WORDPRESS SECURITY CHECKLIST

for Site Owners, Admins & Developers

Protect your site from the most common WordPress threats.
Follow this list weekly and monthly to stay secure.

How to Use This Checklist

1. **Run weekly** → Complete all site-owner and admin actions.
2. **Run monthly** → Review backups, roles, and deeper security settings.
3. **Log results** → Record updates, scans, and backup tests.
4. **Stay consistent** → Security improves through routine checks.

Difficult Key

- Easy = Site owner/admin settings or plugins
- Intermediate = Developer knowledge
- Advanced = Hosting/provider

Client-Side Actions (Site Owners, Admins & Developers)

Weekly Actions

- [ ] **Update WordPress, plugins, themes**
  → Patches known vulnerabilities, preventing XSS, SQL Injection.
- [ ] **Enable 2FA for all admins/editors**
  → Blocks brute force attacks & credential stuffing.
- [ ] **Use strong, unique passwords**
  → Prevents account takeovers.
- [ ] **Limit login attempts**
  → Stops brute force bots.
- [ ] **Run a malware scan with a plugin**
  → Detects infections early.
- [ ] **Check SSL certificate validity**
  → Keeps connections encrypted and prevents browser warnings.
- [ ] **Avoid or disable file manager plugins after use**
  → Reduces risk of backdoors or file injection attacks.

Remember: A few small steps each week protect your site from most attacks.

Published by PRESSIDIUM®

Monthly / As Needed

- [ ] **Test backups by restoring a copy**
  → Ensures recovery works after attacks.
- [ ] **Review user roles & permissions**
  → Reduces risk of privilege escalation.
- [ ] **Ensure secure file permissions**
  → Prevents unauthorized access to sensitive files.
- [ ] **Disable XML-RPC (if unused)**
  → Reduces exposure to brute-force amplification and unauthorized access.
- [ ] **Add/update security headers (CSP, HSTS, X-Frame-Options)**
  → Protects against XSS, CSRF.
- [ ] **Disable file editing in wp-admin**
  → Reduces backdoor and malware risk.
- [ ] **Validate/sanitize inputs (custom code)**
  → Prevents SQL injections and XSS.
- [ ] **Use nonces in forms and AJAX**
  → Prevents CSRF.

Track These Security Signals

- Failed login attempts (spikes mean brute-force activity).
- Malware scan results.
- File integrity changes.
- SSL certificate expiry date.
- Uptime or downtime alerts.
- Unusual CPU or bandwidth usage.

Pro Tips:

- Test restoring a backup monthly.
- Remove inactive plugins and themes.
- Keep an emergency contact list for your host.
- Apply updates right away. Most attacks exploit known vulnerabilities.

Published by PRESSIDIUM®