Fake PCI Compliance Auditors

PCI Comply or Die: The Perfect PCI Compliance Scam
By Nicholas Soulliere
June 24, 2025

A customer I support reported an email to my organization requesting info/explanation.

Original email pretends to be some type of PCI compliance auditor, and trys to direct them to their website (phishing).

Domain in question that was cited in the email, do not visit/click:

managepci . com

Original email:

> From: PayPal PCI Support <paypal@managepci . com>
> Date: June 11, 2025 at 4:52:17 AM EDT
> To: paypalFDM4 paypalFDM4@my-customer.com
> Subject: Action Required: Schedule your mandatory scan as soon as possible
>
> PayPal Global
>
> Merchant ID: 5MRW776K4SM8L
> Forgot your password?
>
> Your mandatory vulnerability scan(s) are overdue.
>
> Dear My Customer Products Inc,
>
> We reminded you recently to complete your mandatory vulnerability scan to maintain your Payment Card Industry Data Security Standard (PCI DSS) compliance. These scans run an external check on the security of your business internet connection.
>
> As of 06/11/2025, these scans are now overdue. Your card payment acceptance set-up requires you to conduct mandatory scans every 90 days
>
> Failure to run these scans could result in becoming non-compliant with the PCI DSS, which will leave your business vulnerable to cybersecurity risk.

Please call us as soon as you can. Your dedicated customer assistance team is available to help with your mandatory scanning tasks. If we don’t hear from you soon, we will continue to reach out by phone and email to help keep your business secure.

Running a Network Vulnerability Scan:

To scan your business network, you'll need to provide your business network’s public IP address (IP.v4). This unique identifier, made up of numbers and periods, is your business network location on the internet.

Finding your IP Address:

There are two main public IP address types:

```
Dynamic IP: This type automatically changes from time to time. Before each scan, you'll need to find your current, public IP address. You can easily do this by visiting www.whatismyip.com.

Static IP: This type remains constant. If your business has a static public IP, you can save it for future scans and avoid needing to look it up each time.
```

Your internet service provider can confirm if your public IP address is dynamic or static.

Running a Website Scan

If you take payments via a website, you will need to scan your website payment pages. If you’re unsure what to scan, we recommend speaking to your web developer to identify the correct domain(s) to scan.

Your next step:

Log in to your online portal at any time to schedule and complete your mandatory scanning activities.

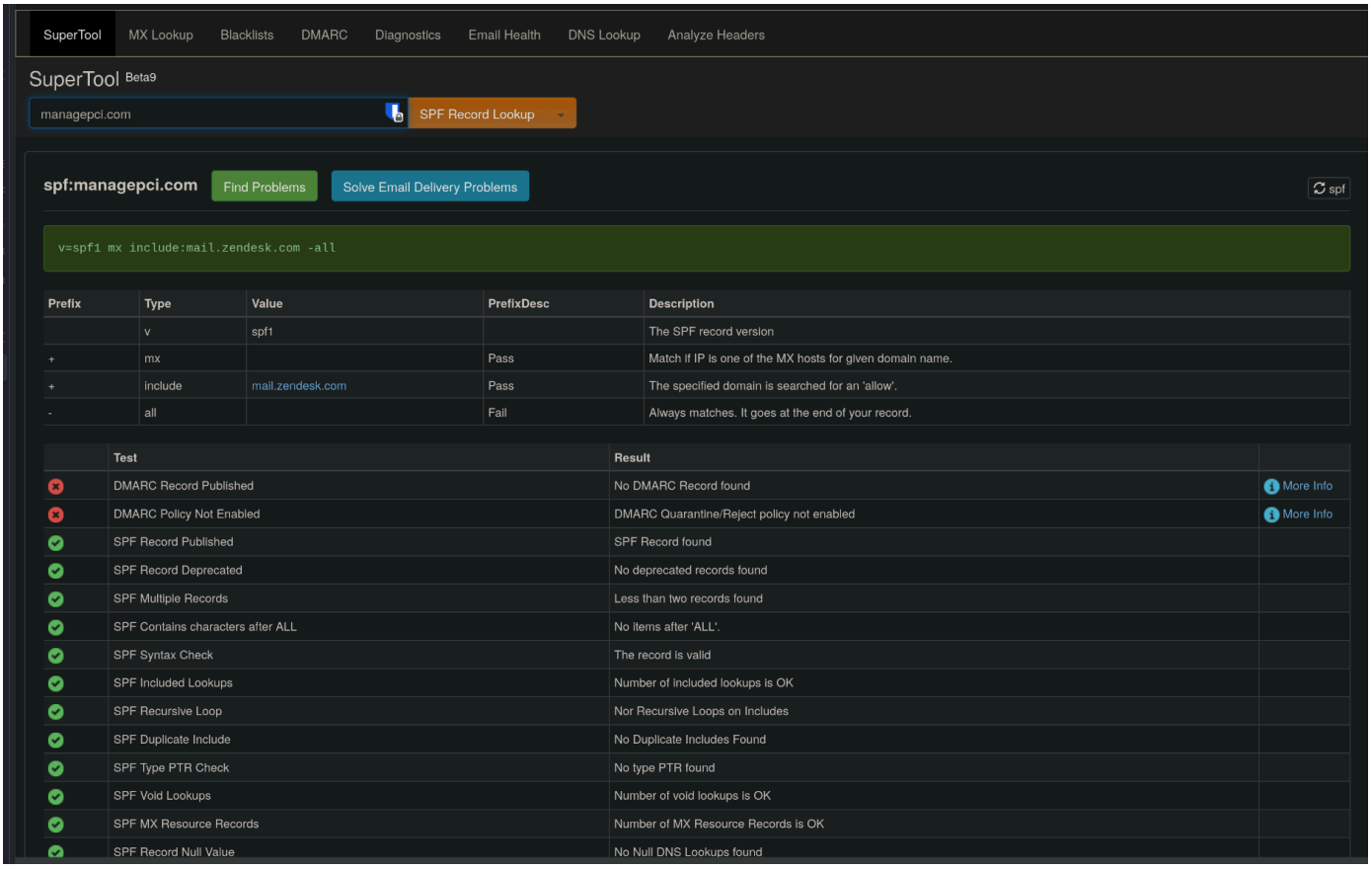
Login
Need Help?
Support Phone 833-770-9555
Support Email paypalsupport@managepci . com

Company Name
My Customer Products Inc
Merchant ID
5MRW776K4SM8L

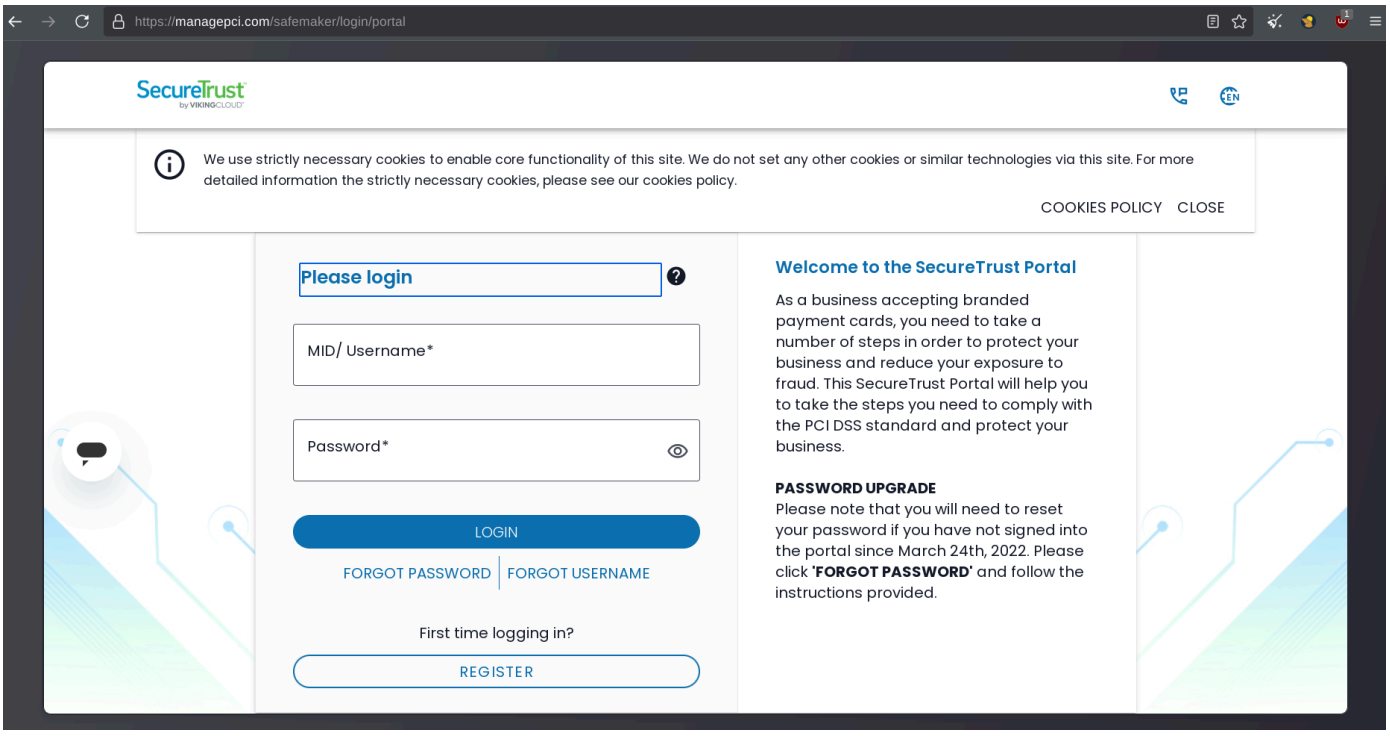
> Username
> paypalFDM4@my-customer.com
>
> Your portal experience has been updated to reflect the latest requirements of the PCI DSS.
> You can find out more about PCI DSS at here.

This is by far one of the best, if not THE best phishing emails I've ever seen. They've got the system down to a T, everything looks so professional.

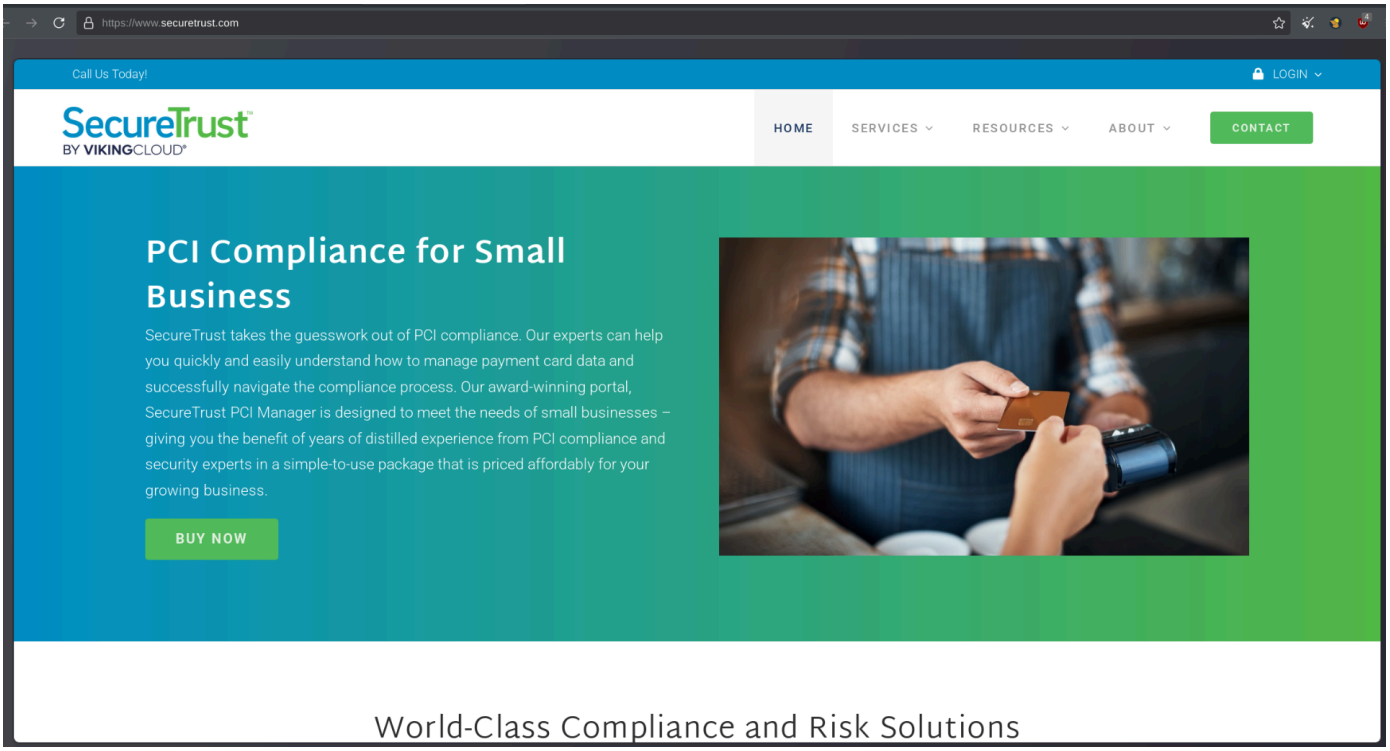
Checking via mxtoolbox.com, looks like that while they don't have a DMARC nor their DKIM records published, they do have their SPF records aligned properly. This all adds to their authenticity and looking credible.



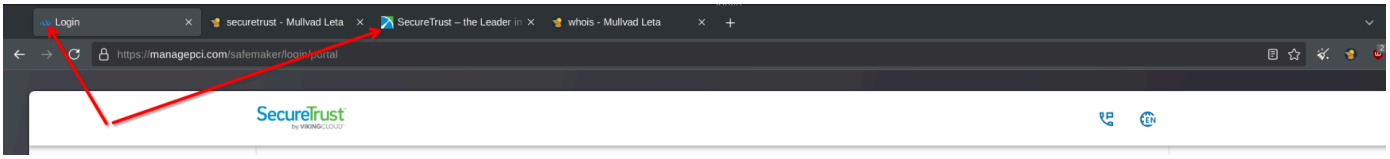
Site is very authentic and professional. SecureTrust by VikingCloud is also a legitimate PCI related entity.



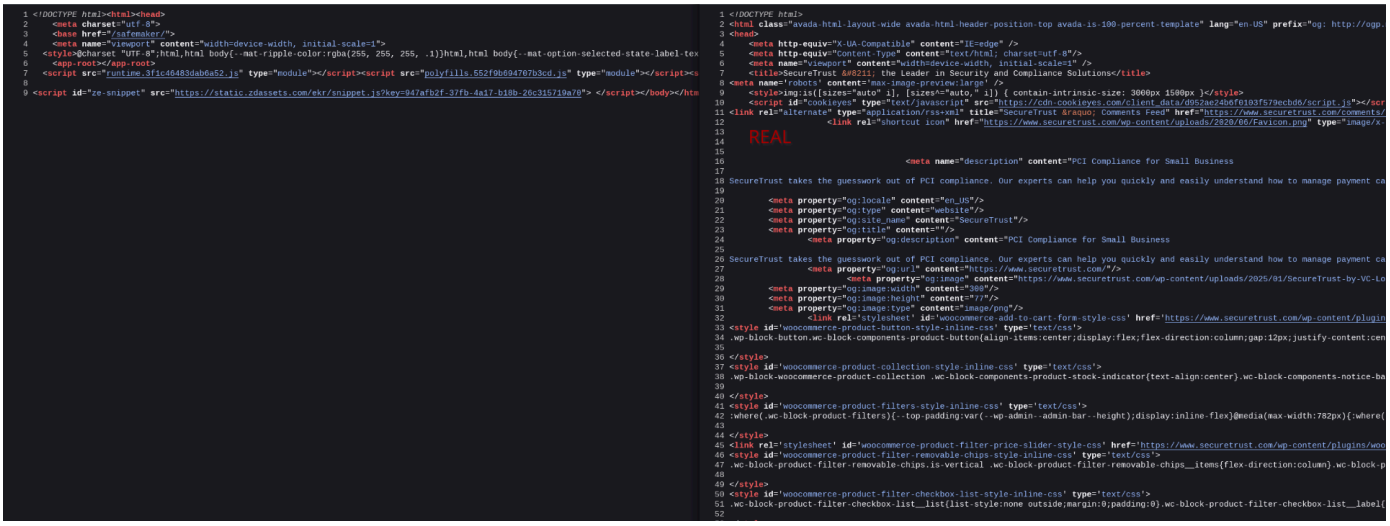
And have a look at the real SecureTrust by VikingCloud:



As always, the devil is in the details. The favicon does not match, its using VikingCloud's default logo, rather than SecureTrust, which is who its pretending to be.



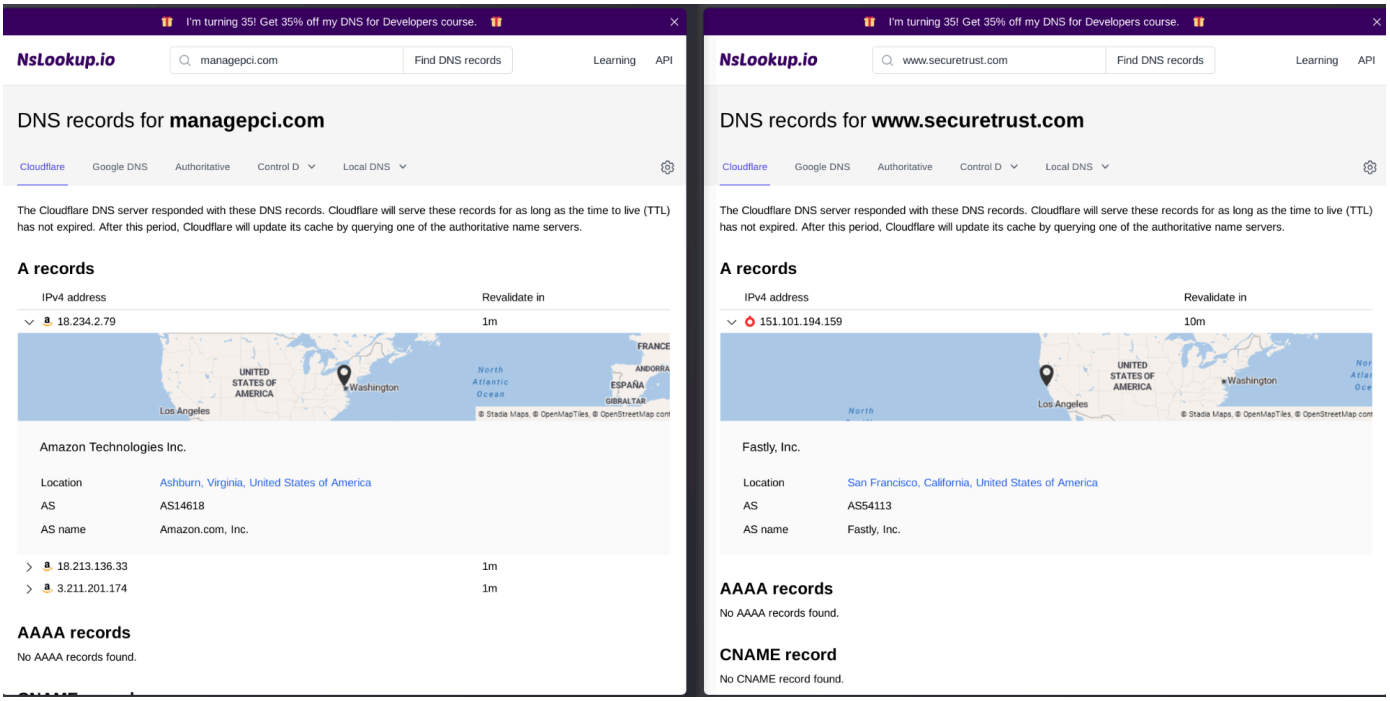
Inspecting the source we can also see its drastically different, fake is left, real is right:



Reviewed the DNS info of both, the scam site is using AWS on the east coast and the real is using Fastly Inc on the west coast.

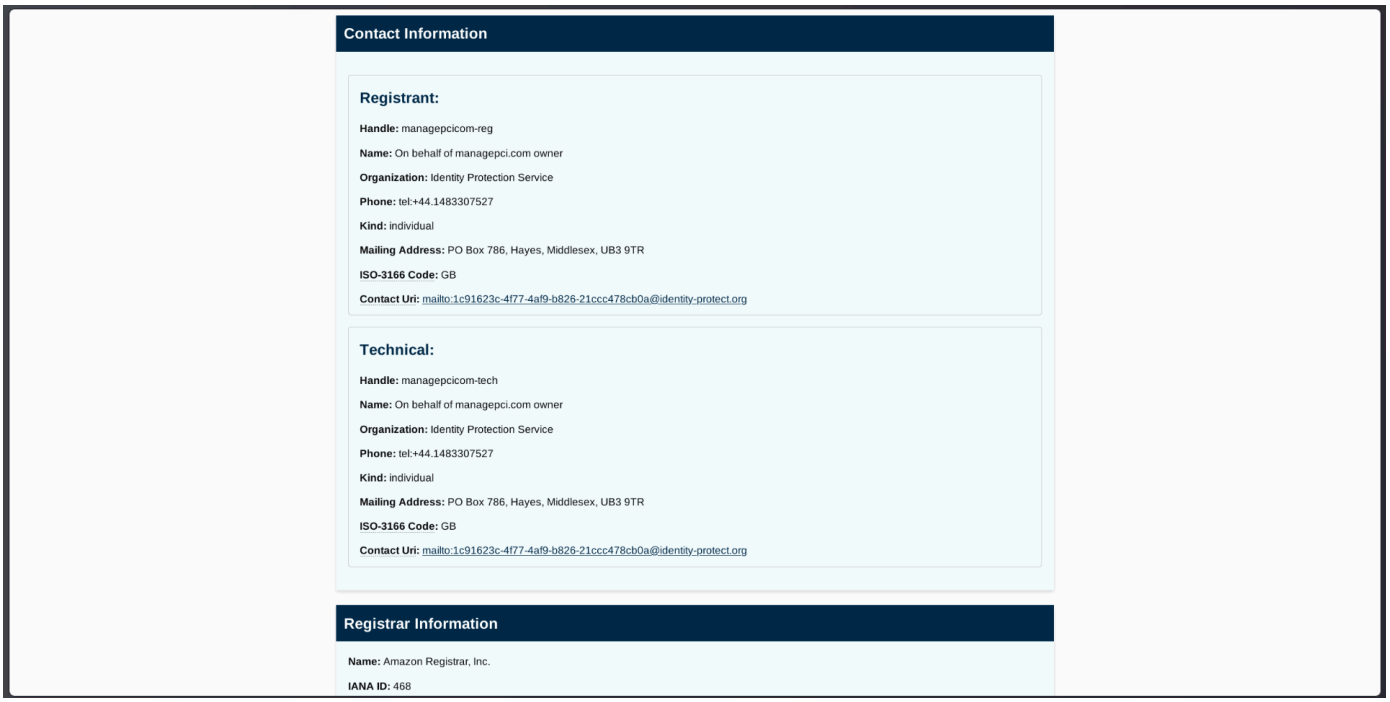
https://www.nslookup.io/domains/www.securetrust.com/dns-records/

https://www.nslookup.io/domains/managepci.com/dns-records/#cloudflare



Entirely falls apart with a basic ICANN lookup as well, checkout the owner of the domain's info.

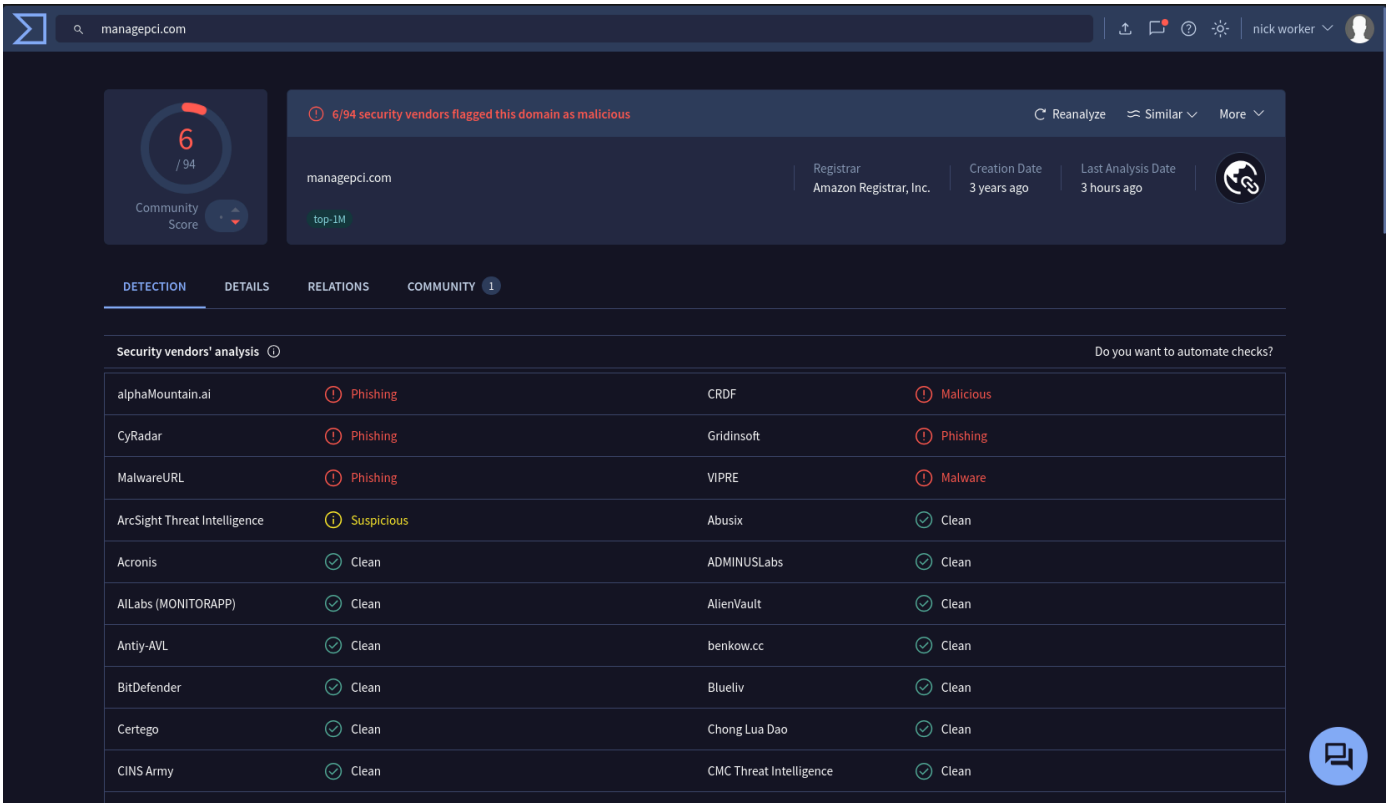
Registered to someone in the UK, with none of the info matching anything mildly legitimate, contact number, email, etc.



---

https://www.virustotal.com/gui/domain/managepci.com

6 hits for a phishing domain is crazy, I typically only see 1-2.



Customer was informed of findings, and advised on cybersecurity best practices.