# Cybersecurity for Small Biz: Your 1-Hour Website Emergency Plan

**Speaker:** Wil Brown
**Format:** Webinar transcript (edited for clarity)
**Timestamps:** Marked in 5-minute intervals

---

## [00:00] Opening & Acknowledgement of Country

**Wil Brown:**
Hello everyone — I'll give folks a moment to join. I hope you've been enjoying the NSW Small Business Month webinars; I've been to quite a few and they've been excellent — great information, presentations, and resources.

**Acknowledgement of Country:**
I acknowledge the Traditional Custodians of the land we meet on today and pay my respects to Elders past, present and future. I extend that respect to Aboriginal peoples joining us today. I'm proud to host this session as part of the 2025 NSW Small Business Month program, in partnership with the NSW Government.

**Quick Poll (in chat):**
If your website were hacked today, what would you do first?

1. I know exactly what to do
2. I'd probably Google it
3. I'd call my hosting company
4. Honestly, I'd have no idea

**[Poll responses noted in chat: mix of 2s and 4s.]**

---

## [05:00] Who I Am & Why This Matters

**Wil:**
I'm Wil Brown — WordPress consultant and educator. I've worked with WordPress since 2006. These days I help small business owners keep websites simple, secure, fast, and manageable. I run local meetups and help with national conferences like WordCamp Sydney and Everything Open.

I've seen how stressful outages are. It's not just the tech — it's your reputation and income. My aim is to help small business owners feel confident managing and protecting their sites.

**Contact:**

- Website: zeropointdevelopment.com
- Email: wil (one L) @ zeropointdevelopment.com

---

# [10:00] Why Small Businesses Are Targeted

**Wil:**
You might think, “I’m small — why would anyone target me?” That’s exactly why small businesses get targeted.

- **Automation & scale:** Attackers scan thousands of sites for easy wins — outdated plugins, weak logins, misconfigured servers.
- **Lower defences:** Small businesses rarely have dedicated security staff.
- **Maintenance gaps:** “Set and forget” sites with weak passwords, expired SSLs, and neglected updates.

**What’s at stake:**

- **Downtime → lost revenue.** Even an hour offline can cost leads and sales.
- **Trust & reputation.** Customers worry about their data; rebuilding trust is hard.
- **Recovery cost & time.** Coordinating hosts, developers, and comms adds hidden costs.
- **Legal exposure.** Breaches may trigger privacy notifications and other obligations.

**Recent Australian figures (summarised during talk):**

- Average SMB cyber-attack cost in 2025 estimated at ~$122,000; ~6% of small businesses close within six months of an attack.
- ABS data: ~22% of businesses reported a cyber incident in 2021–22; increasing trends since.
- Reports cite ~8% YoY rise in small-business incidents; average ~$50,000 per incident.
- Mastercard: ~309,000 Australian SMBs report being targeted; ~33% with financial loss.

Key mindset: you can’t always **prevent** hacks, but you can control how you **respond**. Today is about a practical, calm, one-hour emergency plan.

---

# [15:00] Case Study: The Food Truck Hack

**Wil:**
A local Mexican food truck business (two trucks, small WordPress brochure site) listed weekly times and locations. Friday–Sunday were their peak revenue days.

**What happened:**

- **Signs:** Phones went quiet; online orders dropped; lunchtime queues disappeared.
- **Site looked "normal,"** but attackers had:
    - Installed a **crypto-miner** on the homepage (fans spinning up on visitors' laptops is a clue).
    - **Changed the event schedule** (times/locations wrong), sending customers to the wrong places.

**Impact:**

- Lost the **entire weekend's trade** (~$6k–$7k).
- **Food wastage** costs.
- **Trust** took a hit.
- **Emergency cleanup** cost (my time), comms with customers to repair confidence.

**Complication:**

- **No regular backups.** Host was in the US; had to wait for business hours to request a backup (thankfully available).
- I removed vulnerable plugins, installed **Wordfence**, enabled **Two-Factor Authentication (2FA)**, cleaned the site, restored the correct schedule, and trained the owner to do safe updates and offsite backups.

**Takeaway:**
A hack hits more than a website. It hits income, reputation, and relationships. An **emergency plan** is insurance for your livelihood.

---

# [20:00] The 1-Hour Website Emergency Plan — Overview

**Wil:**
I'll use WordPress examples, but the plan applies to Squarespace, Wix, Shopify — principles are the same: logins, updates, backups.

**Five steps:**

1. **Stay calm & contain**
2. **Run your first five checks**
3. **Reset access safely**
4. **Call the right people**
5. **Lock it down for the future**

---

# [25:00] Step 1 — Stay Calm & Contain

**1) Stay calm.**
Don't panic-click, delete plugins, or roll random backups. That erases evidence and can worsen things.

**2) Go offline if you can.**

- Use **maintenance mode** or ask your host to **isolate** the site.
- Post a **holding message:** "We're performing urgent maintenance." Professional and prevents alarm.
- Most hosts have **24/7 chat**; ask them to isolate first to stop the bleed.

**3) Capture the data.**

- Take **screenshots** or quick phone videos of anything odd: strange pop-ups, new admin users, weird media filenames.
- Think like an **insurance claim**: good documentation speeds diagnosis.

**4) Don't start uninstalling yet.**
Contain first, **diagnose next**, then clean.

**5) Tone & reassurance.**

- Communicate calmly; silence erodes trust.
- A brief status message beats rumours.

**Key:** Pause, isolate, document. Then move to checks.

---

# [30:00] Step 2 — Run Your First Five Checks (Lightweight "Detective Work")

**Wil:**
You're gathering clues, not fixing code yet.

1. **Who's logged in / users**
   - In WordPress, check **Users** for unknown admins.
   - Add **Simple History** (plugin) to log logins and actions.
   - If locked out, ask the host to examine **server access logs**.
2. **Password reuse**
   - Be honest: is this password used elsewhere?
   - Use a password manager (**Bitwarden**, **1Password**) to generate **unique, long** passwords.
3. **Plugins/themes status**
   - Identify **outdated** items — common entry points.
   - Deactivate and **remove** unused plugins/themes. Inactive files can still be exploited.
4. **Google/domain warnings**
   - In Google, search `site:yourdomain.com` for odd pages or spam.
   - Watch for **browser warnings** (malware/deceptive). Note them now; they can be cleared post-cleanup.
5. **Email/traffic anomalies**

- Weird **delivery failures** or spam complaints may indicate the domain is sending junk.
- **Analytics spikes** from unusual countries can signal abuse.

**Key:** You can't fix what you don't understand. These checks give facts before actions.

---

# [35:00] Step 3 — Reset Access Safely (Re-Key the Locks)

1. **Change all admin passwords — everywhere.**
   - Website admin, **hosting panel**, **FTP/SFTP**, **domain registrar**, **email** — anything connected.
   - Don't reuse old passwords. Use 16+ characters or a strong passphrase.
2. **Use a password manager.**
   - Bitwarden/1Password generate and store unique credentials.
   - Top managers use **end-to-end encryption**.
3. **Enable MFA/2FA.**
   - WordPress example: **Wordfence** + an authenticator app (Google Authenticator, Authy, Bitwarden Authenticator).
   - Even with a stolen password, attackers can't log in without your one-time code.
4. **Clean up user accounts.**
   - Remove unknown or no-longer-needed users, especially **admins**.
   - Disable contractor accounts when projects end.
5. **Check recovery details (advanced but valuable).**
   - Confirm your **host/registrar account** recovery email and phone are current and secure.

---

# [40:00] Step 4 — Call the Right People (Your Emergency Crew)

**Start with your hosting provider.**

- Ask them to **isolate** the site, preserve or restore **backups**, and check **access logs**.
- They may scan for obviously malicious files.
- **Important:** Hosts generally **don't fix your site's code**. Think of them as the landlord, not the mechanic.
- Script you can use:

  > "My website appears compromised. Please isolate it and preserve a backup before making any changes."

**Then bring in your developer/IT contact.**

- They remove malicious code/files, clean databases, reinstall clean versions, add monitoring and 2FA, and file requests to clear browser/Google warnings.

**If you don't have a developer:**

- Consider reputable **specialist cleanup services** like **Sucuri** or **MalCare** for one-off remediation and short-term monitoring. Check reviews and ensure post-clean monitoring is included.

**Avoid:**

- Random "cheap fix" offers from unvetted social media posts. Stick with known providers.

**Key:** Host contains, developer repairs, security service monitors.

---

# [45:00] Step 5 — Lock It Down for the Future (Simple Habits)

**Monthly 15-minute check** (or weekly if you prefer):

1. **Auto-updates**
    - For small brochure sites, enable auto-updates on WordPress core/plugins/themes.
    - For complex e-commerce/LMS/membership sites, use a **staging** copy to test updates first, then push live.
2. **Offsite backups**
    - Keep at least **two copies**: one with the host, one **offsite** (e.g., Google Drive/Dropbox via UpdraftPlus, BlogVault, or JetBackup).
    - Backup both **files and database**.
    - Frequency guide:
        - Static brochure site: **monthly**
        - Active content site: **weekly**
        - E-commerce/LMS/membership: **daily or real-time**
3. **Delete unused plugins/themes**
    - Don't just deactivate; **remove** them. Inactive code can still be exploited.
4. **Monitoring & alerts**
    - Use **Wordfence** (free for most sites; premium for high-risk). Review weekly summary emails; don't obsess over every alert.
5. **Quarterly extras**
    - Review users and permissions.
    - Confirm **SSL** renews automatically.
    - Ensure **domain registrar** contact details are current so renewal notices reach you (lapsed domains are a massive risk).

**Key:** Security is a **habit**, not a one-time fix.

---

# [50:00] Mid-Session Pulse Check (Poll)

**Wil:**
Quick pulse check:

1. I already have auto-updates turned on
2. I don’t
3. Not sure

**[Poll responses noted in chat: several 2s and 3s.]**

**Wil (guidance):**

- Small, simple sites: turn on auto-updates.
- Larger/complex sites: use **staging** to test, then update.

---

# [55:00] Recap & Tools Mentioned

**Wil (recap of the five steps):**

1. **Don’t panic — contain the issue.**
2. **Run your first five checks** and document evidence.
3. **Reset access safely** so only you hold the keys.
4. **Call the right people** — host for containment, developer for repairs, optional specialist services for cleanups/monitoring.
5. **Lock it down** — simple maintenance habits to stay safe.

**Cleanup services mentioned:**

- **Sucuri** (recommended first if you have no IT contact)
- **MalCare**

**Security & utility tools mentioned:**

- **Wordfence** (firewall/monitoring, 2FA support)
- **Bitwarden**, **1Password** (password managers; Bitwarden Authenticator also noted)
- **Simple History** (WordPress activity logging)
- **UpdraftPlus**, **BlogVault**, **JetBackup** (backups)

**Downloadable resource:**

- **Website Emergency Checklist**: zeropointdevelopment.com/sbm (QR code shown during session).
    - Includes the five-step response, contact worksheets, incident worksheet, and recommended tools.

- Direct download; no email gate.

---

# [60:00] Q&A and Wrap-Up

**Audience Q (chat):** “Can you repeat the cleanup services?”
**Wil: Sucuri** and **MalCare**. Sucuri is widely recognised and a good first stop if you don’t have an IT person.

**Audience Q (chat):** “Any Facebook Professional Dashboard safety advice?”
**Wil:** I don’t work much with Facebook now — lots of spam, shifting rules. I’ve moved groups to **Telegram** and focus on **LinkedIn**. If you email me specifics, I’ll see if I can help.

**Wil (closing):**
Thanks for spending an hour with me today. Please review the security plan and jot down your key contacts so you’re ready. I hope you never need it — but if you do, you’ll be prepared. I’ll upload the replay and slides to the SBM page (cybersecurity session) shortly. Next week’s webinar is **Automation Starter Kit — Save 5 Hours a Week**; keep an eye on the schedule.

Have a great day, and I’ll hopefully see you in the next webinar!