LY FORENSICS

ANALYSING SCAMS

INVESTIGATION OF AN ACTIVE COINBASE PHISHING SCAM

DATE:
11 Dec 2024

WRITTEN BY :
Marcus Kalman

1300 168 380 Option 4
lyforensics.com.au

Report Objective

This report was published by LY Forensics (formerly trading as Blockstars Forensics) and prepared by a Blockstars Forensics analyst.

It was developed to raise awareness of an active phishing campaign involving the impersonation of the legitimate cryptocurrency exchange, Coinbase.com. The report outlines the investigative steps taken by our team in response to the targeted phishing attempt and presents our key findings.

No exploitation activities were conducted during this investigation. All analysis was limited to reconnaissance of publicly available information, including the examination and enumeration of the scammers' source cod

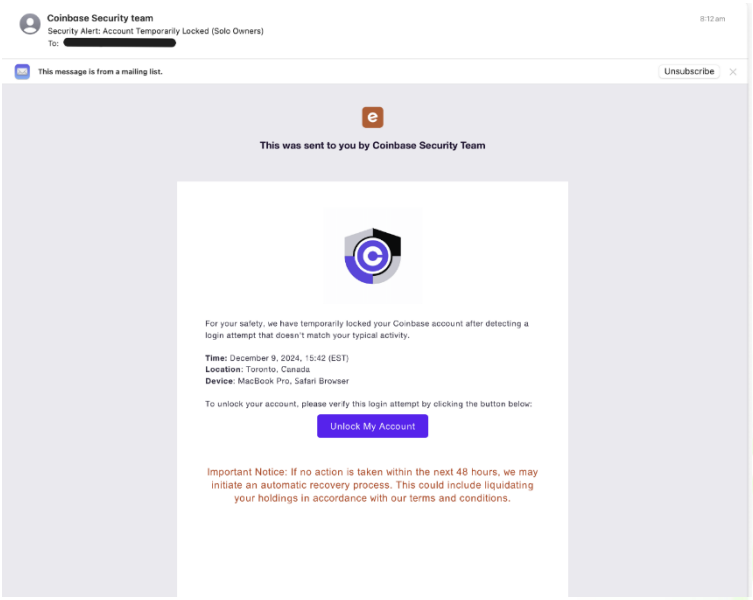
Please note that this is a real scenario and is intended for educational purposes only. It demonstrates what these scams look like and how they operate based on observations. All links provided in this report should **NOT** be interacted with. Use this report solely for learning and understanding how to stay safe from such scams.

During this investigation, our team utilised a secure, external Virtual Machine to conduct all testing. Best practices and security procedures were strictly followed and thoroughly verified upon completion.

Please also note throughout this report, we make mention of both Coinbase and Eventbrite. Both these companies are legitimate and are **NOT** tied to this scam.

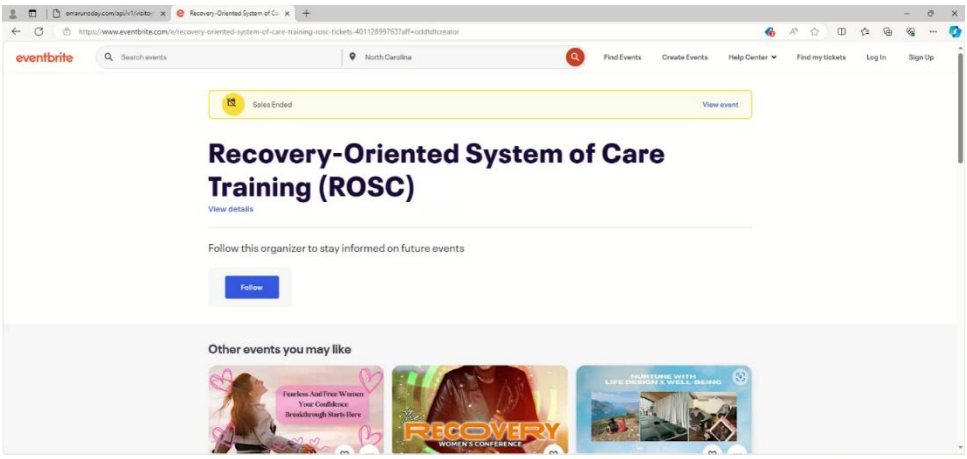
Scam Initiation

A client recently received an email claiming that their Coinbase account had been locked due to an “attempted login” that did not match their “typical activity.” Naturally, they suspected this to be a scam, so our team decided to follow the rabbit hole a bit further.



Screenshot of the initial email

The email was sent to a personal email address, with the display name spoofed as “Coinbase Security Team.” Upon further investigation, we found that the actual email address was “noreply@event.eventbrite.com.” Interestingly, the subdomain “event.eventbrite.com” redirects to the legitimate Eventbrite website.



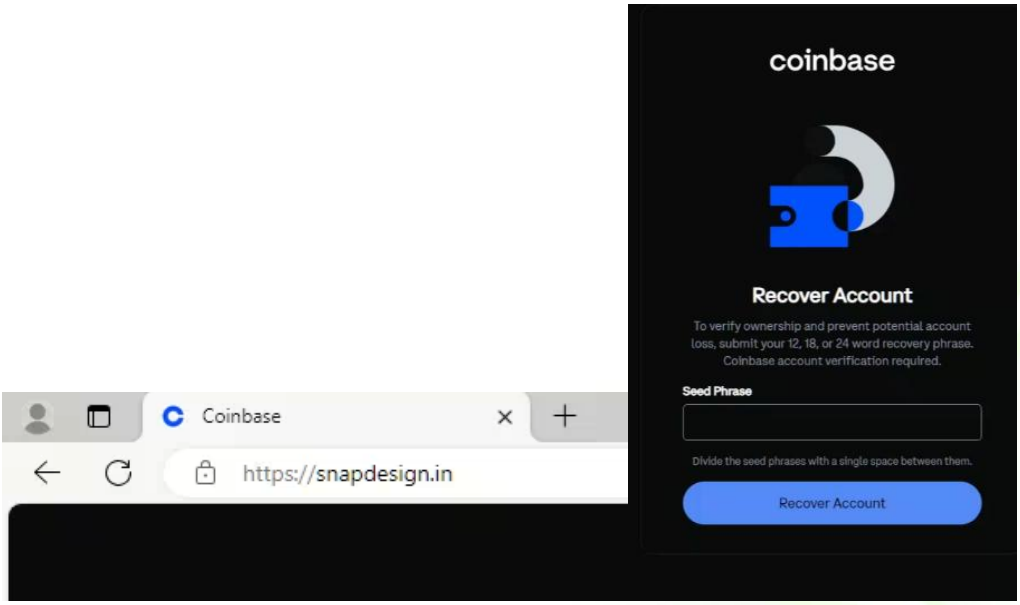
The eventbrite.com domain

The Eventbrite site itself appears to be legit. However, using the event management system within Eventbrite, these scammers simply added target emails to their events (in this case, a Coinbase scam) and used the service to send out these phishing emails. This is a unique strategy, disregarding traditional platforms such as SendGrid or others.

Now we have identified the email contents as suspicious, lets dive deeper into the link itself and see if we can understand their intentions closer.

Down the Rabbit Hole

Upon opening the link from the provided phishing email, we notice a few things. One obvious observation is that this site looks very similar to a Coinbase form:

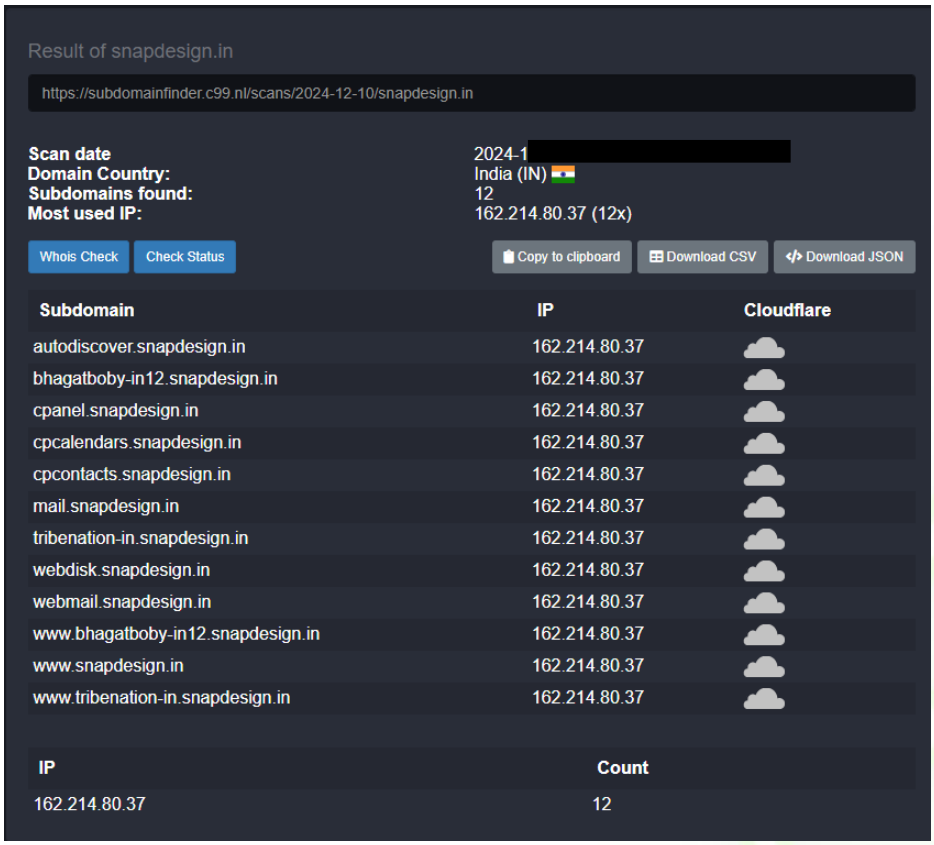


The spoofed Coinbase site

The first red flag was the immediate request to submit a wallet seed phrase. No legitimate exchange, including Coinbase, would ever request this information in such a manner (or at all) in this type of scenario.

The second issue was the URL. The “snapdesign.in” domain clearly has no resemblance to “coinbase.com.” It seems the site is relying on desperate targets acting quickly, believing they are recovering their accounts, without taking the time to notice subtle details like the URL itself. This suggests that this Coinbase scam is ongoing and that the scammers may be rotating between random domains.

Further reconnaissance revealed 12 subdomains associated with the parent domain “snapdesign.in”. Most of these subdomains appear to have been recently discontinued, although their certificates remain valid.

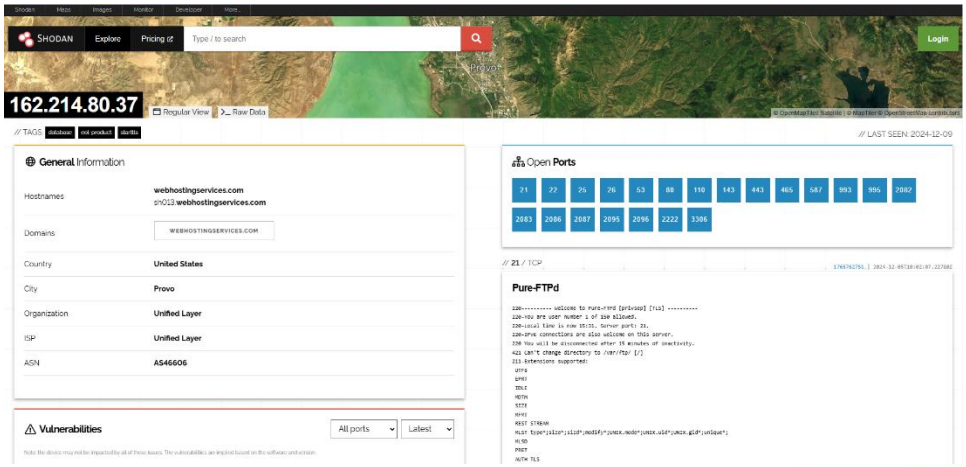


Using Sublist3r to view subdomains and metadata

The team also noticed that the domain's country of origin is listed as India, although other WHOIS data has been redacted.

An analysis of the subdomains reveals they host various services, including webmail, control panel services (cPanel), drive mapping (via cPanel), and other functionalities.

To delve deeper, the team examined the associated IP address using Shodan, which provided access to all publicly available records linked to it.

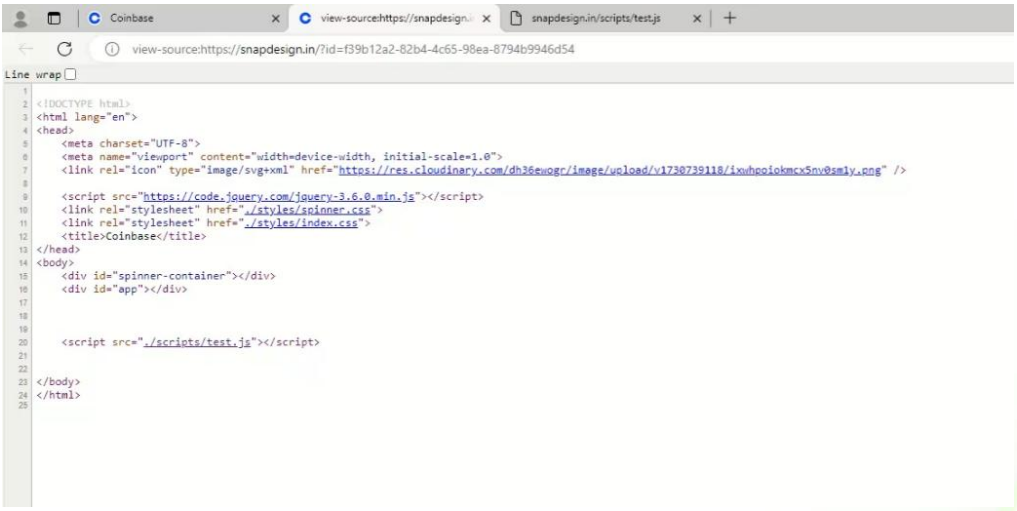


Using Shodan to view public records of target IP address

We found many ports open on the IP address “162.214.80.37”:

- **21** Pure-FTPd
- **22** OpenSSH
- **25** Exim smtpd
- **26** Exim smtpd
- **53** TCP
- **53** UDP
- **80** Apache httpd
- **110** TCP
- **143** TCP
- **443** Apache httpd
- **465** Exim smtpd
- **587** Exim smtpd
- **993** TCP
- **995** TCP
- **2082** cPanel
- **2083** cPanel
- **2086** WHM
- **2087** TCP
- **2095** Webmail Login
- **2096** TCP
- **2222** OpenSSH
- **3306** MySQL

Circling back to the phishing site, we aimed to enumerate through the source code.



Snapdesign.in source code

Fortunately for us, there wasn't much to analyse aside from their scripts, as shown in the screenshot above. One file stood out: "./scripts/test.js", which seemed particularly interesting at this stage.

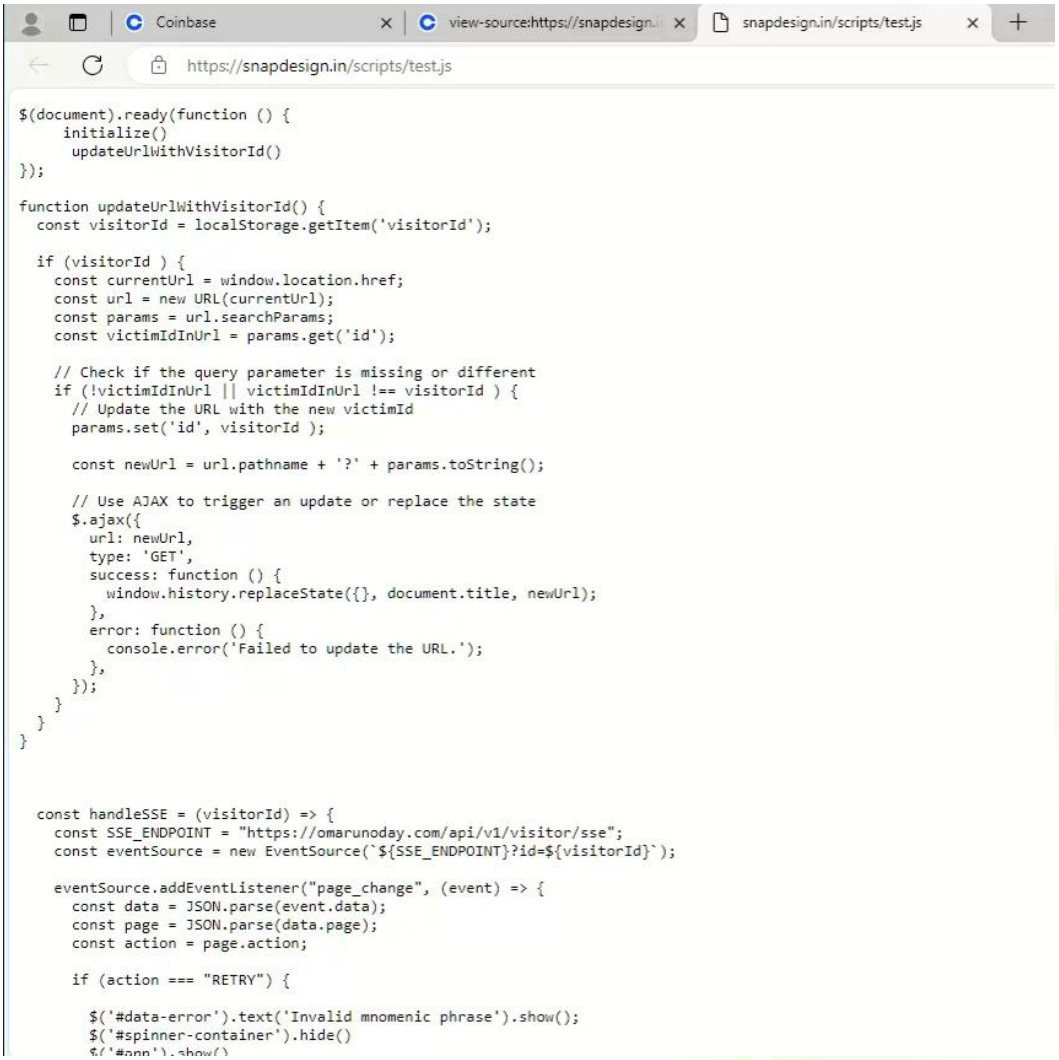
Navigating to "snapdesign.in/scripts/test.js", we found a ~400-line JavaScript file. Upon reviewing the code, it was clear this was a scam. The syntax blatantly referred to the current user as a "victim," using terms like "victimIdInUrl". It's almost as if the scammers weren't even trying to obfuscate their intentions anymore or was just outright lazy.

Further analysis of the script revealed two API endpoints. Both endpoints include parameters for a visitorId, which appears to be randomly generated using a salting function.

1. **GET** https://omarunoday.com/api/v1/visitor/**sse**?id=visitorId
2. **POST** https://omarunoday.com/api/v1/visitor/**hello**?id=visitorId

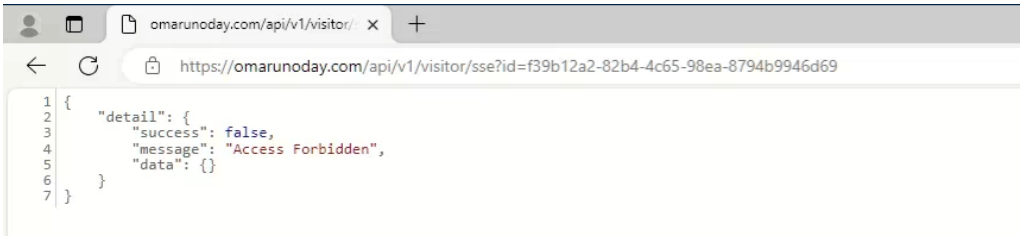
Apart from this, we also identified another POST request for pushing the seed phrase payload.

3. **POST** https://omarunoday.com/api/v1/visitor/**push**?id=visitorId

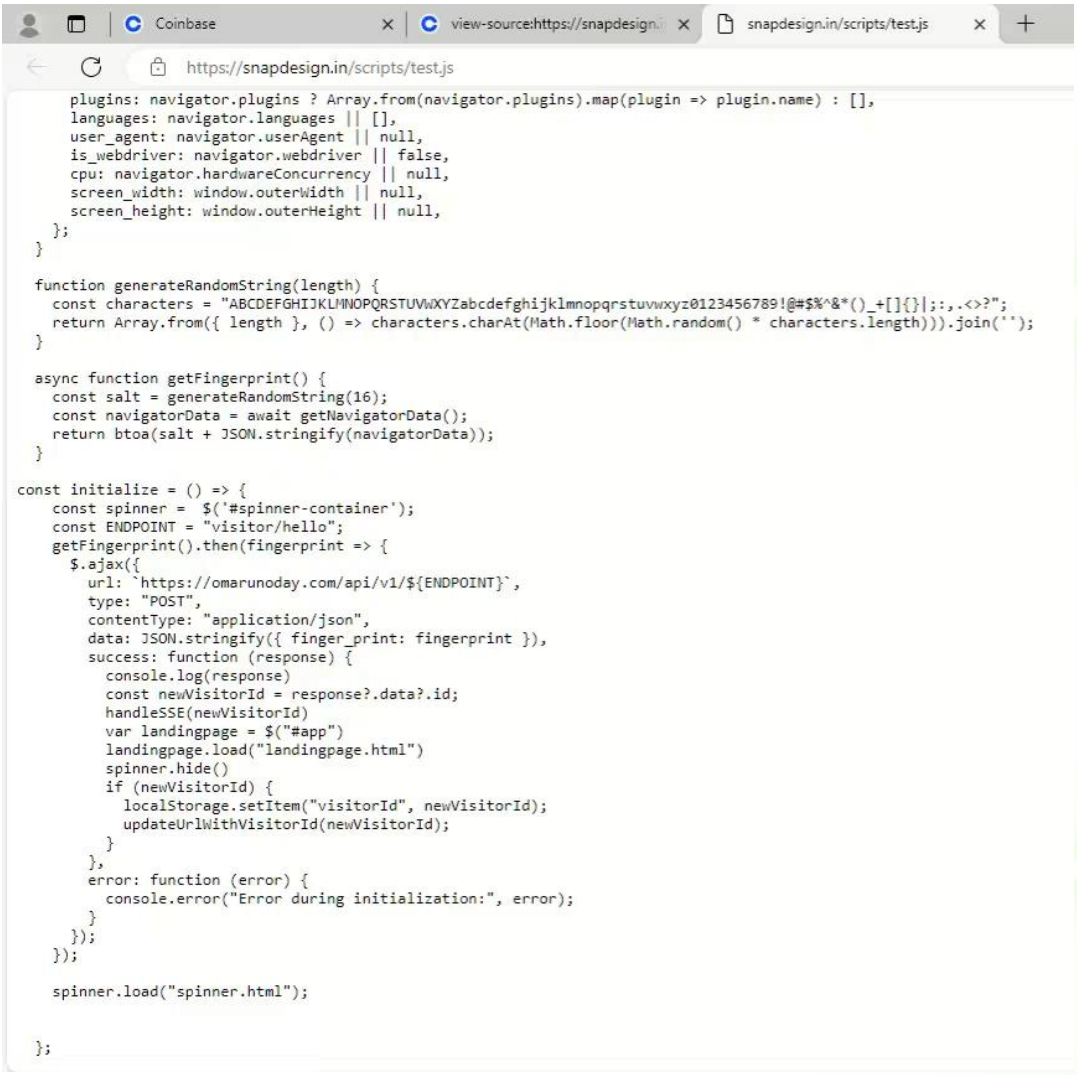


The first half of the test.js file containing the GET req

Here, the team identified a **GET** request endpoint that appears to set up a "Security Service Edge" (SSE) for visitors accessing the page. When tested with a valid, generated “visitorId”, the SSE endpoint responded with an "Access forbidden" message, as shown below:



Response from API using existing visitorId



The second half of the test.js file containing the POST req

During the analysis of the second part of the “test.js” code, we discovered that the “initialize” function is a part of the core mechanism of the scam. This function is designed to collect and post victims' seed phrases directly to the scammers' database. No other request methods are accepted, confirming its sole malicious intent.

Conclusion

The investigation into the spoofed Coinbase email, which led to the “snapdesign.in” phishing site, has provided valuable insight into how these types of scams operate. By diving into the various elements of the scam, such as the subdomains, scripts, and API endpoints, our team was able to uncover the methods these attackers use to manipulate unsuspecting users. This report outlines the basic steps and techniques used in this phishing attempt, showing the processes that occur at face value.

One crucial aspect of the investigation was identifying and analysing the subdomains. These subdomains not only revealed the infrastructure behind the scam but also highlighted how attackers leverage legitimate services like Eventbrite to conduct their malicious activities. The use of a domain like “snapdesign.in,” which doesn’t even remotely resemble the actual Coinbase domain, serves as a red flag. However, many victims may overlook this detail in their rush to recover an account, which is why it’s important to pay attention to even the smallest inconsistencies, such as a suspicious URL. These scams rely on creating a sense of urgency, hoping victims will act quickly without scrutinising the details.

Additionally, the rotating domains used by these scammers are another tactic designed to evade detection. By jumping between random domains and utilising subdomains associated with legitimate services, the attackers can maintain the illusion of legitimacy and evade traditional spam filters or security measures. Recognising domain rotation is key to identifying ongoing scams that may not have a fixed URL.

Platforms like Eventbrite, typically known for event management, are also being exploited. Scammers can easily create events under false pretences and use them to distribute phishing emails to large groups of potential victims. This approach bypasses traditional email service providers and increases the perceived credibility of the scam, as Eventbrite is a well-known and trusted platform.

This serves as a reminder that even seemingly legitimate services can be misused by malicious actors, which is why it's important to be cautious when receiving unsolicited emails or messages, even if they appear to come from trusted sources.

Throughout this investigation, we utilised various tools and methods, such as Shodan for IP address analysis and manual inspection of the source code, to dig deeper into the scam's infrastructure. By reviewing the "test.js" script and identifying its core functionality which posted victim seed phrases to the scammer's database. we were able to understand the specific actions the scam was designed to carry out throughout this process. This level of detail is necessary to comprehend the full scope of the attack and provide actionable insights for others to avoid falling victim to similar scams.

This investigation was not intended to provide a deep technical analysis, but rather to give a foundational understanding of a real, ongoing scam. The tactics used here, such as domain spoofing, social engineering, and the use of reputable platforms for malicious purposes are all part of the evolving landscape of cybercrime. By being aware of these methods and understanding the behaviours of scammers, you can better protect yourself from falling prey to similar scams in the future.

At the time of publication, the specific phishing campaign described in this report is no longer active. However, similar scams remain prevalent and continue to target users.

LY Forensics strongly recommends maintaining vigilance when receiving unsolicited emails or links, particularly those requesting sensitive information such as wallet seed phrases. Always verify the legitimacy of the source, carefully examine URLs, and avoid interacting with any suspicious or unexpected communications.