



GRO

CASE STUDY

When Fake Sites Go Down, Trust Goes Up:
**How GRO is Winning the
Battle Against Scammers**

GR0 Overview:

Industry: GR0 is an award-winning digital marketing agency best known for SEO and performance growth. GR0's mission is to help "underdog" brands punch above their weight through organic search, content, and integrated, ROI-driven campaigns.

Headquarters: Los Angeles

Company Size: 100–200 employees

Use Cases: recruitment scams, fake sites, phishing URLs, lookalike domains, social media takedowns

Paul Richter — Director of Tech

Mateo Villalobos — Operations Support Manager

// "If you're working at a startup today and working in security, you think **maybe** there's going to be a scammer. But it's really not an "if" issue, it's a "when" issue. And I don't ever think of cyber protection as a frivolous "should we have it or not" spend, because this stuff happens. And every time it happens, it's really bad."

— **Paul Richter**, Director of Tech

Challenge:

Beginning in June 2024, scammers impersonated GR0 and CEO Kevin Miller to run fake recruiting schemes. They spun up lookalike websites and funneled prospects through LinkedIn, Instagram, and Facebook, pushing victims into WhatsApp groups and payment flows.

Impact on people and the business:

- Victims lost between \$200 and \$15,000.
- Daily scam reports created a constant operational burden.
- Angry victims commented on GR0's social channels accusing the company of scamming them, threatening brand reputation, new customer acquisition, and hiring.

"People on our Facebook posts were commenting, 'Don't work with them because they're scammers. They took my money.'"

—**Mateo Villalobos**, Operations Support Manager

"This is an existential threat to the company... If Glassdoor says 'this company scams you,' you can't hire A-level people."

—**Paul Richter**, Director of Tech

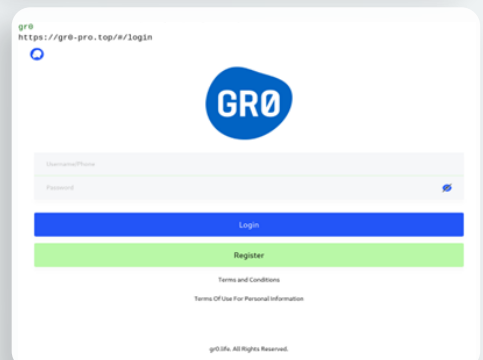
Netcraft Reported

Available for: **1 hour**

Final Outage: **1 hour**

Phishing URL:
<https://gr0-pro.top/#/login>

Hosting Provider:
Alibaba Group



Solution:

GR0 Partnered with Netcraft:

- Netcraft began **rapid takedowns** of lookalike domains and coordinated reporting on WhatsApp groups and social profiles.
- The team managed authorizations directly from Gmail notifications and Netcraft's platform, eliminating the need for manual screenshotting and back-and-forth emails with victims.

"There are short- and long-term costs. In the short term, people might not want to work with you. **In the long term, your reputation suffers.** Some think there's an endless pool of talent, but there isn't—people read reviews on social media and Glassdoor and take their skills elsewhere. The same goes for customers: they see one bad review and pick your competitor instead. That kind of reputational damage can threaten the entire business."

—**Paul Richter**, Director of Tech

Impact with Key Results:



10–20 fraudulent websites taken down in the first two weeks, with an average take-down time of < 2 hours

Scam activity fell by **90%** within 2-3 months

Attacks down **100%**

After the large campaign resolved, reports have fully stopped with only one website popping up on occasion.



1:51 median takedown time

// "The platform is really user-friendly, and communication with the Netcraft team has been extremely good."

— **Mateo Villalobos**,
Operations Support Manager

Teammates recovered ~2 hours per day that were previously spent triaging, documenting, and contacting victims.

// "We just need to make it not economically viable to come after us. They might test it out in another few months, we'll be ready."

— **Paul Richter**,
Director of Tech

Scammers have moved on after seeing rapid, repeated takedowns.

Why Netcraft?

Simplicity

Customized alerting with an easy-to-view dashboard.

Preventative Brand Abuse

Detects and takes down threats before victimization.

Partnership

"Excellent communication" with the Netcraft team.

// "It's harder to rob a house if it has a dog. Burglars can still rob the house, but it will be harder for them to succeed. It might even deter them if there's a Beware of Dog sign; you could have them running pretty quickly. Netcraft is one of those guard dogs for us."

— **Paul Richter**, Director of Tech

Summary

Scammers impersonated GR0 to run fake recruiting scams, siphoning up to \$15,000 from individual victims and harming the brand with public accusations on social media. Before Netcraft, GR0 could collect reports but was unable to remove the fraudulent sites, leaving operations burdened and victims frustrated.

After implementing Netcraft's solutions, GR0 quickly eradicated the campaign: dozens of sites removed immediately; reports collapsed from daily to near-zero, and scammers abandoned GR0 as a target. Netcraft's easy workflow and rapid response restored brand trust, protected prospective talent and clients, and freed the team to focus on growth.



Connect with Netcraft today for greater speed and global reach at scale.

