

Inner Melbourne accounting firm

The hack only Google could see.

A small accounting practice's tax return page was quietly serving an Indonesian betting page to Google, and only to Google. Here's how we found it, how we explained it, and how it was removed. (We've left the firm's name out.)

2

Versions of one page: the real one for people, a gambling page for Google

630KB

Of hidden gambling content, nearly three times the size of the real page

0

Signs of it when the owners browsed their own site

2021

The last time anyone had touched the website

The challenge

A break-in you couldn't see from your own browser.

The firm is a small accounting and tax practice in inner Melbourne. Its website was about ten pages, built on WordPress, and nobody had touched it since 2021. It still carried WordPress's default tagline, "Just another WordPress site", and ran a 2020-era copy of Slider Revolution, a popular add-on with a history of serious security holes.

The first warning came from our AI-driven lead generation process, which flagged possible gambling links on the firm's Tax Return Accountant page. So we looked. And found nothing. The page looked completely normal in a browser and to the standard web tools.

That's where most checks stop. We asked for the page twice instead: once as a normal visitor, and once posing as Googlebot, the program Google uses to read websites. Then we compared the two.

What we found

- ✓ **The site had two faces.** People got the genuine accountant page (about 219 KB). Google got an entirely different Indonesian gambling page (about 630 KB) selling sports betting and online slots. The trick is called cloaking.
- ✓ **It was built to rank.** The gambling page had its own title, description and social sharing details, plus fake customer reviews and question-and-answer data designed to show up as star ratings and FAQ boxes in Google's results.
- ✓ **It was aimed at this firm.** Every button (login, register, buy now, the footer links) pointed to an outside spam website, at an address named after this firm and this page. A managed campaign, not random junk.
- ✓ **It borrowed the firm's good name.** The firm's own web address was linked using the betting brand as the link text, so the spammers could ride on the domain's age and reputation to rank for gambling searches.
- ✓ **Only Google could see it.** The spam switched on when the visitor said it was Googlebot. The owners would never have seen it by browsing their own site.
- ✓ **Google's own tool confirmed it.** Google's testing tool, which shows a page exactly the way Google sees it, showed the same gambling page.

Why it mattered

Google thought their tax return page was about gambling.

Lost visibility

Google was being told the page was about betting, which hurts its chances for searches like “tax return accountant Melbourne”.

A public warning

Sites like this risk a “This site may be hacked” label in Google’s results, or a penalty applied by Google’s team.

Reputation

A prospective client who saw gambling content next to the firm’s name wouldn’t think “hacked”. They’d think “dodgy”.

Security

An outsider had working access to the website and could change it whenever they liked.

“Your website looks normal to you and your clients, but when Google visits, it’s shown an Indonesian gambling site instead. Someone has broken in and is using your good reputation with Google to promote their betting site.”

How we explained it to the firm. We also asked them to search **site:** and their own web address in Google, on their own phone, so they didn’t have to take our word for it.

The plan

Removing the spam is easy. Stopping it coming back is the real job.

- 1 **Snapshot the infected site** first, as evidence
- 2 **Find and remove the cloaking code** that decided who saw what
- 3 **Replace WordPress, every add-on and the theme** with clean copies
- 4 **Hunt down hidden back doors:** rogue admin users, disguised files, re-infection tasks, code in the database
- 5 **Close the way in:** update or remove the outdated add-ons and turn on automatic updates
- 6 **Change every password and key:** hosting, file access, database, WordPress admins, security keys
- 7 **Check again as Google**, then ask Google to re-read the site through Search Console

We also offered a clean rebuild, which for a site this small can be faster and more certain than forensic cleaning. And we were upfront: removal is quick, but Google can take days to weeks to show the clean version.

The results

One page. One face. The real one.

- ✓ **The firm engaged us** to remove the compromise.
- ✓ **The hidden gambling content is gone**, along with the malicious code that was serving it.
- ✓ **Visitors and Google now see the same page:** the firm’s genuine tax return content.

The lesson: your website can look perfectly fine to you and still be hacked. Cleaning off the spam is the quick part. Ongoing managed hosting and updates are what stop it coming back.

Is your website showing Google something you can't see?

Search **site:** and your web address in Google, on your phone. Pages in another language, or about gambling or things you don’t sell, are a red flag. Spot one? Call us.

Book a free Security Scorecard

1300 313 384

contactus@unitysystems.com.au