

Report esercizio S5-L4

Domanda fatta a chatgpt:

“Ciao chatgpt, essendo che sto facendo un corso sulla cybersecurity volevo chiederti se potevi farmi una panoramica dettagliata su "tecniche di social engineering e imparare come difendersi da questi tipi di attacchi". Inoltre mi suggerisci strategie e migliori pratiche per difendersi dagli attacchi di social engineering”?

Bonus: potresti fornirmi una lista dei CVE relativi a Wordpress? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate.”

Risposta di chatGPT

Tecniche di social engineering (panoramica pratica)

Obiettivi degli attaccanti: farti compiere un’azione (clic, download, trasferimento denaro, rivelare credenziali/codici) facendo leva su fiducia, urgenza, autorità, curiosità o paura. Le campagne più comuni rientrano nelle tecniche “Phishing” dell’ATT&CK di MITRE (T1566 e correlate) e varianti OSINT/social.

Tecniche più usate:

- **Email phishing / spear-phishing:** messaggi credibili (spoof del mittente, thread hijacking) con link o allegati malevoli; spesso imitano IT interno, banche, corrieri, HR.
- **Smishing & vishing:** SMS o telefonate che spingono a rivelare OTP o a visitare siti clone; sempre più realistici grazie a AI/voice cloning.
- **Consent & OAuth phishing:** pagine di “consenso app” che ti fanno autorizzare accessi (niente password, ma token).
- **MFA fatigue / push bombing:** ondate di notifiche MFA finché la vittima “accetta”; spesso combinato con SIM-swap.
- **Pretexting & imposture:** finti colleghi/fornitori/tecnici (anche su LinkedIn/Teams) che chiedono dati o “convalide”.
- **Quid-pro-quo / baiting:** offerte (accessi, carte regalo, file “documenti_paga.zip”) per indurre download o contatti.
- **Tailgating & drop di dispositivi:** ingresso fisico dietro dipendenti o chiavette “perdute” con malware.
- **Phishing per informazioni (T1598):** sondaggi, form o DM che estraggono dati “innocui” poi usati per attacchi mirati.

Come difendersi (strategie, processi e best practice)

1) Persone (abitudini e formazione)

- **Formazione continua e realistica:** simulazioni di phishing con debrief; includi casi di vishing/smishing, thread hijacking e MFA fatigue. Linee guida e poster aiutano l’“igiene comportamentale”.
- **Regola dell’“interruzione”:** davanti a urgenza/autorità → fermati, verifica su canale *indipendente* (numero ufficiale, chat interna separata).
- **“Zero shame” policy:** nessuna colpevolizzazione; segnalazione immediata = migliore difesa.

2) Processi

- **Playbook di risposta al phishing:** come segnalare, isolare allegati/link, resettare sessioni, invalidare token OAuth, forzare MFA reset.
- **Verifiche “fuori banda” per pagamenti/anagrafiche fornitori:** doppia approvazione e call back su numeri noti (non quelli nell'email).
- **Gestione identità forte:** password manager + MFA *resistente al phishing* (FIDO2/passkey) dove possibile.
- **Principio del minimo privilegio:** riduci superficie di abuso di account “Contributor/Editor” su CMS come WordPress.

3) Tecnologie

- **Protezione email & web:** SPF/DKIM/DMARC corretti; banner “esterno”, sandbox allegati, blocco macros, DNS filtrato.
- **Hardening SaaS/IdP:** disabilita legacy auth, sessioni corte e alert su login anomali; controlli rischi OAuth.
- **MFA anti-fatigue:** limiti ai prompt, numeri di abbinamento, o passkey. Monitor su push anomale.
- **EDR + telemetry:** per allegati cliccati, beaconing, esecuzioni script, anomalie creazioni di utenti admin. Allinea controlli alla matrice MITRE ATT&CK.
- **Protezione social:** policy account “verificati”, privacy stretta, attenzione a link in DM e a “verifiche” su HR/recruiting.

Nota trend

L'uso dell'AI rende messaggi/voce molto più convincenti: alza la soglia di scetticismo e automatizza controlli (DMARC, sandbox, EDR).

CVE e vulnerabilità WordPress (selezione aggiornata + rimedi)

Fonti principali: database WPScan, NVD e bollettini WordPress/ricercatori. Tieni aggiornata la tua istanza e limita plugin/temi al minimo indispensabile.

Core WordPress

WordPress 6.6.2 – aggiornamento di manutenzione/bugfix; la discussione comunitaria cita una **CVE a bassa severità** riconosciuta ma poco sfruttabile; in generale: **mantieni sempre l'ultima minor**.

Plugin (casi recenti e impattanti)

TI WooCommerce Wishlist – CVE-2024-43917: SQL Injection non autenticata ($\leq 2.8.2$); patch $\rightarrow \geq 2.9.0$; rischio esfiltrazione DB. Mitigazione: aggiorna subito o disattiva; WAF regole SQLi.

- **Elementor Website Builder**
 - **CVE-2024-5416: Stored XSS** ($\leq 3.23.4$); patch successive pubblicate. Limita ruoli “Contributor”, sanitizza input, aggiorna a versione $\geq 3.24+$ (o più recente).
 - **CVE-2024-6757: Exposure informazioni** via get_image_alt ($\leq 3.23.5$). Mitigazione: aggiornare; rivedere permessi bozza/privati.
 - **CVE-2024-8494** (Elementor Pro $\leq 3.25.10$): **leak contenuti** tramite shortcode elementor-template per utenti con permessi Contributor+. Patch parziale in 3.24.4, aggiornare a **versione più recente**.
 - **CVE-2024-50555** (famiglia XSS Contributor+): aggiornare $< 3.29.1 \rightarrow \geq 3.29.1$.
- **WooCommerce Customers Manager – CVE-2024-0399: SQLi post-autenticazione** (v29.4). Mitigazione: aggiornare alla versione corretta del vendor; monitora query anomale.
- **Kadence Blocks (Gutenberg Blocks with AI) – CVE-2024-9655: Stored XSS** ($\leq 6.6.2$). Aggiorna plugin; limita ruoli e revisione contenuti.
- **WP SMS** – CSRF ($\leq 6.6.2$) \rightarrow possibili cambi di configurazione se l'admin visita pagina trappola. Mitigazione: aggiorna, forza nonce, usa estensioni anti-CSRF/isolamento browser.
- **WP File Manager** – storico **RCE non autenticata** (2020) + problemi recenti (traversal/exposure). Anche se datato, è un caso-scuola: **se non serve, rimuovere**.

Temi

Alone – Charity Theme – CVE-2025-4394: upload arbitrario \rightarrow RCE/takeover ($\leq 7.8.3$), patch in **7.8.5** (16 giu 2025). Aggiornare *immediatamente*; rimuovere backdoor, ruotare credenziali.

Checklist di mitigazione per WordPress

- **Aggiorna** core, plugin, temi; abilita **auto-update** dove possibile.
- **Riduci** plugin/temi al minimo; rimuovi quelli inattivi.
- **Ruoli & capability minime** (Contributor/Editor solo se necessario).
- WAF / protezione applicativa** con regole per SQLi/XSS e upload; blocco di *.php in /uploads.
- **-Backup e staging:** prova aggiornamenti su staging; backup verificati.
- **Inventario CVE:** monitora WPScan/NVD per gli elementi installati.

Riepilogo

Titolo: Tecniche di Social Engineering e Difese – con Focus su Vulnerabilità WordPress

Data: 23 ottobre 2025

1. Riepilogo esecutivo

Gli attaccanti sfruttano la componente umana (phishing email/SMS/voce, pretexting, MFA fatigue) per ottenere accessi o esfiltrare dati.

L'AI aumenta verosimiglianza e volume degli attacchi. Difese efficaci combinano formazione continua, processi anti-frodi (verifiche fuori banda, playbook) e controlli tecnici (DMARC, sandbox allegati, MFA FIDO2/passkey, EDR). Nel perimetro WordPress, il rischio principale è legato a plugin/temi terzi: aggiornamento, minimo privilegio e WAF sono fondamentali.

2. Tecniche chiave di social engineering

Phishing (T1566), smishing, vishing, pretexting, MFA fatigue, OAuth consent phishing, baiting/tailgating, phishing per informazioni (T1598). Indicatori tipici: urgenza/autorità, link accorciati, domini simili, richieste di OTP.

3. Difese e migliori pratiche

- Formazione periodica con simulazioni e cultura “zero shame”.
- Policy pagamenti/fornitori con doppia verifica fuori banda.
- Password manager + MFA resistente al phishing; disabilitare legacy auth.
- Email security (SPF/DKIM/DMARC), sandbox allegati, filtro DNS.
- EDR/telemetria, hardening SaaS/IdP, revisione permessi WordPress.

4. WordPress – CVE selezionate (2024-2025) & mitigazioni

- **CVE-2024-43917** – TI WooCommerce Wishlist (SQLi non autenticata): aggiornare $\geq 2.9.0$; WAF.
- **CVE-2024-5416 / 6757 / 8494 / 50555** – Elementor (XSS/InfoLeak): aggiornare a versioni correnti; ridurre ruoli Contributor; audit contenuti.
- **CVE-2024-0399** – WooCommerce Customers Manager (SQLi autenticata): aggiornare; monitor query.
- **CVE-2024-9655** – Kadence Blocks (Stored XSS): aggiornare; limitare ruoli.
- **CVE-2025-4394** – Tema Alone (upload arbitrario \rightarrow RCE): aggiornare $\geq 7.8.5$; bonifica e rotazione credenziali.
- **Storico:** WP File Manager – RCE (2020) + altri bug: rimuovere se non necessario.

5. Raccomandazioni operative

1. **Inventario WordPress** (plugin/temi attivi) + confronto con WPScan/NVD settimanale.
2. **Auto-update** per core/estensioni critiche; staging per siti business-critical.
3. **WAF** con regole per SQLi/XSS e blocco esecuzione PHP in /uploads.
4. **Runbook phishing** (chi fa cosa entro 15 minuti dalla segnalazione).
5. **Passkey/MFA phishing-resistant** per admin e autori.