienda.it>

Gentile Utente,

abbiamo rilevato **differenti tentativi di accesso non autorizzato** al suo profilo aziendale. Per evitare **importanti malfunzionamenti**, è necessario completare una rapida procedura di verifica.

Clicchi sul seguente pulsante per confermare la sua identità e aggiornare le impostazioni di sicurezza:

[Verifica immediata del profilo]

https://techvision-secure-check[.]com/login/verify

Se non completata la verifica entro 30 minuti, il suo accesso potrebbe essere limitato.

Cordiali saluti,

Reparto Sicurezza – TechVision Solutions
```

Analisi tecnica (cosa controllare)

Analizziamo nel dettaglio gli indicatori tecnici di un contatto sospetto:

Analisi header email – Verificare:

- SPF (Sender Policy Framework): fallito? → email spoofata
- DKIM (DomainKeys Identified Mail): fallito? → alterazione in transito
- DMARC (Domain-based Message Authentication): fallito? → probabile frode

URL intelligence – Controllare:

- Whois del dominio: registrato pochi giorni fa?
- Certificato TLS: autofirmato o di provider sconosciuto?
- Reputazione su **VirusTotal** o **URLhaus**: segnalata come malevola?

Analisi della pagina clone – Cercare:

- CSS/loghi discordanti dal sito ufficiale
- Assenza di link Privacy/Terms coerenti
- Form che non usa HTTPS o certificato self-signed

Analisi della chiamata – Segnali di rischio:

- Numero nascosto (caller ID nullo)
- Numero "simile" ma con qualche cifra diversa
- Rumore di fondo incoerente o strano

Difese e contromisure

Cosa possiamo fare per difenderci?

Utente finale:

Regola 30-10-5:

- Fermati per **30 secondi** e respira.
- Verifica **10 dettagli**: mittente esatto, dominio, link reali (hover del mouse), errori di impaginazione, urgenza sospetta.
- Cerca **5 conferme**: chiama numero dal sito ufficiale, vai personalmente sul portale aziendale, consulta intranet, parla con il team IT di persona, verifica col responsabile diretto.

Protocollo di contatto:

- Se ricevi email IT sospetta, **chiama** il numero della compagnia (quello dal sito/badge) prima di cliccare link.
- Non usare numeri forniti nell'email.

Mai fornire:

- Password e username

- Token, codici 2FA, OTP
- Numeri di badge, tessere, identificativi
- Accesso remoto non autorizzato

VirusTotal e URLhaus:

- Copia URL sospetti in VirusTotal per scansione da 70+ motori.

Team IT/SOC (Security Operations Center):

Controlli email:

- SPF/DKIM/DMARC **rigorosi** (p=reject, non p=quarantine).
- Banner **"External Email"** su tutti i messaggi da fuori organizzazione.
- Riscrittura link malevoli (safe-link gateway).
- Filtraggio allegati pericolosi (eseguibili, macro).

Controlli di accesso:

- **MFA obbligatorio** su tutti gli account.
- Monitoraggio accessi anomali (IP nuovo, orario inusuale, dispositivo sconosciuto).
- Whitelisting app VPN e remote access autorizzate.

Awareness e simulazioni:

- **Phishing simulations** mensili con metriche (tasso di click, tempo di segnalazione).
- Training obbligatorio su pretexting e social engineering (1-2 volte l'anno).
- Creazione di **culture di segnalazione** (pulsante "Report Phish" in Outlook).

Incident response:

- Protocollo di conferma per richieste sensibili (callback a numero noto).
- Quarantena e analisi forense di email sospette.
- Comunicazione trasparente agli utenti su incidenti confermati.

Checklist rapida "anti-pretexting"

Di seguito una checklist per riconoscere e respingere tentativi di pretexting:

- [ ] Il mittente è un dominio **esatto** dell'azienda o generico? (no, maiuscole strane, TLD straniero)
- [ ] Il numero di telefono coincide con quello **sul sito ufficiale**?
- [ ] Mi sta chiedendo **credenziali, token o codici 2FA**?

- [ ] C'è **urgenza ingiustificata** o minaccia di blocco?
- [ ] I **dettagli sono specifici** (data esatta, ora precisa, IP reale) oppure vaghi?
- [ ] Posso **verificare in autonomia** tramite portale ufficiale senza cliccare link in email?
- [ ] Il **linguaggio è coerente** con gli standard aziendali o sembra improvvisato?
- [ ] L'email/chiamata è **verificabile** tramite un secondo canale (telefonata diretta, intranet)?
- [ ] Ho dubbi? **Contatta il tuo responsabile IT** prima di agire.

Suggerimento

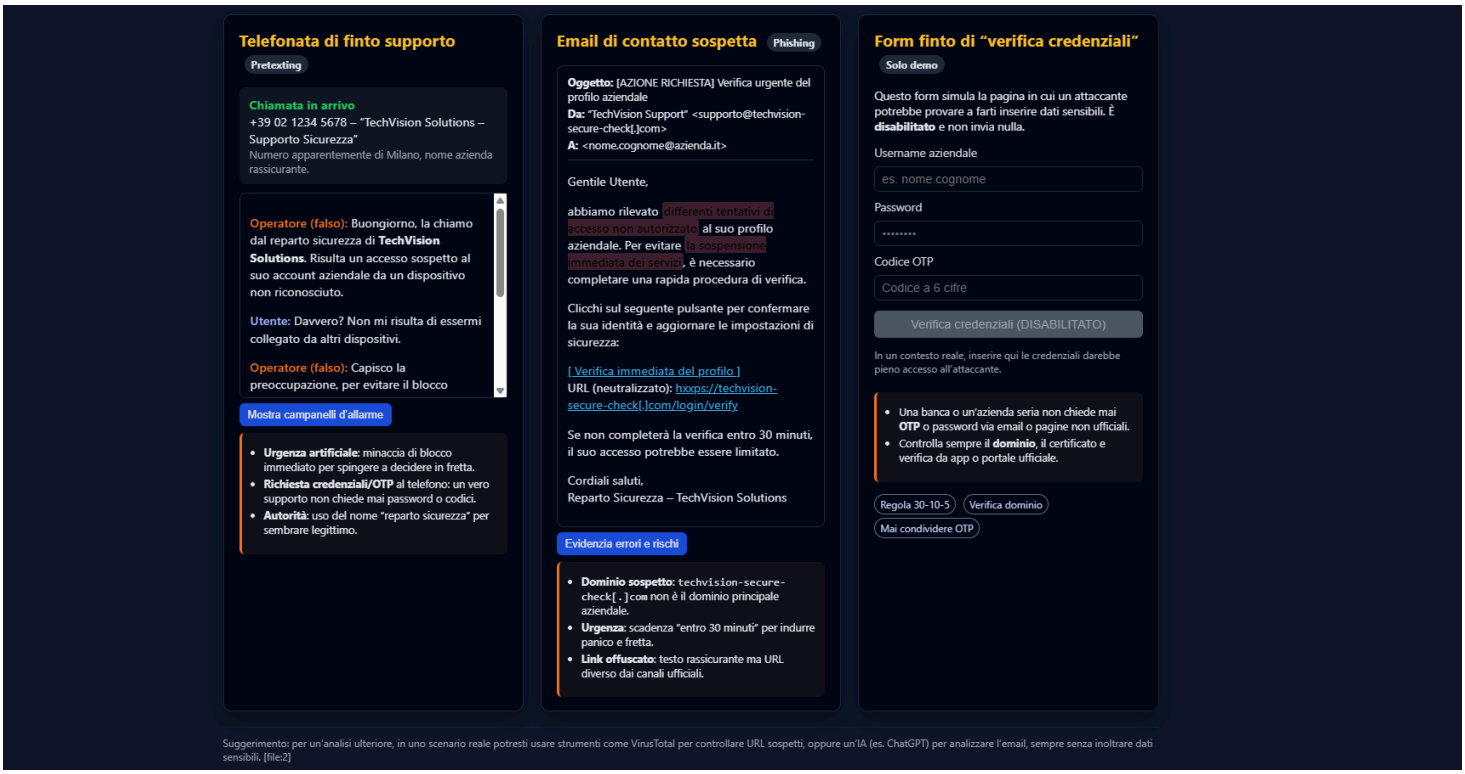
L'**Intelligenza Artificiale** può aiutare. Se ricevi un'email sospetta:

- Allega lo screenshot o il testo su **ChatGPT**, **Copilot** o strumenti simili.
- Chiedi: "È questa un'email di phishing/pretexting? Quali sono i campanelli d'allarme?"
- L'IA può riconoscere pattern di social engineering anche subtili.

Inoltre, servizi email come **Gmail** e **Outlook** hanno filtri che identificano mail malevole e le mettono in **SPAM** automaticamente. Controlla anche le cartelle di spam se non trovi un'email attesa.

Simulazione didattica

Prima di passare alle conclusioni, ho creato una piccola simulazione che può aiutare gli utenti a capire anche visivamente cosa accade realmente. Ho usato un semplice file .html per creare una pagina su un localhos. Quello che vedremo è una piccola pagina web interattiva nella quale si possono cliccare link e bottoni.



Conclusioni

Questa attività ha dimostrato come il **pretexting sia una delle tecniche più efficaci** di social engineering, proprio perché sfrutta la fiducia e la cortesia umana anziché vulnerabilità tecniche.

Un attaccante esperto non ha bisogno di firewall 0-day se riesce a convincere un dipendente a fornire credenziali di persona. Questa consapevolezza rende **l'educazione dell'utente finale** il primo strato di difesa.

La combinazione di:

- **Scetticismo costruttivo** (dubitare di richieste non verificate)
- **Protocolli chiari** (sempre verificare tramite numero ufficiale)
- **Consapevolezza tecnica** (riconoscere i campanelli d'allarme)

...trasforma gli utenti da **bersagli facili** a **sentinelle di sicurezza**.

In definitiva, la cybersecurity è una responsabilità condivisa: i tecnici creano le difese, ma gli utenti formati le mantengono vive.