CASE STUDY · WEBSITE CLEANUP

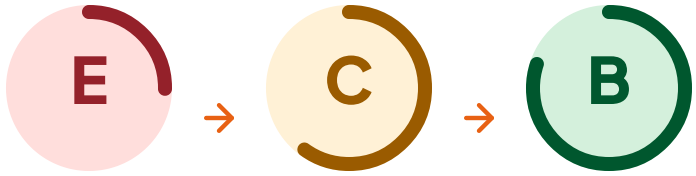
How we cleaned up a hacked HVAC contractor *website*

A Phoenix-area commercial HVAC company's WordPress site was quietly filled with casino spam, hidden betting links and an expired security certificate. Here's how PickupCrew's website cleanup service got it clean, secure and trustworthy again.

462	0	A	0
spam posts removed	spam left on 115 live pages	SSL security grade	malware flags after cleanup

SUCURI SITECHECK · OVERALL GRADE

Independent scan: E to B



OVERALL GRADE
Start of cleanup

OVERALL GRADE
Mid-cleanup

OVERALL GRADE
After

Sucuri SiteCheck flagged the site for malware with an E grade at the start of the cleanup, reached C after the first spam removal, and B after the new SSL went in. The remaining gap to an overall A is a web application firewall in front of the site, such as a free Cloudflare setup.

SUCURI SITECHECK · SCORECARD

Before-and-after scan results

CHECK	BEFORE	AFTER
Overall grade	E	B
SSL / TLS	C · 0/6	A · 6/6
Security checks	B · 5/6	B · 6/6
Domain rating	A	A
Warnings	Expired SSL	None
Malware	Flagged	None
Blacklisting	—	None

Before: overall grade and malware flag from the start of cleanup; other checks from the first saved scan. After cleanup, Sucuri reported no malware, no blacklisting and no warnings. The new SSL certificate is valid through May 2027.

WORDPRESS CONTENT

462 spam posts removed, 52 real posts kept

462
spam posts moved to Trash
(of 514 posts on the site)

52
owner's real posts kept
and left published



Spam removed · 90% Real posts kept · 10%

FINAL LIVE-PAGE SCAN

115 live pages, 0 spam



115
live pages rescanned
after cleanup.
Zero spam remaining.

Before

- Hundreds of casino and betting spam posts
- Hidden spam on the homepage and 11 pages
- Malicious hidden plugin injecting betting links
- Expired SSL ("Not Secure" warning)
- Leftover demo pages and old backdoor scripts

After

- All 462 spam posts removed; 52 real posts kept
- Zero spam on all 115 live pages
- Malicious code and backdoors removed
- New 3-year SSL, all traffic on https, grade A
- No malware, blacklisting or Sucuri warnings

Wordfence *firewall & malware scan*

Firewall on

The WordPress web application firewall was enabled and protecting, with extended protection turned on.

Brute-force protection

Login brute-force protection was on, and XML-RPC login (a common attack path) was turned off.

Malware scan: clean

A full Wordfence malware scan after cleanup came back clean. No malware was found.

From the after-cleanup Wordfence firewall and malware scan. A matching before-cleanup Wordfence score was not available to chart.

Our website cleanup *process*

1. **Backup and assess.** We took a full backup first, then scanned every page, post and user account to map the damage.
2. **Spam removal.** We moved 462 spam posts published by rogue accounts to the trash, kept all 52 of the owner's real posts, and stripped hidden spam out of the homepage, notification bar and 11 service pages.
3. **Malware removal.** We found and removed the hidden "must-use" plugin that was injecting betting links, plus the database entry that fed it, and saved evidence of everything.
4. **Backdoor cleanup.** We removed leftover restore scripts, an old remote-access connector, a demo installer and an unused theme, and locked down a folder anyone could write to.
5. **SSL repair.** We installed a new 3-year SSL certificate and sent all traffic to the secure https version, so the "Not Secure" warning is gone.
6. **Security hardening.** We turned on a WordPress firewall, disabled XML-RPC login, added browser security headers, hid server details and the user list, and updated WordPress core and plugins.
7. **SEO cleanup.** We fixed a robots.txt that blocked Google from rechecking old spam pages, hid theme demo and filler pages from search, cleaned up the sitemap and fixed broken menu and footer links.
8. **Verify.** We ran a final scan of every live page (zero spam), a firewall malware scan and an independent Sucuri scan (no malware, no blacklisting).

Signs your contractor website may be *hacked*

- Google shows strange casino, pharma or foreign-language results for your name
- Browsers show a "Not Secure" warning
- Admin users or posts you don't recognize
- Your site redirects or loads slowly for no reason
- Contact form leads stopped arriving
- Your hosting company flagged malware

Why it matters for HVAC and *trade businesses*

Your website is often the first thing a customer checks before they call. A security warning or spammy search results can send that call to a competitor, and a hacked site can drag down your Google rankings for months. A clean, secure site protects your reputation and the leads you're already paying to get.

WEBSITE CLEANUP | HACKED WEBSITE REPAIR | WORDPRESS MALWARE REMOVAL | SPAM REMOVAL | SSL REPAIR

Website Cleanup & Security

PickupCrew helps Phoenix-area HVAC and trade businesses with hacked website repair, WordPress malware removal, spam cleanup and SSL fixes, and then makes sure every call and lead actually gets answered. Visit **pickupcrewhq.com** or email **pickupcrewhq@gmail.com**.

Book a free website review