



# WEBSITE EMERGENCY CHECKLIST

Your 1-Hour Plan to Respond, Recover, and Rebuild

# Table of Contents

|                                         |    |
|-----------------------------------------|----|
| Introduction                            | 1  |
| Step 1: Don't Panic. Contain the Damage | 2  |
| Step 2: Run Your First Five Checks      | 3  |
| Step 3: Reset Access Safely             | 4  |
| Step 4: Call the Right People           | 5  |
| Step 5: Lock It Down for the Future     | 6  |
| Website Emergency Contact Worksheet     | 7  |
| Incident Response Log                   | 8  |
| Recommended Tools & Resources           | 9  |
| Final Tips                              | 10 |
| About the Author                        | 11 |

# Introduction

## If your website was hacked today, would you know what to do?

Most small-business owners don't, and that's okay.

When panic hits, every minute counts, but it's calm, not code, that saves you.

This mini-guide gives you a clear, printable action plan to follow if your website is compromised.

It shows you how to:

- Contain the problem quickly
- Identify what went wrong
- Restore control and security
- Prevent it happening again

No jargon. No scare tactics. Just five practical steps you can use even if you're not technical.

✖ **Tip:** Print this and keep it with your business records, it's your website's fire-drill plan.

— Wil Brown

Zero Point Development

## Step 1: Don't Panic. Contain the Damage

**Goal:** Stop the issue spreading and capture what's happened.

### Quick actions

- ☐ Put the site in maintenance mode or ask your host to suspend it temporarily.
- ☐ Don't delete anything yet; evidence helps your developer trace the problem.
- ☐ Screenshot or photograph anything unusual (error messages, new users, defaced pages).
- ☐ Post a short "under maintenance" notice so customers know you're on it.
- ☐ Take a breath, panic leads to mistakes; method beats mayhem.

 **Why this matters:** Acting calmly prevents further damage and preserves vital clues for cleanup.

## Step 2: Run Your First Five Checks

**Goal:** Understand what happened before touching the code.

- 1 **Users:** Any unfamiliar admin accounts or recent logins?  
→ Tool: Simple History (lightweight login tracker)
- 2 **Passwords:** Were credentials reused on other platforms?  
→ Use a password manager like Bitwarden.
- 3 **Plugins & Themes:** Anything outdated or unused?  
→ Update what's safe, note any that need replacement.
- 4 **Search & Domain Warnings:** Check Google Search Console or your browser for malware alerts.
- 5 **Traffic & Email Anomalies:** Sudden spam or foreign traffic spikes? Log them for your developer.

💡 **Key insight:** You can't fix what you don't understand; gather facts first.

## Step 3: Reset Access Safely

**Goal: Make sure only trusted users have control.**

- ☐ Change all admin passwords, website, hosting, domain, and email.
- ☐ Use strong, unique passwords via Bitwarden.
- ☐ Enable two-factor authentication (2FA) using Wordfence + Google Authenticator, Authy or Bitwarden Authenticator.
- ☐ Remove old staff, contractors, or unknown users.
- ☐ Confirm recovery emails and phone numbers in your host and registrar accounts.

 **Analogy:** You wouldn't change the shop lock but leave the back door open — secure every entry point.

## Step 4: Call the Right People

**Goal: Get help from those who can actually fix it.**

- 1 Your Web Host Support**
  - Ask them to isolate the site and preserve a backup copy before changes.
- 2 Your Developer / Tech Person**
  - They'll clean code, restore from a clean backup, and test security
- 3 Cleanup Services** (if you don't have a dev)
  - Sucuri or MalCare offer one-off malware cleanups and post-scan reports.
- 4 Avoid "Who Can Fix My Hacked Site?" posts**
  - Random online offers often make things worse. Stick with verified help.

 **Phrase to use when contacting your host:**

"Please suspend my site and preserve a full backup before any changes; I believe it's been compromised."

## Step 5: Lock It Down for the Future

**Goal: Build resilience so it doesn't happen again.**

- ☐ Turn on plugin/theme auto-updates for trusted software.
- ☐ Schedule monthly backups and store a copy off-site (try UpdraftPlus or BlogVault).
- ☐ Delete inactive plugins or themes; don't just deactivate them.
- ☐ Enable security monitoring with Wordfence.
- ☐ Review users quarterly and renew your SSL certificate on time.

 **Maintenance habit:** Block 15 minutes on the first Monday each month for updates and backups.

# Website Emergency Contact Worksheet

For Website: \_\_\_\_\_

| Category         | Company / Name | Login URL | Email / Phone | Notes |
|------------------|----------------|-----------|---------------|-------|
| Domain Registrar |                |           |               |       |
| Web Host Support |                |           |               |       |
| Web Dev          |                |           |               |       |
| Tech Support     |                |           |               |       |
| Email Provider   |                |           |               |       |
| Backup Service   |                |           |               |       |
| Security Plugin  |                |           |               |       |
| Security Service |                |           |               |       |

Updated On: \_\_\_\_\_ Updated By: \_\_\_\_\_

 Print this page, complete it, and store with your business continuity plan.

# Incident Response Log

Use this page to record actions taken during or after a website incident. It helps you stay organised, communicate clearly with your web host or developer, and document what was done for insurance or reporting purposes.

For Website: \_\_\_\_\_

[illegible]

## Recommended Tools & Resources

| Purpose          | Tool                 | Link                                                                                                      |
|------------------|----------------------|-----------------------------------------------------------------------------------------------------------|
| Password Manager | Bitwarden            | <a href="https://bitwarden.com">https://bitwarden.com</a>                                                 |
| MFA Apps         | Google Authenticator | Search on Google Play or Apple App Store                                                                  |
| MFA Apps         | Authy                | <a href="https://authy.com">https://authy.com</a>                                                         |
| Security Plugin  | Wordfence            | <a href="https://wordpress.org/plugins/wordfence/">https://wordpress.org/plugins/wordfence/</a>           |
| Login Tracker    | Simple History       | <a href="https://wordpress.org/plugins/simple-history/">https://wordpress.org/plugins/simple-history/</a> |
| Backup Tools     | UpdraftPlus          | <a href="https://updraftplus.com">https://updraftplus.com</a>                                             |
| Backup Tools     | BlogVault            | <a href="https://blogvault.net">https://blogvault.net</a>                                                 |
| Cleanup Services | Sucuri               | <a href="https://sucuri.net">https://sucuri.net</a>                                                       |
| Cleanup Services | MalCare              | <a href="https://malcare.com">https://malcare.com</a>                                                     |

# Final Tips

## Keep your plan close.

Print this checklist, add your key contacts, and revisit it yearly.

Security confidence comes from clarity, not complexity.

Small habits = big protection:

- Update monthly
- Backup twice
- Review users quarterly

💡 You've already done the hardest part - getting prepared.

## Need Help?

If your site's been hacked or you'd like a proactive security audit, contact Zero Point Development for professional recovery and protection.

🌐 Visit → [zeropointdevelopment.com/contact](https://zeropointdevelopment.com/contact)

✉ Email → [wil@zeropointdevelopment.com](mailto:wil@zeropointdevelopment.com)

# About the Author

I'm Wil Brown, a WordPress consultant, developer, and educator who's been helping businesses build and optimise websites since 2005.

Over the years I've worked with brands like Nikon, Google, CMC Markets, and Queensland Health, as well as hundreds of small businesses here in Sydney.

Through Zero Point Development, I focus on helping small business owners get real results from their websites; **more enquiries, more sales, and less stress.**

My approach is practical, outcome-focused, and built on 18+ years of experience solving web challenges for organisations big and small.



If you're ready to turn insights into action, I'd love to help you plan the next steps for your business.

👉 **Book a free 15-minute strategy call at [zeropointdevelopment.com](https://zeropointdevelopment.com)** and let's see how we can make your website pay for itself.

