Tab 1

✅ 2025 WordPress Security Checklist

Protect your site in 15 minutes or less

🔐 1. Secure Your Login Page

☐ Enable **Two-Factor Authentication (2FA)**
☐ Change your default login URL (e.g., from /wp-login.php)
☐ Limit login attempts (use plugins like Limit Login Attempts Reloaded)
☐ Disable XML-RPC if not in use (can be done via plugin or .htaccess)
☐ Require strong passwords for all users

🛡️ 2. Install a WordPress Security Plugin

☐ Choose and activate ONE comprehensive plugin:

- 🔹 Wordfence Security
- 🔹 iThemes Security
- 🔹 Sucuri Security
- 🔹 MalCare

☐ Enable features like:

- Real-time firewall
- Malware scanning
- File integrity monitoring
- Login attempt alerts

📦 3. Keep WordPress Software Up to Date

☐ Update WordPress core (enable auto-updates for minor versions)
☐ Update all plugins and themes regularly
☐ Remove unused or inactive plugins and themes
☐ Monitor for vulnerable or abandoned plugins via tools like Patchstack

---

🌐 4. Secure Your Hosting & Server

☐ Use a **reputable managed WordPress hosting** provider (e.g., Kinsta, WP Engine, Cloudways)
☐ Enable **SSL/HTTPS** (install free SSL via Let's Encrypt)
☐ Run PHP 8.1+ and keep server software updated
☐ Ensure your host provides:

- Daily offsite backups
- Built-in WAF (Web Application Firewall)
- Malware removal support

🧾 5. Use Proper User Roles & Permissions

☐ Audit your users: remove unused or suspicious accounts
☐ Apply **least privilege** rule (no "Admin" access unless absolutely needed)
☐ Use a plugin like "User Role Editor" to fine-tune permissions
☐ Disable user registration if not needed

🔁 6. Automated Backups

☐ Set up **daily backups** using:

- 🔹 UpdraftPlus
- 🔹 BlogVault
- 🔹 Jetpack Backup

☐ Store backups **offsite** (e.g., Google Drive, Dropbox, Amazon S3)

☐ Test restoring a backup at least once per quarter

🚨 7. Harden WordPress Configuration

☐ Disable file editing via wp-config.php:

```php
define('DISALLOW_FILE_EDIT', true);
```

define('DISALLOW_FILE_EDIT', true);

☐ Hide your WordPress version number
☐ Use secure file permissions:

- wp-config.php = 400 or 440
- wp-content = 755

☐ Disable directory browsing via .htaccess:

```apache
Options -Indexes
```

🔎 8. Monitor & Respond to Threats

☐ Enable email alerts for:

- Failed logins
- Plugin/theme changes

- Suspicious file changes

☐ Scan your site for malware weekly
☐ Use a free scanner like Sucuri SiteCheck (https://sitecheck.sucuri.net)
☐ Subscribe to plugin vulnerability alerts (Wordfence, Patchstack)

🔮 Bonus: Advanced Optional Steps

☐ Implement **Content Security Policy (CSP)** headers
☐ Enable **Geo-blocking** if your site only targets specific countries
☐ Use a CDN with built-in WAF (e.g., Cloudflare Pro)
☐ Consider AI-driven threat monitoring (MalCare AI, Wordfence AI)

🎯 Final Tip

You don't need to do everything at once. Start with:
✅ Login security
✅ Updates
✅ Backups
✅ A trusted security plugin

The rest can be built over time for **layered, long-term protection**.

Reach me through info@techsupport.solutions for professional collaboration and WordPress Management services.