

How to Lock Down Your WordPress Site After a Security Breach

By Dave | Sunshine Coast Web Design

Recently, we dealt with a serious WordPress security breach where attackers repeatedly gained access to a client's site, deactivated security plugins, and created backdoor admin accounts. Here's exactly what we learned and how to secure your WordPress site after an attack.

The Warning Signs

If you're experiencing any of these, you may have been compromised:

- Unknown admin users appearing in your user list
- Security plugins being mysteriously deactivated
- Unfamiliar plugins installed on your site
- Suspicious login activity from foreign countries
- Files modified that you didn't touch

Immediate Response: The First 24 Hours

Step 1: Run Complete Security Scans

Don't skip this step. You need to find the backdoor before anything else.

Run multiple layers of scanning:

1. WordPress Security Plugin Scan

- Run a full Wordfence scan (or your security plugin of choice)
- This catches most common malware and backdoors

2. Hosting Provider Malware Scanner (Critical!)

- Contact your hosting provider and request a server-side malware scan
- Most quality hosts offer tools like Imunify360, SiteLock, or similar
- These detect files that WordPress-level scanners might miss
- **At Sunshine Coast Web Design, we run weekly malware scans on all client sites as standard practice**

3. Manual File Inspection

- Check for backdoor files, especially in `/wp-content/uploads/` (should contain NO .php files)

- Look for recently modified files (check dates against when attacks occurred)
- Review file permissions for anomalies

What to look for:

- PHP files in your uploads directory
- Suspicious plugins you didn't install
- Modified core WordPress files
- Hidden users in the database
- Files with suspicious names or obfuscated code
- Recently created files during the attack timeframe

Step 2: Delete Malicious Users Immediately

Go to **Users** → **All Users** and look for:

- Users you didn't create
- Users with random usernames like "admin1backup" or similar
- Recently created admin accounts

Delete them immediately. Don't just change their role – delete them completely.

Step 3: Take the Site Offline (If Severe)

If the attack is ongoing, consider:

- Enabling maintenance mode
- Password-protecting the site via .htaccess or cPanel
- This gives you time to clean and secure without ongoing interference

The Core Security Hardening Steps

1. Change ALL Passwords (Non-Negotiable)

Change these passwords immediately, in this order:

WordPress Admin Passwords:

- Every admin account
- Use 20+ characters
- Mix uppercase, lowercase, numbers, symbols
- Make them unique (never reuse passwords)

cPanel/Hosting Password:

- Attackers may have gained hosting access
- This is often overlooked but critical

FTP/SFTP Password:

- They may have uploaded files via FTP
- Change this to cut off that access route

Database Password (Advanced): This requires updating two places:

1. Your hosting control panel (cPanel → MySQL Databases)
2. Your `wp-config.php` file (must match exactly)

Note: If you're not comfortable with this, ask your hosting provider to do it.

2. Change WordPress Security Keys

This is **critically important** and often forgotten.

What it does:

- Logs out ALL users immediately (including hidden attacker sessions)
- Invalidates all existing login cookies
- Forces everyone to log back in fresh

How to do it:

1. Go to <https://api.wordpress.org/secret-key/1.1/salt/>
2. Copy the generated keys
3. Access your site via FTP or cPanel File Manager
4. Edit `wp-config.php`
5. Find the section with AUTH_KEY, SECURE_AUTH_KEY, LOGGED_IN_KEY, etc.
6. Replace ALL those lines with your new keys
7. Save the file

This won't break anything – it just logs everyone out temporarily.

3. Enable Two-Factor Authentication (Your Strongest Defense)

This is the **single most important security measure** you can implement.

Even if attackers have your password, 2FA stops them cold.

In Wordfence:

- Go to Wordfence → Login Security → Two-Factor Authentication
- Enable it for ALL admin accounts
- Use an authenticator app (Google Authenticator, Authy, etc.)

This makes your site exponentially more secure.

4. Block Attacker IP Addresses

Check your security logs for successful login attempts (usually marked as "200" response codes).

In Wordfence:

- Wordfence → Firewall → Blocking
- Add the attacker IP addresses to your block list
- Look for patterns (IPs that logged in successfully during suspicious times)

5. Enable Country Blocking

If your business only operates in Australia, there's no reason to allow login attempts from Iran, Russia, or China.

In Wordfence:

- Wordfence → Firewall → Blocking → Country Blocking
- Block countries you don't need access from
- Keep Australia and any countries where you have legitimate users

Exception: If you use international booking systems or services, check their IP locations first.

6. Protect or Disable xmlrpc.php

The `xmlrpc.php` file is a legacy WordPress API that's constantly attacked. It allows unlimited login attempts and DDoS amplification.

Do you need it?

- Only if you use mobile apps to post
- Only if you use Jetpack or remote publishing tools
- Most sites don't need it

To disable it:

- Wordfence → Firewall → Firewall Options → Disable XML-RPC
- Or use the "Disable XML-RPC" plugin
- Or add this to your `.htaccess` file:

```
apache
```

```
# Block xmlrpc.php
<Files xmlrpc.php>
order deny,allow
deny from all
</Files>
```

7. Update Everything

Outdated software is a common entry point.

Update immediately:

- WordPress core
- All plugins
- All themes
- PHP version (via cPanel, if outdated)

In our case, the attackers actually updated WordPress themselves – a sign they had deep access.

8. Disable File Editing

Prevent attackers from editing theme/plugin files through the WordPress dashboard.

Add this to your `wp-config.php`:

```
php

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

9. Set Proper File Permissions

Incorrect file permissions can allow unauthorized modifications.

Recommended permissions:

- Folders: 755
- Files: 644
- wp-config.php: 440 or 400

You can set these via FTP or cPanel File Manager.

10. Review and Remove Suspicious Plugins/Themes

Check your **Plugins** → **Installed Plugins** list:

- Any plugins you don't recognize?

- Any installed during the attack timeframe?
- Any with suspicious names?

Deactivate and delete them immediately.

Do the same for **Appearance** → **Themes**.

Advanced Protection Measures

Enable Wordfence Firewall

- Wordfence → Firewall
- Enable "Extended Protection" mode (recommended)
- This provides real-time protection against threats

Limit Login Attempts

Wordfence does this automatically, but verify:

- Maximum 3-5 login attempts
- Longer lockout periods (15+ minutes)
- This stops brute force attacks

Enable File Integrity Monitoring

Wordfence can alert you when files change:

- Wordfence → Scan
- Enable alerts for file changes
- You'll know immediately if something is modified

Consider a Web Application Firewall (WAF)

Services like Cloudflare (free tier available) add DNS-level protection:

- DDoS protection
- IP blocking at the edge
- Caching and performance benefits

Backup Strategy

After securing your site, establish regular backups:

- **Daily or weekly automated backups** (minimum)
- Store backups off-site (not just on your server)
- Test restoration occasionally to ensure backups work

- Keep multiple backup versions (not just the most recent)

At Sunshine Coast Web Design, we run weekly backups of all client sites as part of our standard maintenance. This ensures that if a site is compromised, we can quickly restore to a clean version from before the attack occurred.

We recommend these backup solutions:

- UpdraftPlus
- BackupBuddy
- Your hosting provider's backup service
- Off-site storage (Dropbox, Google Drive, or dedicated backup services)

Monitoring Going Forward

Check These Regularly

Weekly:

- Review Wordfence security logs
- Check user list for unauthorized accounts
- Review recently modified files

Monthly:

- Update WordPress, plugins, themes
- Review and remove unused plugins
- Check file permissions

After Any Suspicious Activity:

- Run full security scan
- Review all login attempts
- Check for new admin users

Set Up Security Alerts

Configure Wordfence to email you about:

- Failed login attempts (above a threshold)
- New admin user creation
- File modifications
- Plugin/theme installations

What We Learned







From our recent incident, here are the key takeaways:

1. **2FA is non-negotiable** – It's your strongest single defense
2. **Backdoors persist** – Changing passwords alone isn't enough
3. **Attackers are persistent** – They came back multiple times over 24+ hours
4. **Session management matters** – Changing security keys is critical
5. **Monitor everything** – Security logs revealed the full attack pattern
6. **Act fast** – The longer you wait, the more damage they can do

The Bottom Line

WordPress security isn't a one-time task – it's an ongoing process. But with these measures in place, you'll be protected against 99% of attacks.

Your minimum security stack should include:  Strong, unique passwords

-  Two-Factor Authentication
 -  Security plugin (Wordfence or similar)
 -  Regular updates
 -  Country/IP blocking
 -  File integrity monitoring
 -  Regular backups
-

Need Help?

If you're dealing with a WordPress security breach and need professional help, contact us at **Sunshine Coast Web Design**. We provide:

- Emergency security response and site cleanup
- Complete malware detection and removal
- Site hardening and security audits
- **Weekly malware scanning** for all client sites
- **Weekly automated backups** as standard
- Ongoing security monitoring
- WordPress maintenance plans

Our proactive approach means most of our clients never experience a security breach. We catch and eliminate threats before they become problems.

Don't wait until you're attacked – secure your site today.

Dave / Sunshine Coast Web Design
www.sunshinecoastwebdesign.com.au

Quick Security Checklist

Print this and keep it handy:

Immediate Response:

- ☐ Run WordPress security scan (Wordfence/similar)
- ☐ Request hosting provider malware scan
- ☐ Delete malicious users
- ☐ Check for backdoor files in /wp-content/uploads/
- ☐ Review recent file modifications

Password Changes:

- ☐ All WordPress admin passwords
- ☐ cPanel/hosting password
- ☐ FTP/SFTP password
- ☐ Database password (or schedule with hosting)

Critical Security Steps:

- ☐ Change wp-config.php security keys
- ☐ Enable 2FA on ALL admin accounts
- ☐ Block attacker IP addresses
- ☐ Enable country blocking
- ☐ Disable or protect xmlrpc.php

Updates & Hardening:

- ☐ Update WordPress core
- ☐ Update all plugins
- ☐ Update all themes
- ☐ Set proper file permissions (755/644)
- ☐ Add DISALLOW_FILE_EDIT to wp-config.php

Ongoing Monitoring:

- ☐ Set up security alerts
- ☐ Schedule weekly log reviews
- ☐ Enable automated backups

☐ Test backup restoration

Stay safe out there!