Guida per mettere in sicurezza il tuo sito

Christian Cantinelli - 2025-10-15 - Supporto Tecnico

Per aiutarti a gestire al meglio una possibile compromissione e prevenire ulteriori problemi di sicurezza, segui i passaggi indicati di seguito.

1. Metti subito in sicurezza il sito

- Sospendi temporaneamente l'accesso al sito se noti comportamenti anomali (ad esempio redirect, popup o contenuti sconosciuti).
  Puoi farlo inserendo in testa al file `.htaccess` le seguenti righe per consentire l'accesso solo dal tuo indirizzo IP:

  ```
  Deny from all
  Allow from TUO_IP
  ```

  Sostituisci `TUO_IP` con il tuo indirizzo IP pubblico (puoi trovarlo facilmente da questa pagina).

- Cambia tutte le password, in particolare:
  - Accesso al CMS (WordPress, Joomla, Prestashop, ecc.)
  - Accesso FTP o File Manager
  - Accesso al pannello di controllo (cPanel o Plesk)
  - Accesso al database (ricordati di aggiornare anche il file di configurazione del sito con la nuova password)

2. Controlla e rimuovi i file segnalati

- Accedi al tuo pannello **cPanel** e vai in **Sicurezza → Quarantena Malware** per visualizzare i file individuati dalle scansioni automatiche.
- Puoi anche eseguire una **scansione manuale** da **cPanel → Programma antivirus**.
- Esamina i file segnalati:
  - Rimuovi quelli che non riconosci o che contengono codice sospetto.
  - Se disponibili, confrontali con una versione pulita del file (ad esempio da un backup o dal pacchetto originale del CMS, tema o plugin).
- Se hai un backup precedente all'infezione, valuta di ripristinarlo.
- In caso di dubbi, apri un ticket di assistenza per una verifica tecnica.

3. Aggiorna e proteggi il CMS

- **Aggiorna** subito il CMS, i temi e i plugin all'ultima versione disponibile.
- Rimuovi temi o plugin non utilizzati o non più supportati.
- Installa un plugin di sicurezza per il tuo CMS (ad esempio Wordfence o iThemes Security per WordPress).
- Verifica che non siano presenti utenti amministratori sconosciuti.

4. Prevenzione continua

- Controlla periodicamente i log di accesso **amministrativo** del CMS per verificare eventuali tentativi di accesso sospetti.
- Su **cPanel** puoi abilitare la **protezione a due fattori (2FA)** per aumentare la sicurezza del tuo account: Guida per attivare la protezione 2FA su cPanel »
- Mantieni sempre aggiornato il CMS e le sue estensioni.