LiteSpeed Hosting Security Hardening Checklist

1. Lock Down Your Account

- Use strong passwords (16+ random characters) for cPanel, FTP/SFTP, and CMS admin.
- Enable Two-Factor Authentication (2FA) for cPanel and CMS.
- Disable unused accounts, including old FTP users and unused email addresses.

2. Harden WordPress / CMS

- Keep CMS core, themes, and plugins updated.
- Delete unused plugins/themes to reduce attack surface.
- Install a security plugin (Wordfence, iThemes Security, All-In-One WP Security).
- Set file permissions: Files → 644, Directories → 755, wp-config.php → 600.

3. Use LiteSpeed's Built-In Security

- Enable ModSecurity WAF in cPanel (use OWASP or Comodo rules).
- Enable reCAPTCHA for login and comment forms.
- Set connection limits and request throttling if available.

4. Malware & Vulnerability Scanning

- Enable Imunify360 or ClamAV scanner in cPanel.
- Schedule daily automatic scans and email alerts.
- Use Sucuri SiteCheck weekly for external verification.

5. Prevent Cross-Site Contamination

- Use separate cPanel accounts for unrelated sites.
- Store backups off-server (Google Drive, Dropbox, local storage).
- Add a 'canary' file in your root directory to detect tampering.

6. SSL/TLS & Traffic Security

- Force HTTPS via .htaccess or cPanel Force SSL.
- Enable HTTP/2 or QUIC in LiteSpeed settings.
- Add HSTS in .htaccess: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"

7. Ongoing Monitoring

- Check Google Search Console Security Issues weekly.
- Monitor server IP reputation via MXToolbox.
- Set up uptime and security alerts via UptimeRobot or Better Uptime.