FREE CHAPTER

Freelancing with WordPress Malware Removal

FROM *WORDPRESS MALWARE REMOVAL FOR DEVELOPERS & SITE OWNERS*

Opportunity, evidence-led proposals, portfolio strategy, and trust

MD PABEL

Founder, 3Zero Digital

ABOUT THIS FREE CHAPTER

Turn a technical skill into professional trust

Malware removal can become a valuable freelance service, but only when technical skill is matched by evidence, authorization, careful scope, and honest communication. This complete chapter examines the opportunity without promising easy clients or guaranteed income.

INSIDE THIS CHAPTER

- Current WordPress attack and infection figures, with their limitations.
- A practical comparison of visible Fiverr service categories.
- An evidence-led Upwork proposal for a redirect-malware job post.
- LinkedIn, portfolio, and symptom-focused search strategies.
- Safe scoping, client trust, and a practice path before production work.

> *Educational and authorized use only: Practise in an isolated lab, a disposable sandbox, or a system you own or have explicit permission to inspect and modify. Never test or clean a public system without authorization.*

Book and service information: mdpabel.com

CHAPTER 18

18. Freelancing with WordPress Malware Removal

WordPress powers more than 43 percent of the web.[1] That enormous footprint includes personal blogs, company websites, news publications, membership platforms, and stores that cannot simply ignore a compromise.

Attack data helps show the scale of the problem. In 2024, Wordfence logged more than 54 billion malicious requests across the websites in its network. That is an average of approximately 148 million malicious requests per day. During the same year, Wordfence saw just under one million distinct sites infected with malware, with approximately 325,000 to 350,000 infected sites observed on any given day.[2]

The problem continued. During the fourth quarter of 2025, Wordfence detected malware on 467,000 distinct sites in its network.[3]

These figures need careful interpretation. A malicious request is not the same as a successful compromise. One bot may send thousands of requests, and one site may contain many infected files. The figures describe Wordfence's network, not every WordPress installation on the internet.

Even with those limitations, the conclusion is clear: WordPress attacks and infections are not rare events. Website owners regularly need someone who can investigate suspicious behavior, remove malware, recover a suspended site, resolve a blacklist warning, and reduce the chance of the same incident returning.

That creates a real professional opportunity for people who develop the necessary skills. It does not promise easy work or guaranteed income.

> ***No earnings guarantee:*** *This chapter describes possible freelance and career paths. Completing this book does not guarantee clients, employment, marketplace ranking, or income.*

Why malware removal is valuable work

A new website project usually begins with planning. The client can compare designs, features, prices, and schedules before choosing a developer.

A malware-removal enquiry often begins under pressure.

The owner may be watching visitors redirected to another domain. Google may be displaying a dangerous-site warning. The hosting provider may have suspended the account. Spam pages may be appearing in search results, or a fake checkout may be putting customers at risk.

These owners do not only need someone who knows how to delete a suspicious file. They need someone who can answer difficult questions:

- What is actually happening?
- Which sites, accounts, and customers may be affected?
- What evidence should be preserved before cleanup?
- Is the visible malware the complete infection or only one symptom?
- What is restoring the malware after deletion?
- Can the website be recovered without destroying legitimate work?
- What must be tested before the business can safely use the site again?

The value is in the complete recovery decision: investigate, preserve, clean, revoke, restore, verify, and explain.

If you followed the investigations in this book, you already understand many parts of that process. You have seen malware in WordPress files, database rows, users, cron jobs, hosting accounts, DNS, browser state, and external reputation systems. That knowledge is a foundation. Professional confidence comes from practising the method until you can apply it safely to a new situation.

AI Can Build Websites - but Can It Clean Them?

AI tools can generate a layout, draft code, compare files, explain a PHP function, summarize logs, and help prepare a report. A malware-removal specialist can use these capabilities to work more efficiently.

But an AI response does not automatically know whether an unfamiliar plugin is a client's private integration or an attacker-created copy. It may not see a hosting cron job, a second database, an old developer's account, a registrar delegate, or another infected site under the same hosting account. It can also recommend a confident deletion when the evidence is incomplete.

The human specialist still has to confirm authorization, understand the business context, protect the evidence, decide what can be changed safely, verify the result, and accept responsibility for the work.

Use AI as an assistant, not as proof. Never give an unapproved AI service a client's passwords, API keys, private customer data, complete database dump, or live malware. Understand and reduce the scope of every generated command before using it on an authorized system.

AI does not remove the opportunity. It gives a careful specialist another tool.

What the Fiverr marketplace shows

Fiverr search results provide a useful snapshot of the visible marketplace. On September 4, 2026, I recorded the following approximate result counts:[7]

Fiverr search	Visible results
WordPress design	33,000+
WordPress development	15,000+
WordPress customization	9,700+
WordPress malware removal	4,100+
WordPress hacked	1,100+
Blacklist removal	166

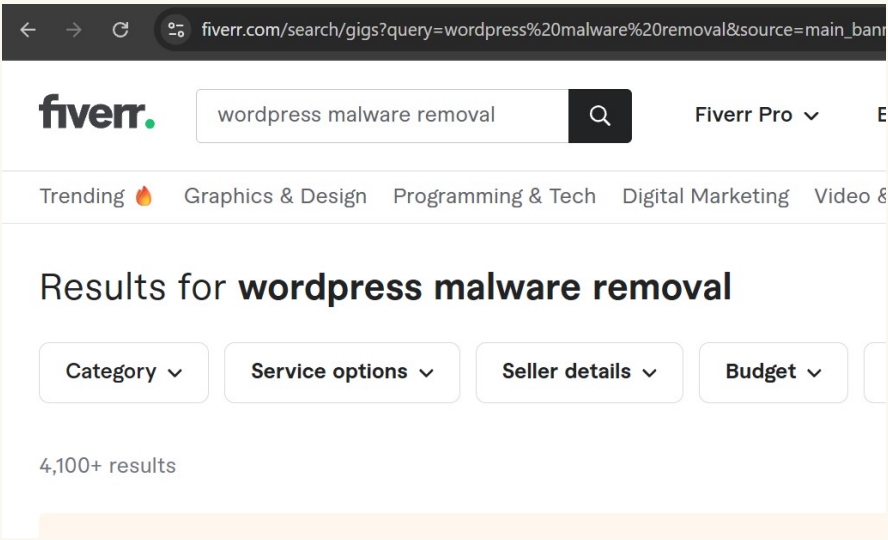

Figure 18.1. The WordPress malware-removal search confirms an established service category. Search totals are a dated marketplace snapshot, not a count of unique specialists or available clients.

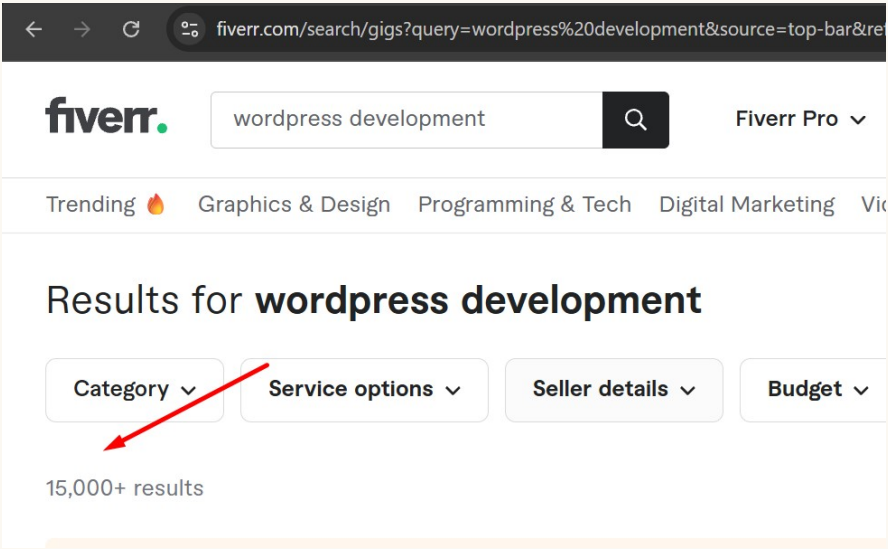

Figure 18.2. The broader WordPress-development search displayed more than three times as many results as the malware-removal search in the same research session.

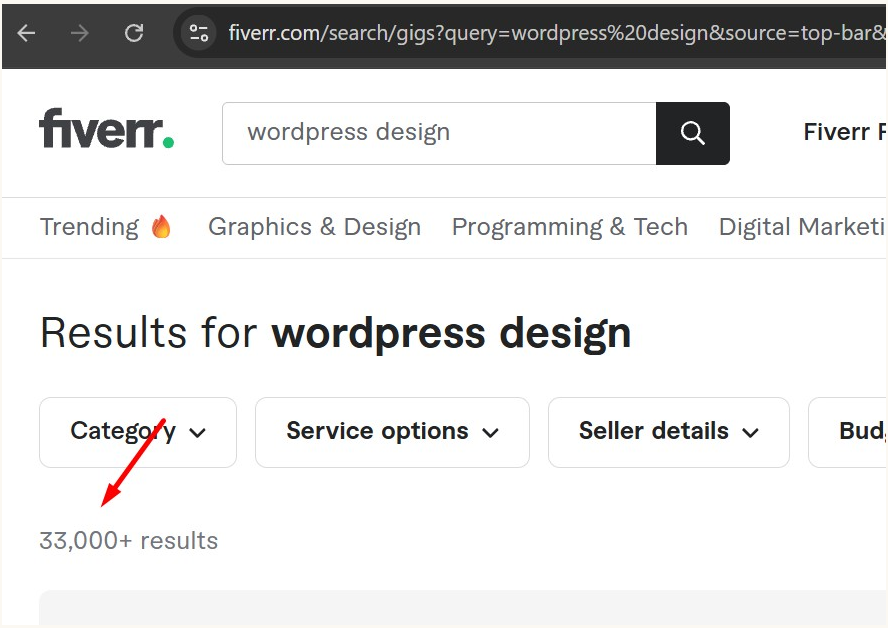

Figure 18.3. WordPress design produced the largest result set in this small comparison.

This research does not prove that malware removal is easy or that every search result represents a different competitor. The same seller may have several gigs, services can overlap, and Fiverr can change or personalize its results. The figures also measure visible service listings, not buyer demand.

They do show something useful: malware removal is an established but more specialized category than general WordPress design or development in this snapshot. Specific problems such as hacked-site recovery and blacklist removal produce smaller visible result groups again.

A new seller still needs trust, reviews, clear communication, and successful delivery. A useful gig should explain:

- the exact problem it addresses;
- what one order includes;
- whether the scope covers one site or the whole hosting account;
- which access, reports, and backups the buyer must provide;
- what will be investigated and verified;
- which results depend on Google, a host, or another external vendor; and
- which conditions require a revised scope or specialist escalation.

Do not copy an unrealistic price or one-hour promise simply because another seller uses it. A returning infection, payment skimmer, or multi-site hosting compromise cannot be scoped honestly from the message "my website is hacked."

Finding projects on Upwork

Upwork normally begins with a client posting a problem and freelancers sending proposals. The client may describe one symptom while expecting several kinds of work.

One WordPress malware-removal posting reviewed for this chapter requested infected-file cleanup, vulnerability review, prevention recommendations, cPanel work, and the removal of unused websites from the hosting account. The posting displayed 20 to 50 proposals within hours.[4]

One posting cannot define the entire marketplace. It does demonstrate that there are real projects and real competition.

Start with the client's exact symptom

Imagine that a client posts this job:

> ***Example job post - WordPress website redirecting to a spam site:*** *My WordPress website is redirecting visitors to an unknown spam website. It does not happen on every visit, and sometimes the homepage looks normal. I have included the website URL. I need someone to find the cause, remove the malware, and stop the redirect from returning.*

Many freelancers will reply with a generic sentence such as "I can fix your website" or a long list of security plugins. Neither response shows that they understand this client's redirect.

If the client has explicitly invited applicants to review the visible public symptom, use the investigation method from Chapter 8 before writing the proposal. Work from an isolated browser or disposable environment and limit the review to ordinary public requests. Do not log in, scan directories, fuzz endpoints, download unknown files, or attempt cleanup before the client's authority and the working scope have been verified.

Depending on the reported condition, check the public site as a logged-out visitor and record what the browser actually does:

1. Capture the original URL, time, device condition, and referral condition.
2. Record the redirect chain and HTTP status codes in the browser's Network panel.
3. Identify whether the navigation was initiated by a server response, a meta refresh, JavaScript, an iframe, or a replaced page.
4. Inspect the delivered page source for the exact external domain, encoded script, unexpected loader, or redirect instruction observed in the browser.
5. Save small screenshots showing the evidence, while hiding unrelated private information and defanging a malicious destination where appropriate.

A useful proposal could then say:

> *Hello, I reviewed the public URL you included from an isolated browser. I was able to reproduce the redirect when **[state the exact condition, such as a logged-out mobile visit or a visit from a search result]**. My first screenshot shows **[the relevant request or redirect chain]** in the browser Network panel. The second shows **[the matching source-code or response evidence]** that initiated the navigation to the spam domain. This confirms the visible redirect mechanism, but it does not yet prove where the malware is stored or how it returns. After access and authorization are confirmed, I would preserve a backup and investigate the connected WordPress files, plugins, theme code, database values, users, scheduled tasks, and hosting rules. I would remove only the confirmed unauthorized components, check for the writer or persistence behind them, and retest the original redirect condition after cleanup. I have attached the two redacted evidence screenshots from the public review.*

Replace every bracketed field with what you actually observed. If you could not reproduce the redirect, say that honestly and explain which client-provided conditions or evidence you would need next. Never invent a screenshot, claim a

root cause from one browser request, or describe a public signal as proof that a particular file or plugin is infected.

This proposal is stronger because it gives the client three things before any sales promise: evidence that you read the job, evidence that you understand the visible behavior, and a safe plan for moving from the symptom to the storage and persistence behind it.

Review the client's history, requirements, expected availability, and the platform's current rules before accepting a project. Never execute an unknown backup on your everyday computer simply to prepare a proposal.

Using LinkedIn for services and career opportunities

LinkedIn can help with both client relationships and employment. Relevant jobs may use titles such as WordPress support specialist, website operations specialist, incident responder, malware analyst, security analyst, or web application security engineer. Search the responsibilities and skills, not only the exact phrase "WordPress malware remover."

LinkedIn also allows members to create a Service Page. LinkedIn describes this as a landing page where potential clients can find a provider and send a project request. A client can contact a provider without already being a connection.[5]

Useful posts can demonstrate your judgment before someone contacts you:

- why deleted malware returned;
- why a scanner missed a mobile-only redirect;
- how an administrator can be hidden from the dashboard;
- what to preserve before asking a host to restore a site; or
- how to verify that checkout, forms, DNS, and scheduled work survived cleanup.

Publish only anonymized material you are authorized to share. Do not expose a client's domain, credentials, customer information, or working malicious code.

Your portfolio website can become a client channel

Marketplaces are not the only way to find work. An independent portfolio gives you a place to explain your services, publish useful investigations, and show how you think without reducing everything to a gig title.

I started building `mdpabel.com` about one year before writing this chapter. In the 16-month view selected in Google Search Console, the website received 25,600 search impressions and 558 clicks from Google.[7]

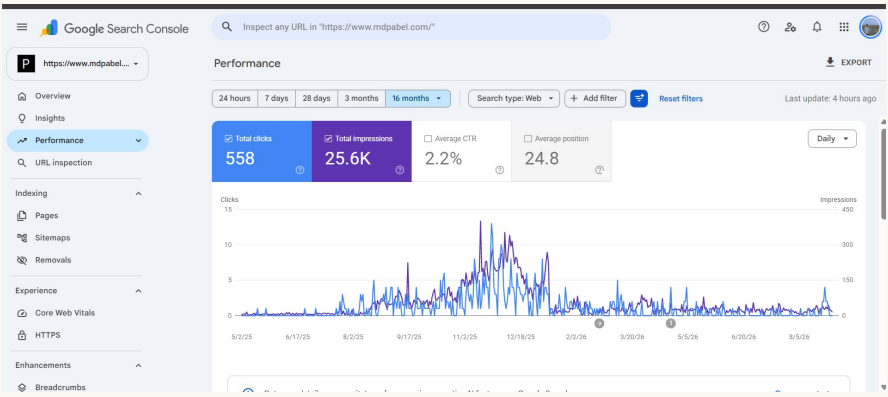

Figure 18.4. Search visibility developed over time. Impressions and clicks show discovery; they are not the same as enquiries or paying clients.

The website's stored form totals recorded 29 free malware-scan requests and six direct **Hire Me** submissions. Other people contacted me through WhatsApp and Tawk live chat, which are not included in those form counts.

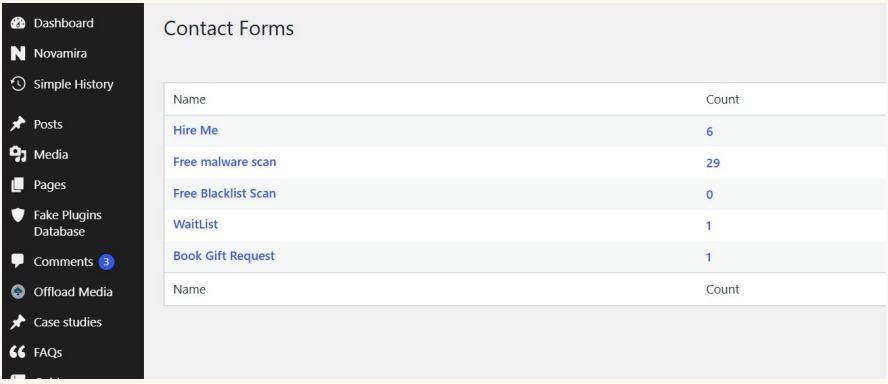

Figure 18.5. These are recorded form enquiries, not 35 confirmed clients. WhatsApp and live-chat conversations were separate channels.

Across the forms, WhatsApp, and live chat, `mdpabel.com` helped me acquire more than 15 clients. This is my experience, not a forecast of what another website will earn.

The important lesson is how the portfolio supported the decision. I did not publish only a page saying "I remove malware." I published focused service pages, practical guides, and technical case studies. A potential client could see examples of redirect malware, hidden administrators, hacked URLs, blacklist warnings, and persistent infections before contacting me.

Google helped people discover the content. The evidence on the website helped build confidence.

Write for the exact problem

A new portfolio should not depend only on winning a broad search such as **WordPress malware removal**. Large security companies and established sites already compete for broad phrases.

Keep one clear page describing the complete service, then publish supporting pages around the problems owners actually see:

Main service	Specific problem-led content
WordPress malware removal	WordPress redirect malware
Hacked-site recovery	Mobile-only redirect from Google
WordPress cleanup	Malware returning after deletion
Search reputation recovery	Japanese SEO spam or hacked URLs
Blacklist removal	Google dangerous-site warning
WooCommerce security	Fake checkout or payment skimmer
Hosting recovery	Hosting account suspended for malware

Someone searching for **WordPress redirect malware** is usually not browsing for design inspiration. Their visitors may already be redirected and their business may be losing trust or revenue. This is strong problem-solving intent, although it does not mean every visitor will hire you.

Do not increase the owner's fear to force a sale. Use the page to make the situation calmer:

1. Describe the symptom in language the owner recognizes.
2. Explain what can cause it without pretending every case is identical.

3. Show a real, anonymized investigation or case study.
4. Explain the first safe steps and what should not be deleted blindly.
5. Describe your service, boundaries, and verification process.
6. Provide a simple way to request help.

Google recommends anticipating the words readers use while producing original, helpful, people-first content based on real experience.[6] The goal is not to manufacture dozens of thin keyword pages. Each page should solve a specific reader problem well enough that it would still be useful if the visitor arrived without Google.

Make urgent contact safe

A visible contact form, WhatsApp link, or live chat can reduce the distance between an urgent visitor and the specialist. The first conversation should collect only enough information to decide the next step:

- the website address;
- the visible symptom;
- when it began;
- any host, browser, or Search Console warning; and
- whether the person is authorized to request work on the site.

Do not ask someone to paste a hosting password, API key, database export, or customer data into an ordinary chat. Move credentials and evidence into an approved secure exchange after the scope and authorization are established.

Turn an enquiry into a bounded service

Do not begin with the promise "I will remove every virus and secure your site forever." Begin with a scope and a result that can be checked.

Stage	Useful deliverable
Initial triage	Confirmed symptom, immediate risk, access needed, affected scope, and next decision
Investigation	Evidence map across the relevant files, database state, users, tasks, logs, and control planes
Cleanup and recovery	Documented changes, revoked access, restored service, and tested business functions

Stage	Useful deliverable
Reputation recovery	Evidence prepared for the relevant host, search engine, browser, or blacklist process
Handoff	Known-good baseline, remaining risks, backup status, monitoring plan, and client-owned actions

Before quoting a fixed scope, ask:

1. How many websites, databases, domains, and hosting accounts may be involved?
2. What exact symptom appears, and under which device, referrer, or login condition?
3. Is the site a store, membership system, publisher, or lead-generation site?
4. Is it online, suspended, or still changing?
5. What access, logs, host reports, and clean backups are available?
6. Is there a deadline from a host, advertiser, search engine, or payment provider?
7. What must work before the owner can safely return the site to service?

When the answers are unknown, propose a diagnostic stage first. Price and scope the responsibility, not merely the number of files named by a scanner.

Trust is part of the service

A malware-removal specialist may receive access to hosting, databases, email, DNS, customer records, and payment-related systems. Technical skill without access discipline creates another risk for the client.

Before work begins, record who authorized it, which systems are included, which actions are permitted, how evidence and credentials will be exchanged, and when temporary access will be removed.

Your final report can remain concise while separating four things:

1. **Observed:** the symptoms and evidence you directly confirmed.
2. **Changed:** what you removed, replaced, revoked, or reconfigured.
3. **Verified:** the conditions and business functions you tested afterward.
4. **Unresolved:** missing logs, unknown access, external reviews, or client actions that remain open.

This structure makes the work easier to verify and harder to overstate.

Practise before accepting production risk

> ***Educational and authorized use only:*** *Practise these techniques in an isolated lab, a disposable sandbox, or a system you own or have explicit permission to inspect and modify. Do not scan, access, test, alter, or attempt to clean a public website, server, database, or account without authorization. Never execute suspicious code or malware outside a properly isolated environment.*

A sensible next path is:

1. Build several disposable WordPress labs and practise restoring known snapshots.
2. Analyze captured examples as inert evidence instead of executing live malware.
3. Write two or three redacted case-style reports showing observation, evidence, action, verification, and uncertainty.
4. Define one narrow starting service and a checklist for accepting its scope.
5. Practise explaining an investigation to a nontechnical owner.
6. Accept smaller authorized cases first and improve the checklist after every job.
7. Keep studying WordPress internals, PHP, databases, Linux, hosting, DNS, logs, web security, and incident response.

Malware removal needs advanced hands. Finishing this book does not make every incident safe for you to accept, but it means you already understand many of the places where malware can hide and many of the mistakes that cause a cleanup to fail.

Keep learning. Keep practising safely. Build evidence of your work, communicate honestly, and let the quality of each recovery earn the next opportunity.

Source notes

[1]: WordPress.org, "Features". WordPress states that it powers more than 43 percent of the web.

[2]: Wordfence, "2024 Annual WordPress Security Report". The figures describe malicious requests and infections observed within Wordfence's network, not every WordPress website worldwide.

[3]: Wordfence, "Quarterly WordPress Threat Intelligence Report - Q4 2025". The report recorded 467,000 distinct sites with malware during the quarter.

[4]: Upwork, "WordPress Malware Removal Expert", reviewed September 4, 2026. This single time-specific posting is an example, not a measure of typical demand, price, competition, or earnings.

[5]: LinkedIn Help, "Get started as a service provider on LinkedIn". LinkedIn describes Service Pages as operating through client requests and provider proposals.

[6]: Google Search Central, "SEO Starter Guide" and "Creating helpful, reliable, people-first content".

[7]: Figures 18.1 through 18.5 are the author's own marketplace, Search Console, and website-form screenshots captured on September 4, 2026. Marketplace counts and search performance change over time. Form submissions are enquiries, not automatically paying clients.

CONTINUE LEARNING

The complete recovery process

This free chapter focuses on turning recovery knowledge into responsible professional work. The complete book develops the technical process behind that service across eighteen evidence-led chapters.

THE FULL BOOK COVERS

- Confirming whether a site is actually compromised.
- Preserving evidence and identifying the affected scope.
- Cleaning WordPress files, databases, users, cron jobs, hosting, and DNS.
- Investigating redirects, SEO spam, hidden administrators, and skimmers.
- Recovering suspended or blacklisted sites.
- Removing persistence, securing the baseline, and monitoring recovery.

> *A clean site is not a screenshot or a moment when the homepage loads. It is a supported conclusion - and a baseline worth protecting.*

Visit mdpabel.com for the complete book

Written by MD Pabel, founder of 3Zero Digital.