

Social Engineering: Tecniche e Difese

Introduzione

L'obiettivo dell'attività è scrivere un prompt per ChatGPT che ci permetta di ottenere informazioni dettagliate sulle tecniche di social engineering e imparare come difendersi da questi tipi di attacchi.

Come prima cosa, è utile fare presente che siamo studenti di cybersecurity così da escludere il rischio che ChatGPT celi le sue informazioni. Inseriremo ovviamente dettagliate informazioni quali informazioni inserire.

Prompt: Sono uno studente di cybersecurity. Forniscimi le più importanti nozioni di Social Engineering (Principali tecniche e prevenzioni)

Risposta data:

Il social engineering è il **vettore di attacco più efficace** nel panorama della cybersecurity, responsabile del 74% dei breach gravi. A differenza degli exploit tecnici, manipola la psicologia umana per estorcere informazioni sensibili o accesso ai sistemi[2].

Fatto chiave: Danno medio per incidente: €50,000-€500,000+; Tasso di successo spear-phishing: 25-30%

1. Le 8 Principali Tecniche

1.1 Phishing & Spear-Phishing

Phishing: Email di massa che imita entità legittime. Indicatori: sender sospetto, link non corrispondenti, urgenza artificiale, richieste di credenziali.

Spear-Phishing: Attacco personalizzato mirato a individui specifici usando ricerca preliminare (LinkedIn, social media). Tasso di successo 25-30% vs 3-5% del phishing generico.

Prevenzione: Non cliccare link – accedere direttamente al sito; verificare mittente; usare filtri anti-phishing; hovering su email per controllare dominio reale.

1.2 Business Email Compromise (BEC) - "CEO Fraud"

Attacco sofisticato che compromette account executive per autorizzare trasferimenti fraudolenti. **Impatto:** €50,000-€500,000+ per incidente.

Indicatori: Richieste urgenti di trasferimenti a nuovi conti; cambio coordinate fornitori; email con tono inusuale; comunicazioni fuori orario.

Prevenzione: Dual approval per transazioni > €50,000; verificare cambio coordinate via telefono; MFA su email executive; email gateway DMARC/SPF/DKIM.

1.3 Vishing & Pretexting

Vishing (Voice Phishing): Telefono per estorcere info. "Sono IT support", "Ho rilevato virus", "Verifichiamo identità".

Pretexting: Scenario fittizio credibile per ottenere dati. "Sono HR", "Sono fornitore", "Sono collega".

Prevenzione Vishing: Mai fornire credenziali al telefono; dire "Ti richiamo al numero ufficiale"; contattare IT via canale interno.

Prevenzione Pretexting: Protocolli di verifica identità; consultare supervisore; mai condividere credenziali; training che verificare identità è positivo.

1.4 Baiting & Tailgating

Baiting: Dispositivi (USB, badge) con malware lasciati in aree pubbliche. Label attraente ("Stipendi_2026.xlsx") sfrutta curiosità umana.

Tailgating: Accesso fisico non autorizzato seguendo persona autorizzata attraverso porta sicura.

Prevenzione Baiting: Policy che vieta collegare dispositivi sconosciuti; disabilitare Autorun USB; awareness training; monitoraggio dispositivi.

Prevenzione Tailgating: Porte sempre chiuse; awareness che "non far entrare nessuno senza badge"; badging system; security guard; vestiboli con porte doppie.

1.5 Smishing

SMS phishing. "Il tuo conto è disabilitato", "Consegna bloccata" con link shortened. Alta efficacia: 98% apertura SMS vs email.

Prevenzione: Non cliccare link da SMS; ignorare urgenze; verificare numeri; usare app ufficiale della banca; segnalare alla banca.

2. Psicologia del Social Engineering

Il social engineering sfrutta 6 principi di influenza:

Principio	Esempio	Contromisura
Urgenza	"Verifica entro 24 ore o bloccato"	Urgenza legittima ha sempre canali di verifica
Autorità	"Sono il CEO, ho bisogno di..."	Verificare identità anche di figure autorevoli
Fiducia	Costruire rapporto prima di richiesta	Fiducia deve essere guadagnata
Validazione Sociale	"50 persone hanno già cliccato"	Comportamento di massa ≠ sicurezza
Reciprocità	"Ti ho aiutato, dammi il tuo badge"	Aiuto legittimo non richiede favori
Impegno/Coerenza	Piccoli step → decisioni più grandi	Consapevolezza dei piccoli step iniziali

Fattori cognitivi: Carico cognitivo (persone occupate = meno critica), pattern matching (cervello riconosce familiarità), bias cognitivi (confirmation bias), paura (bypassa pensiero critico).

3. Strategie di Prevenzione Multi-Layer

3.1 Livello Individuale

- ✓ **Email:** Non cliccare link – accedere direttamente; verificare sender; diffidare allegati
- ✓ **Password:** Password manager + MFA (TOTP vs SMS)
- ✓ **Telefono:** Mai credenziali al telefono; verificare numero ufficiale; contattare IT internamente
- ✓ **Dispositivi:** Non collegare USB sconosciuti; disabilitare Autorun; VPN su reti pubbliche
- ✓ **Reporting:** Segnalare email sospette via pulsante "Report phishing" – comportamento positivo

3.2 Livello Organizzativo

Tecnologia: Email gateway (DMARC/SPF/DKIM), filtri anti-phishing AI, EDR, SIEM, anomaly detection, MFA su executive, passwordless auth (FIDO2)

Conclusioni

Curando il proprio prompt, e' evidente che il risultato dato sia molto piu' curato.

Windows 10: Vulnerabilità CVE Critiche e Soluzioni

Prompt utilizzato

Sono uno studente di cybersecurity. potresti fornirmi una lista dei CVE relativi a windows 10? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e soluzioni consigliate

Risultato:

CVE Critiche 2024-2025

CVE-2025-62549: RRAS RCE (CVSS 8.8 - Critical)

Tipo: Use-after-free in Routing and Remote Access Service

Una vulnerabilità critica consente a un attaccante non autenticato di eseguire codice remoto. Non richiede autenticazione ed è basata su rete, con alto potenziale di worm.

Mitigazione:

- Applicare patch immediatamente
- Disabilitare RRAS: Disable-RemoteAccess
- Firewall: bloccare porte 1723, 500, 4500
- Implementare IDS/IPS rules

CVE-2025-54100: PowerShell Command Injection (CVSS 7.8)

Tipo: Improper neutralization of special elements (CWE-77)

Una vulnerabilità consente l'esecuzione di codice arbitrario localmente tramite caratteri speciali in PowerShell. Richiede interazione dell'utente.

Mitigazione:

1. Applicare aggiornamento dicembre 2025

2. Restrizioni PowerShell Execution Policy
 3. Windows Defender Application Guard
 4. Script block logging per il monitoraggio
-

CVE-2025-55234: SMB Relay Attack (CVSS 8.8)

Tipo: NTLM relay sulla negoziazione SMB

Consente impersonazione di utenti e escalation di privilegi attraverso relay attack sulla rete interna.

Mitigazione:

- Abilitare SMB signing (RequireSecuritySignature \$true)
 - Implementare Extended Protection for Authentication
 - MFA per accesso remoto
 - Monitorare con Windows Defender for Identity
-

CVE-2025-24990: Driver Privilege Escalation (CVSS 8.8 - Active Exploitation)

Tipo: Privilege escalation in driver universale Windows

Una vulnerabilità in driver Windows consente escalation a livello SYSTEM localmente. Attivamente sfruttata dal 4 novembre 2025.

Mitigazione:

- Patch entro gennaio 2026 (scadenza CISA)
 - Implementare Driver Block List (DBL)
 - Virtualization-based Security (VBS)
 - Auditi regolari di driver non firmati
-

CVE-2024-43461: MSHTML Spoofing (CVSS 8.8)

Tipo: Spoofing in MSHTML

Vulnerabilità di spoofing che inganna gli utenti sull'origine di contenuti web, utilizzabile per phishing sofisticato.

Mitigazione:

- Aggiornare Microsoft Edge
 - Forzare HTTPS
 - Web filtering aziendali
 - Educare sulla verifica URL
-

Best Practices per la Sicurezza

Piano di Patching

1. **Prioritizzazione:** CVSS ≥ 8.0 e sistemi esposti a rete entro 30 giorni
2. **Testing:** Ambiente di staging prima della distribuzione
3. **Distribuzione:** WSUS, Intune o Microsoft Update
4. **Verifica:** Confermare installazione con audit

Strumenti Essenziali

- Windows Update for Business - Gestione centralizzata
- Microsoft WSUS - Enterprise patch management
- Microsoft Intune - Conformità dispositivi
- Windows Defender / Defender for Endpoint - Protezione in tempo reale
- Nessus/Qualys - Vulnerability scanning periodico

Monitoraggio Continuo

- Event Viewer per registrazione attacchi
- SIEM per analisi correlata
- Monitoraggio modifiche driver di sistema
- Analisi log PowerShell
- EDR per rilevamento comportamentale