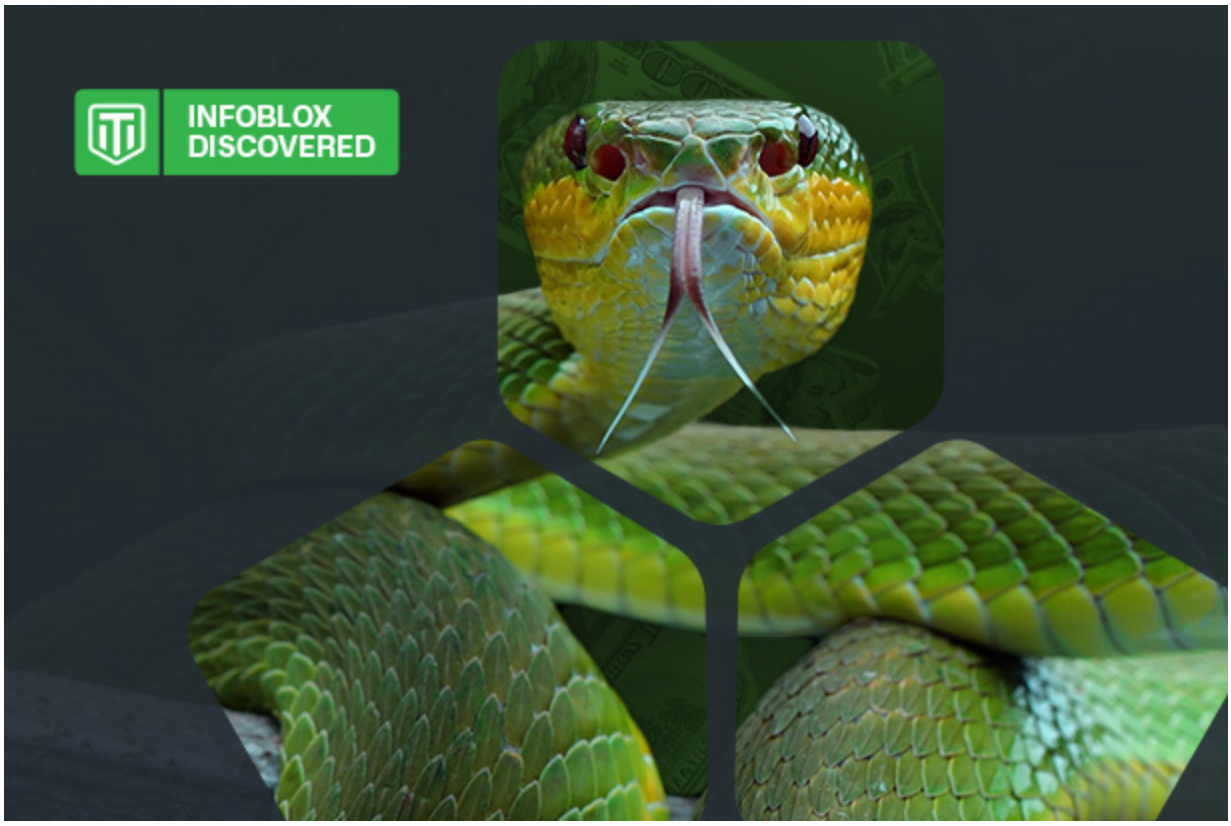
Unsolicited job offers lead to global recruitment scam

blogs.infoblox.com/threat-intelligence/work-hard-pay-harder/

Infoblox Threat Intel March 13, 2025



"We are currently recruiting for a variety of companies for various roles and positions … flexible working hours … training will be provided."

Sounds tempting, doesn't it? A flexible, work from home opportunity that fits in around your busy life and, undoubtedly for many, the perfect side gig to generate some extra income.

No need to dust off the interview jacket or prepare for psychometric assessments so long as you're aged 20 or over, have a local bank account (so far as a bank can be local these days) and presumably have an active pulse—check, check and … check! Basic training will be given and, from what can be seen, the job pretty much entails clicking on buttons—something many, me included, would need little training for. Perfect!

Cybercriminals know full well how appealing this all sounds and are continuing to target individuals globally, stealing their hard-earned money, through recruitment scams that have been operating on a near-industrial scale since at least 2023.

At first, I was expecting little return from this investigation. Instead, I uncovered a vast DNS infrastructure being used to host thousands of active scam sites and was astounded by the sheer scale of the operation.

If you've received an unsolicited job "opportunity" via a messaging service, you are far from alone. Just remember that if it sounds too good to be true, it probably is.

Hello?

Imagine my luck when I received an out-of-the-blue WhatsApp message from an unknown number. In my case a simple "Hello," part of a probing exercise that doesn't show their hand if I were to ignore the message or tell them where to go.

Clearly making a good impression on this (likely) automated process by responding, it was straight down to business. With them posing as a recruiter, I was politely asked (Figure 1) if I would like more information about some remote work opportunities.

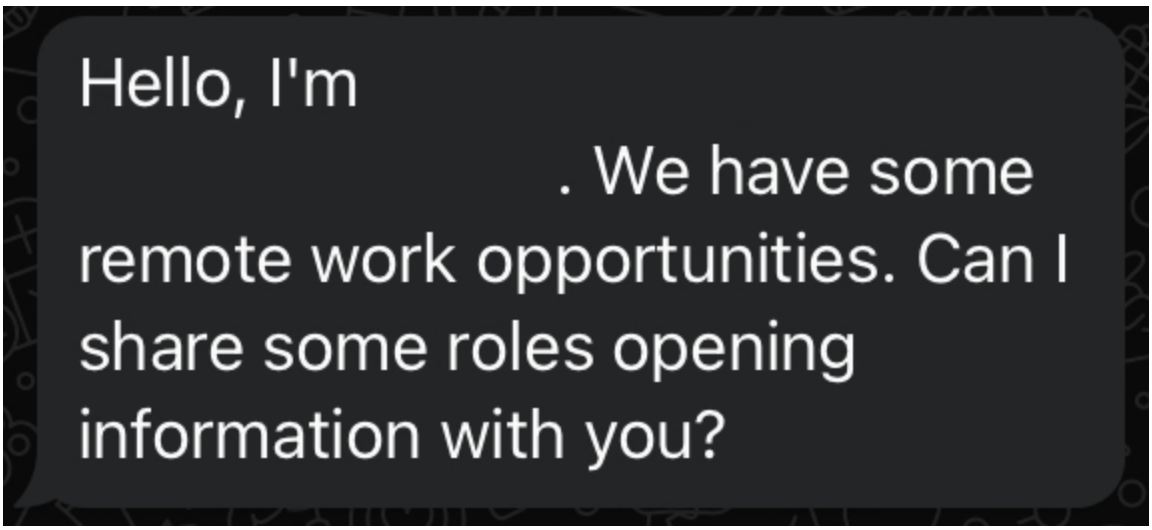


Figure 1: Can I scam you? [WhatsApp message]

Not being one to miss out, I eagerly confirmed my interest, but not before doing some due diligence that confirmed the use of a legitimate recruitment company name.

It is important to note that this legitimate company, and those encountered later, are not involved in these scams other than their brands being abused.

After being provided with their checklist (Figure 2), a step less about finding top-quality job candidates and more about finding suitable victims, the scammer, or more likely their automated process, hands me over to a seemingly human agent to gain further trust and reel me in.

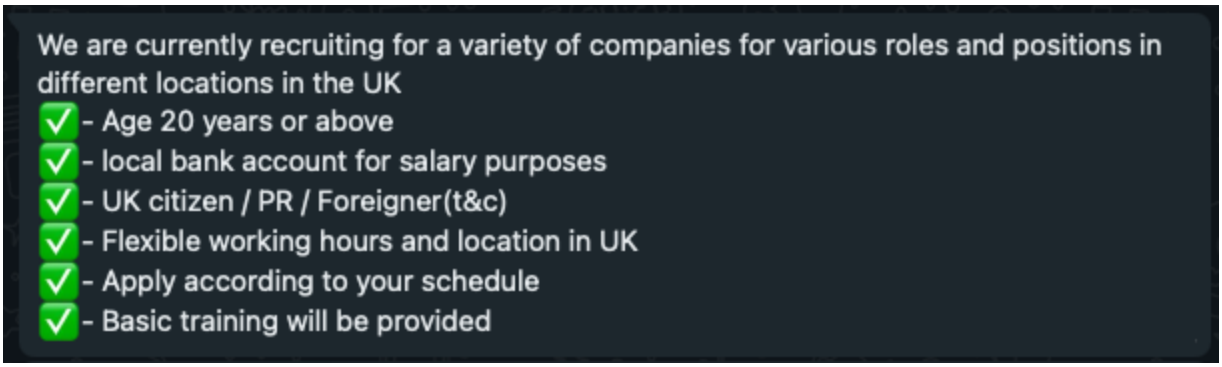


Figure 2: Desired victim checklist [WhatsApp message]

No Prior Experience

Yet again confirming my interest, a tactic used repeatedly during the scam to create a sense of commitment and investment, the messaging tempo increased to engage and encourage me toward accepting the role—no prior experience, no formal interview, no background check, no typical recruitment process.

No doubt varying slightly from interaction to interaction, especially given the scammers operate worldwide, and to save you from the small talk, the gist of the engagement process includes somewhat consistent elements and features:

1. **Building Trust**
   The scammer provides a link to a legitimate business website to add credibility to their pitch and build trust. At the time of writing, these businesses operate in the digital marketing, e-commerce or search engine optimization (SEO) industries. Previous campaigns mimicked the hospitality and travel industries, and future campaigns will undoubtedly evolve and shift to provide fresh opportunities in exciting new industries.
2. **Keep It Friendly**
   Many scammers, especially those plying their trade by telephone, often become agitated and annoyed at a lack of engagement, sometimes using anger and intimidation to coerce victims into continuing. In this case, the scammer maintained a friendly tone throughout and repeatedly prompted me to confirm I understood. When I didn't respond for a day or two, they gave me gentle reminders to encourage me to continue with the process.
3. **Plausibility**
   The job was pitched as requiring us to perform tasks, such as clicking links or submitting data, which sounds simple enough … perhaps too simple? To add to the job's plausibility, the scammer uses technical jargon like "complex data integration algorithms," perhaps implying that the "machine" handles the difficult work while I enjoy the rewards with just a little bit of commitment.

4. **Cryptocurrency Setup**
   The scammer wants to give the impression that I'll be paid and offers to guide me through setting up a cryptocurrency wallet. Their recommendations appear to be region-specific, in my case suggesting the use of Crypto.com, and I was directed to download the application rather than being providing with a dubious-looking link.
5. **Enticement**
   Finally, details of the salary, bonus and commission appear both reasonable and enticingly lucrative. While initial figures were provided in my local currency, on-the-job transactions are conducted using the stablecoin Tether (USDT).

We expect scammers to avoid traditional payment methods because bank transfers can be tracked and potentially reversed. As for why Tether is the scammer's cryptocurrency of choice, they attempt to provide an explanation within the scam portal (Figure 3).

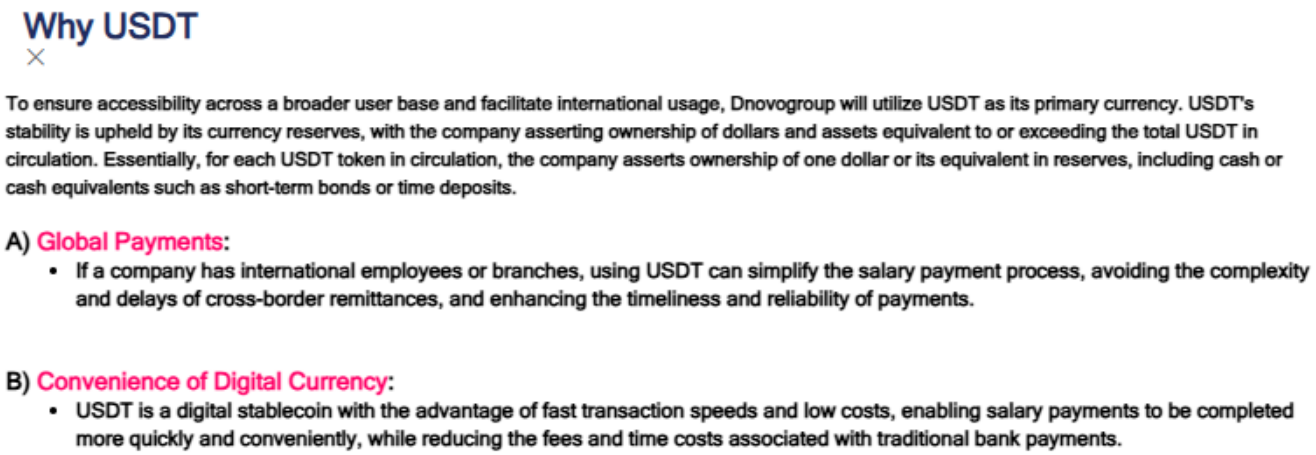


Figure 3: Explanation of why to use harder-to-track USDT [Scam portal]

This is, of course, all part of the illusion of legitimacy. The scammer likely prefers Tether as it is pegged almost one-to-one with the U.S. dollar, making it easy to understand for those of us unfamiliar with crypto-markets and avoiding the volatility of Bitcoin (BTC).

Now knowing how I'd be paid—or more to the point, not paid—it all sounded like an opportunity too good to miss and I was more than happy to proceed. Although I wasn't in a position to accept their offer of immediate training, mainly because the constant message alerts were making me look too popular, I was keen to take a quick peek at their website and get myself set up "later" …

How Big?

Given the scammer's efforts so far, it was clear that this was not the work of an opportunistic individual. I suspected that this was likely bigger than just one or two domains, especially considering how quickly things can be shut down after victims start complaining of losses.

Saving analysis of the website for later, the first thing any self-respecting Infoblox Threat Intel researcher does is investigate the DNS side of things. In this case, the provided portBuiuldinCryptoal domain was a veritable treasure trove of pivots due to the large scale of the scammer's infrastructure and how it has been configured and managed.

Starting with the IP addresses that the portal domain resolved to (Figure 4), it was evident that hundreds of similarly structured domains were active at any one time, mimicking numerous brands.

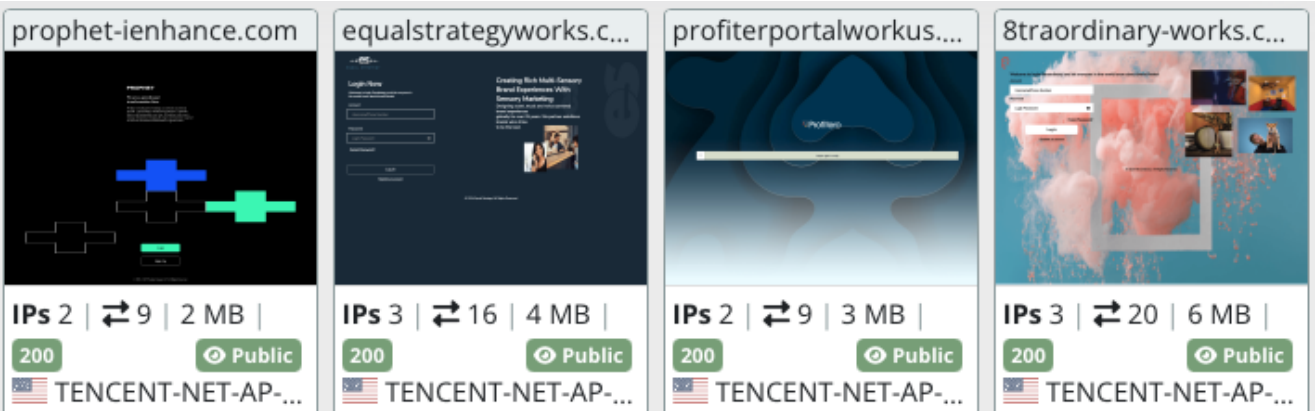


Figure 4: Example IP pivot linked to additional scam domains [URLScan]

Consistent with the scammer's current theme, the majority of these observed brands were operating in the digital marketing, e-commerce and SEO industries. It was also evident that the scammer is not focused on abusing brands or targeting victims in any particular country or region. Abused brands were observed to be headquartered across Asia, Europe and North America, many of which also had a global presence. This allows the scammer to target victims with a brand that would appear plausible should anyone conduct due diligence checks.

Digging deeper into the registration records and the IP addresses these domains resolved to, it became clear that the scammer has specific preferences when setting up their scam domains:

- Use GNAME, a Singapore-based domain name registrar, for domain registration
- Use DNS.com, a China-based DNS infrastructure provider, for name servers
- Often using Tencent and/or Alibaba Cloud, both China-based hosting providers, for hosting
- Occasionally using Cloudflare, the popular global network service provider

Leading to countless more domains associated with this scam, these preferences along with a certain familiarity in their domain naming patterns make it easy to spot clusters of scam domains when investigating.

Further investigation into these domains revealed two intriguing infrastructure patterns: the use of canonical name (CNAME) records and HTTP redirections. These suggest the presence of second-tier infrastructure hosting multiple scam sites, likely simplifying the scam network management and potentially providing some resilience to takedown efforts.

Specifically, the scammer uses ThinkAdmin, a popular Chinese web development framework based on ThinkPHP. This provides an efficient way to deploy new scam portals using a simple template-like structure that can easily be adapted to mimic new brands.

While the scam domains have a reasonable shelf-life, remaining active for long enough to convince someone they're legitimate before stealing from them, the second-tier infrastructure allows domains to be discarded if overly exposed or taken down, and new ones introduced to maintain a healthy pool of fake employers.

Second-Tier Infrastructure

The first indication of second-tier infrastructure I encountered was the discovery of DNS CNAME records (Figure 5) mapping to just a handful of domains, their own content delivery network (CDN) of sorts.

```
prophethostsg.com.          300     IN      CNAME   yy.gtm-yy.cn.
yy.gtm-yy.cn.               600     IN      CNAME   gtm-cn-bcd4043nv01.gtm-yy.cn.
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.246
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.250
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.247
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.251
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.254
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.252
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.248
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.234
gtm-cn-bcd4043nv01.gtm-yy.cn. 60 IN     A       31.42.185.236
```

Figure 5: I dig it, totally!

Having (dig) dug into a large number of domains identified through my earlier pivots, and armed with the CNAME records, it was time to delve into passive DNS (pDNS) and other data sources to determine what else might have been pointing their way.

Analysis of these CDN-like domains provided the golden key, unlocking links to over 9,000 domains, with at least a third seemingly active at any given time and new domains being added at a steady pace.

Over the past year, there have been several months wherein the actor added large clusters of over 1,000 brand-mimicking domains, which could indicate new phases of the scam campaigns and pushes for new victims. In between these large changes, smaller clusters of

domains (often tens of domains rather than thousands), appear to have been added on an ad-hoc maintenance basis.

While these CDN-like domains are mainly used for this large-scale recruitment scam, illegal Chinese gambling domains were also observed as being associated with some subdomains. Although this link may be anecdotal, we have previously identified similar activity as being associated with Vigorish Viper, a sophisticated actor with links to Chinese organized crime.

The scammer seems to favor the CDN-like hosting structure, as evidenced by the large number of associated brand-mimicking domains, but this was not their only method of maintaining their scam infrastructure.

In many cases, and seemingly when using Cloudflare to front their scam domains, I observed sites redirecting visitors with either an HTTP 302 response or a combination of HTML and JavaScript (Figure 6).

```
<html lang="en">
  <head>
    <meta http-equiv="refresh" content="0;url='https://[RANDOM_SUBDOMAIN].[2ND_TIER_DOMAIN].[cyou|icu|sbs]">
    <title>56132</title>
  </head>
  <body>
    <script>
      window.location = 'https://[RANDOM_SUBDOMAIN].[2ND_TIER_DOMAIN].[cyou|icu|sbs]';
    </script>
  </body>
</html>
```

Figure 6: HTML and JavaScript redirection

These redirections, similar to the CNAME method, take victims from the recognisable brand-mimicking domain to subdomains and domains that appear to be created by a registered domain generation algorithm (RDGA) and are predominantly under the top-level domains (TLDs) “.cyou,” “.icu” and “.sbs.” The structure and pattern of these domains suggest the use of automated tools to create and register them in bulk.

The reasons for mixing and matching the methods of getting victims to their second-tier infrastructure are not clear at this point. Aside from the management and resilience advantages, a few working theories include:

- Shifting from their own CNAME and CDN-like infrastructure toward Cloudflare and the redirect DGA-like domains once a portal becomes popular
- Planned migration from one method to the other over time
- Different administrators favoring one method over the other
- They just like to mix it up and keep us entertained

Having finally made it to the scam portal, I was prompted to register an account. Of note: A user could not do this without having first engaged with the scammer via WhatsApp. To prevent casual snooping, new accounts require a valid referral code. Without it you'll be stuck staring at the main page.

Once registered, I was free to browse the site and marvel at the potential future job that awaited me. Unfortunately, having put off my "training" for far too long and neglecting my duties as a diligent employee, the scammer went cold and stopped answering my messages. Sad face.

Conversely, gaining access to the portal did provide enough leads and insights into their general operations, especially the help and tips sections (Figure 7).

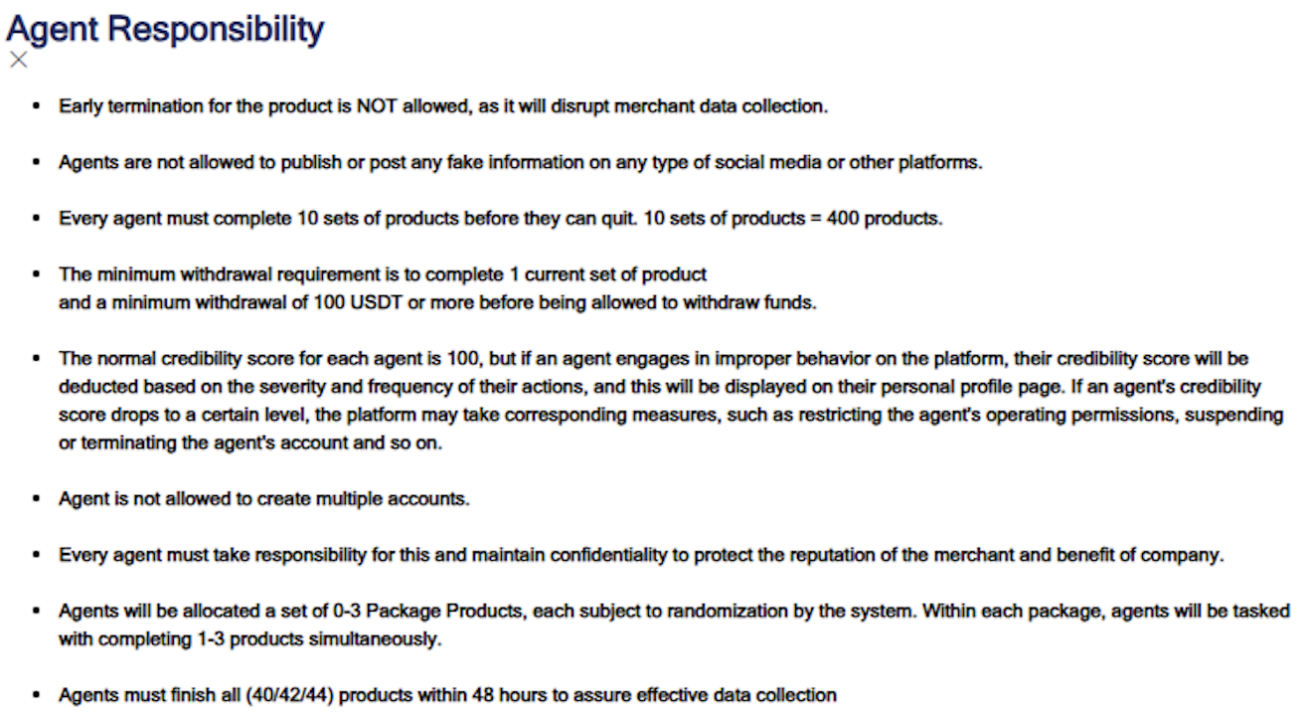


Figure7: Don't worry (point 2)—this article is factual! [Scam portal]

It seems that further exploration of the portal site and discovering what exactly the "job" entails will have to wait until I can find a new recruiter.

So, What's the Catch?

Much like a pig-butchering scam, where the victim is "fattened up," the scammers are manipulating people into willingly paying them under the illusion of legitimate work and increased earnings.

Rather than asking outright for money, something that everyone would be wary of, framing the scam as a job opportunity and appearing to pay a small initial reward builds trust and makes the whole thing appear real.

Having funds appear in your account is a great psychological trick; it must be OK if they're giving me money up front.

After completing a few small tasks and settling into the idea that this will truly be an easy-money gig, the scammer will let you know about the bigger rewards … and here is the catch! To unlock the higher-tier task and get your hands on those sweet higher rates, I'd need to invest more of my own money.

This is when our friendly human agent would lay it on thick, telling me that the more I invest, the more I can earn. By prepaying, I'd be gaining access to exclusive tasks, and everything is safe because payouts are "guaranteed."

Seems reasonable, perhaps? Everyone knows you have to speculate to accumulate.

Further demonstrating their clever use of psychology, people who do invest would start to see a return and believe that all is good. In reality, things would be far from good. Attempting to withdraw earnings from the portal will trigger the scammer to make their final attempt to extract even more money through:

- Withdrawal restrictions—the victim will need to upgrade their account to VIP status to be able to get access to the crypto-cash. This of course comes at a cost.
- Fees—the victim will need to pay service charges or taxes before they can make a withdrawal.

Surely these payments could be taken from the existing account?

The victim has already invested large sums of their own hard-earned money expecting a big payout. This is where some victims would go "all in" to chase their losses while the scammer tries to squeeze them for as much as they can get.

Rather than asking for unreasonably large sums early on, they've been gradually increasing the buy-in while keeping the victim's eyes fixed firmly on the prize pot—an unobtainable reward for what they believed to be honest work. Once the scammers are done, they ghost the victim, and as for the invested money, well that's long gone.

Out of the victim's bank and into unrecoverable cryptocurrency, probably moved into other cryptocurrencies before making its way into the large grubby paws of those responsible.

We're not talking small numbers either, with the portal's Withdraw help page (Figure 8) mentioning Tether amounts of 5,000 USDT, 10,000 USDT and 15,000 USDT: likely target amounts to try and squeeze out of each victim.

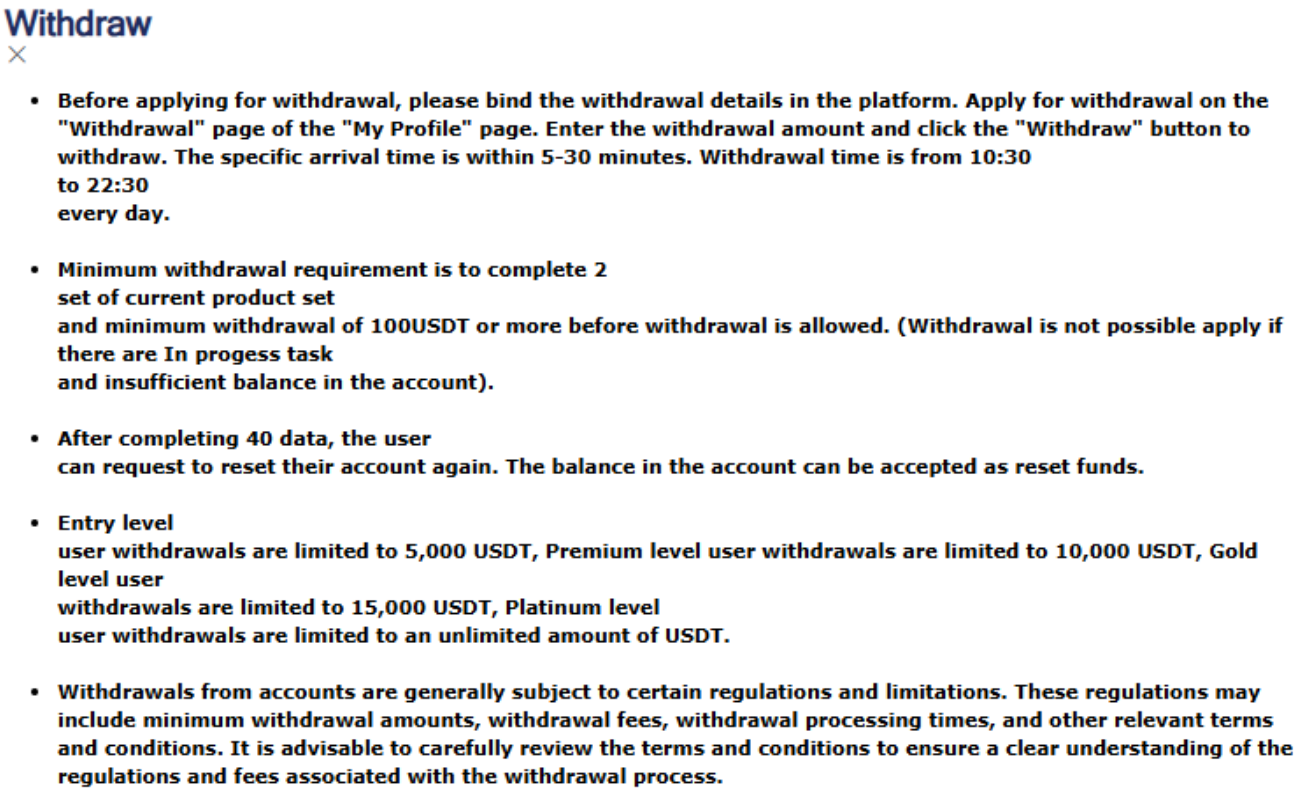


Figure 8: Good luck withdrawing anything like these amounts [Scam portal]

Considering the number of domains I discovered, the likelihood that each portal has multiple victims “working” on it, and the assumption that at least a couple invest a significant amount, the ill-gotten returns for this scam could be astronomical.