Investment Scam

From Job Recruitment To Investment Scam

By Nguyen Nguyen & Ranbir Bhutani

12/01/2024

Introduction

Scams have evolved significantly, progressing from basic phishing emails to complex, multi-stage operations that exploit individuals' vulnerabilities. One particularly insidious form of investment fraud often begins as an innocent job recruitment message and escalates into a high-stakes financial scheme, leading to substantial monetary losses. Understanding the lifecycle of such scams is crucial for individuals and organizations to safeguard against them.

Recently, we encountered a scammer who attempted to draw us into a fraudulent job opportunity, which was a precursor to an elaborate investment scam. This paper chronicles the scammer’s tactics step by step, providing a detailed account of the communications exchanged. By dissecting the language and psychological methods employed, we expose how scammers manipulate their targets, gradually entrapping them in a web of deceit.

Our investigation uncovered at least 60 victims of this scam, with estimated losses exceeding $44,289 USD linked to a single crypto address we reviewed. This type of fraud relies on prolonged engagement, capitalizing on victims' growing investment of time and resources, often driven by greed, leading to significant financial consequences.

Through our analysis, we identified six distinct phases in the scammer’s communication strategy. Each phase acts as a calculated step toward their ultimate objective: coercing victims into transferring funds into fraudulent accounts. Figure 1 provides an overview of the six phases outlined in the scammer’s playbook.

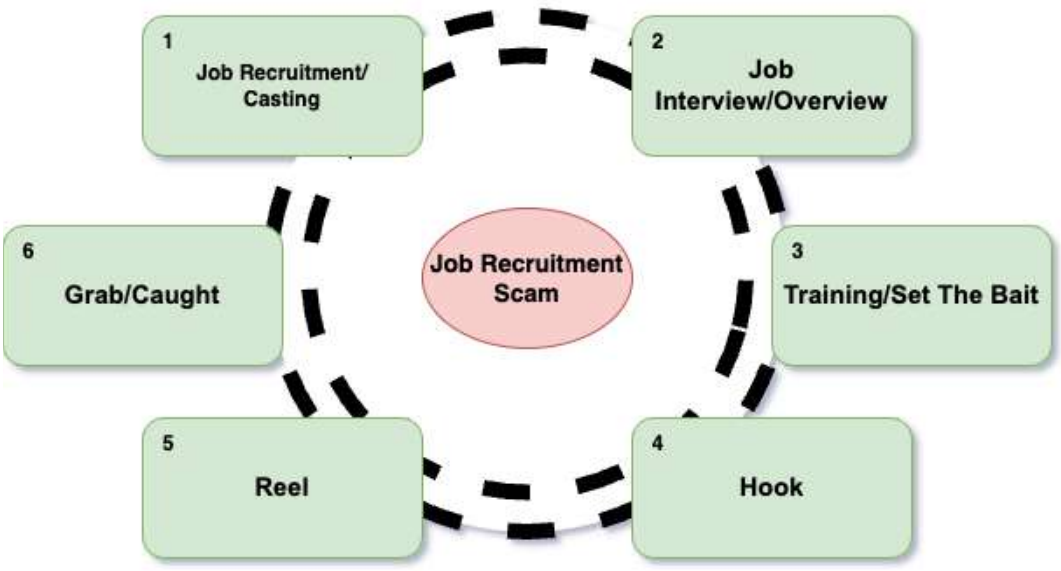

Figure 1: Investment Scam Flow

The Scam Lifecycle

Step 1: Job Recruitment/Casting

The scam typically begins with a job recruitment message, often delivered via email, LinkedIn, or other social media platforms. The victim is approached by a seemingly legitimate recruiter offering an attractive job opportunity. These positions are strategically crafted to appear highly desirable, often featuring remote work, high salaries, and flexible hours—details intended to lower the victim's defenses and increase their interest.

The Scam:

An individual contacts the victim from an unknown phone number (310-303-9304) via SMS, presenting an offer for a remote position. The message requests a simple response of "yes" to receive more details, using casual and non-threatening language to engage the recipient. Below is a screenshot illustrating this recruitment approach, which serves as the initial step in assessing whether the target is viable.

Red Flags to Watch For:

Red Flag #1**: Unexpected Text Messages** - Receiving unsolicited messages from unknown or random numbers is a major red flag. Scammers often use "smishing" (text phishing), leveraging lists of phone numbers to indiscriminately target individuals. The best course of action is to ignore such messages and avoid engaging with the sender.

Red Flag #2: **Unconventional Recruitment Practices** - Legitimate recruiters rarely, if ever, initiate contact via SMS. Professional recruiting practices typically involve formal communication channels such as email or LinkedIn. A text-based approach is highly unprofessional and indicative of a scam.

Red Flag #3: **Unrealistic Job Offers** - Positions promising minimal work (e.g., 1-2 hours per day) with disproportionately high pay ($100-$300 per day) should immediately raise suspicion. These offers are designed to entice and deceive victims by preying on their desire for easy income.

Figure 2: Text Message About The Job

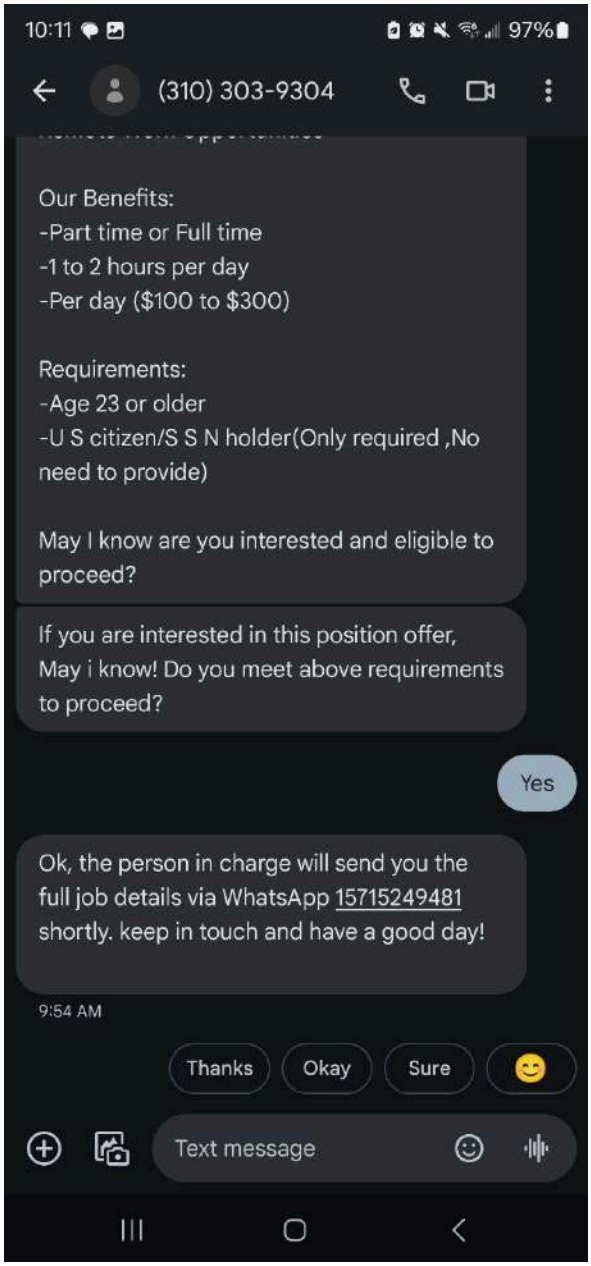

Figure 3: Stage 2 Contact

Step 2: Job Interview/Overview

After identifying a potential target, the next phase involves the scammer reaching out via WhatsApp. This stage is critical for grooming the target and transitioning communication to a more informal platform. The scammer introduces the "job opportunity," explains its purported functions, and directs the target to access a website to proceed further.

Red Flags to Note:

Red Flag #4: Legitimate job - related discussions rarely occur exclusively on WhatsApp. Established companies typically use formal communication channels, such as email or official platforms, rather than casual messaging apps.

The Scam:

After expressing interest in the job, we were contacted on WhatsApp by someone using the number 618-956-0945, identifying themselves as “Emilia.” Emilia described the job as follows:

- Position: Remote role as a "Data Generation User."
- Responsibilities: Boosting an application to increase brand awareness.
- Training Offer: A 30-minute training session with immediate payment ranging from $70 to $120.
- Compensation:
    - $200 for two days of work.
    - $800 for five consecutive days of work.

At first glance, the job seems enticing, offering minimal work for substantial pay. To further establish credibility, the scammer emphasized the immediate availability of training and payment, bypassing any formal hiring procedures.

Red Flags to Note:

Red Flag #5: Offering payment for training without any formal hiring process is highly suspicious. Legitimate employers typically do not pay for training before official **onboarding.**

Red Flag #6: Upfront payments without proper documentation or contracts are a hallmark of scams. Legitimate employers provide clear terms and conditions, often in writing.

The Next Step:

To proceed, we were instructed to register an account on a website provided by Emilia. Below is the URL of the fraudulent website: https://www.totallysoftware[.]tech/index/#/pages/register/register.

Red Flags to Note:

Red Flag #7: The domain "totallysoftware[.]tech" is not associated with any recognized or reputable company. Legitimate businesses generally use established domains with professional branding.

Red Flag #8: The website lacks essential contact information, such as a physical address or phone number, which makes it challenging to verify its authenticity. Legitimate websites always include verifiable details for transparency.

The following section includes a detailed record of our conversations with the scammer, further illustrating their manipulative tactics and strategies.

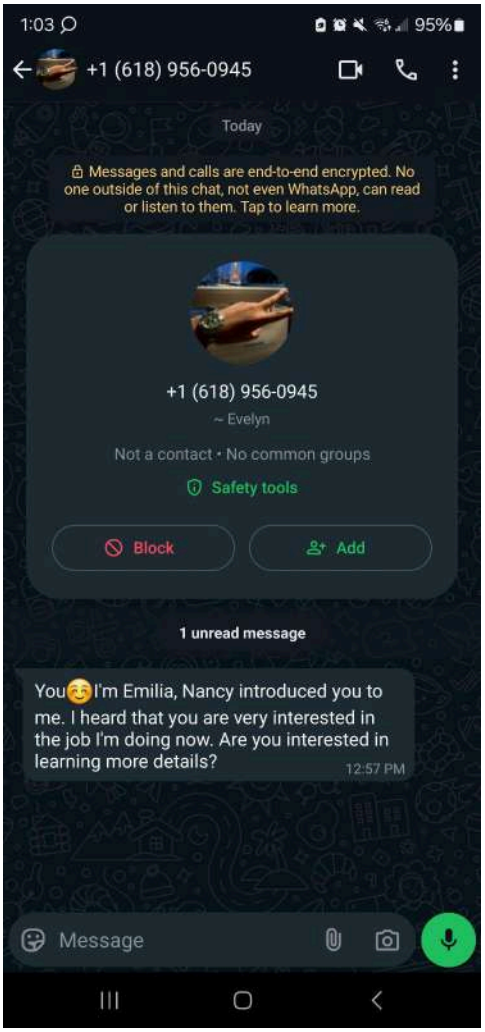

Figure 4: Initial message from scammer

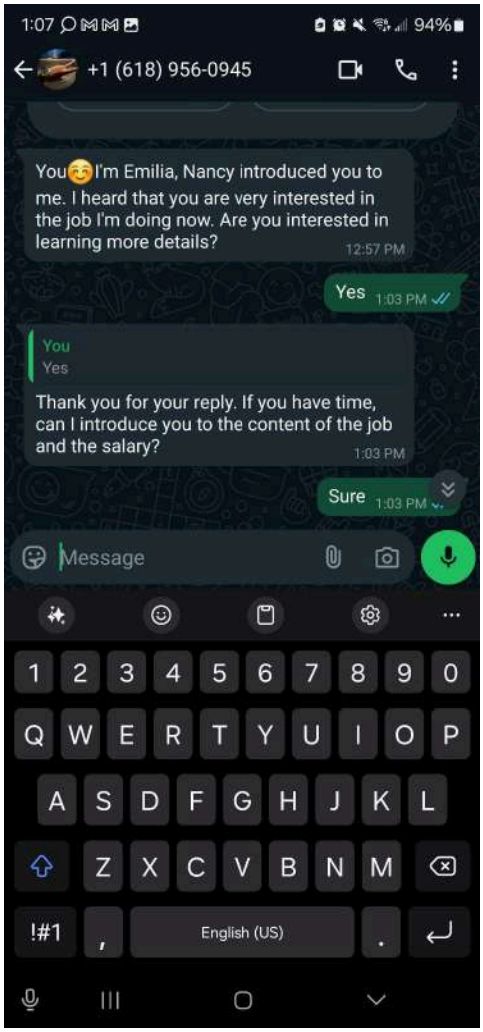

Figure 5: Emilia introduce the job

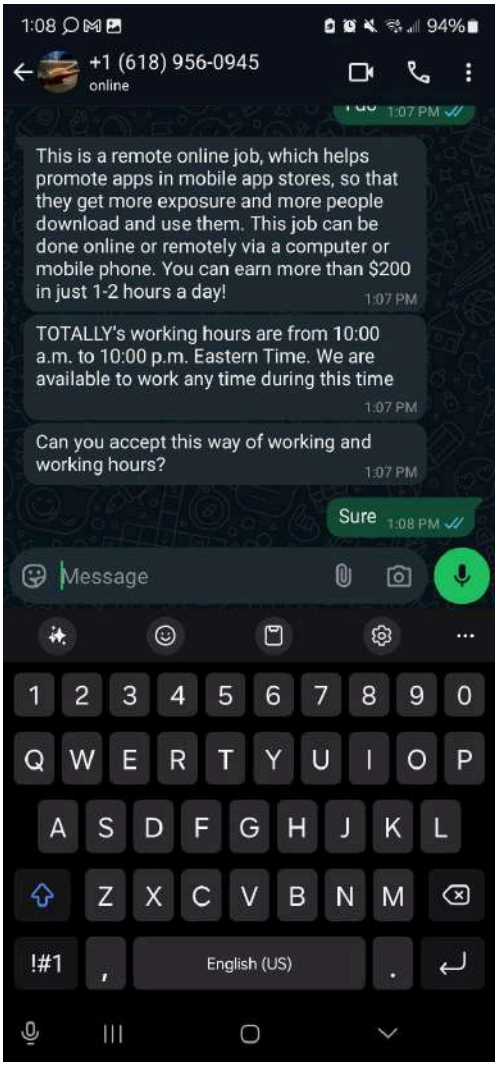

Figure 6: Emilia explains the job description

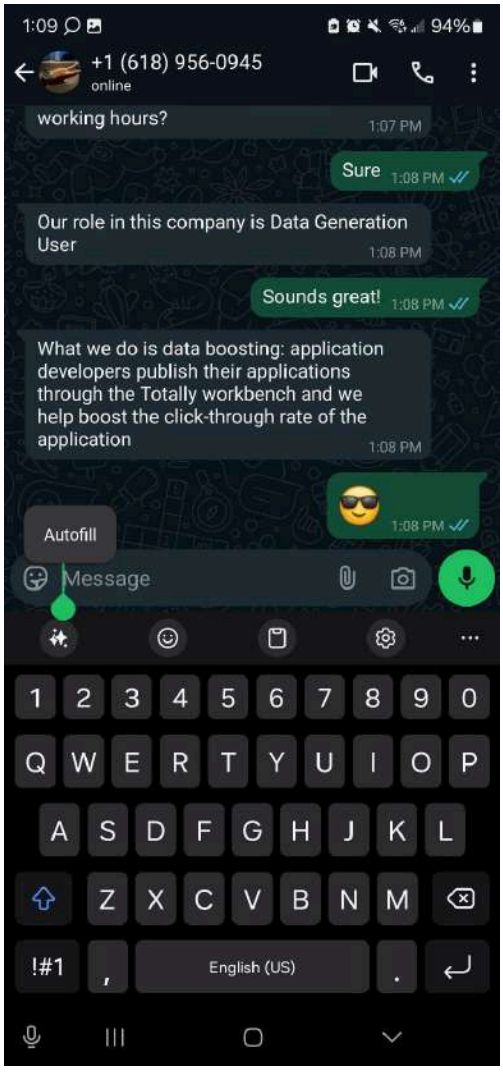

Figure 7: Emilia explains the role of “data generation user”

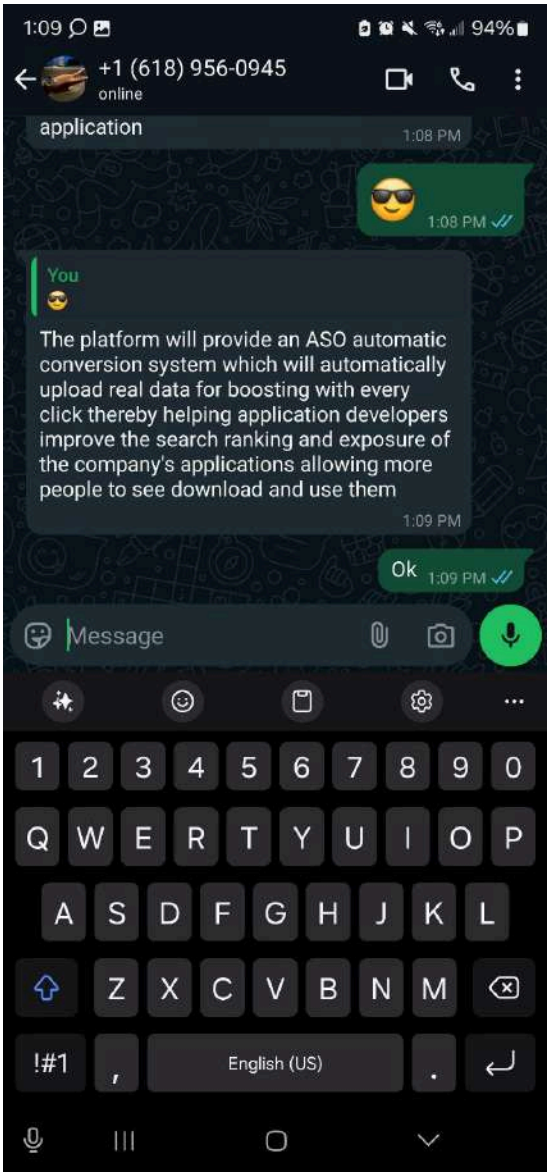

Figure 8: Explains how the platform work

Figure 9: Emilia build up the connection with the user

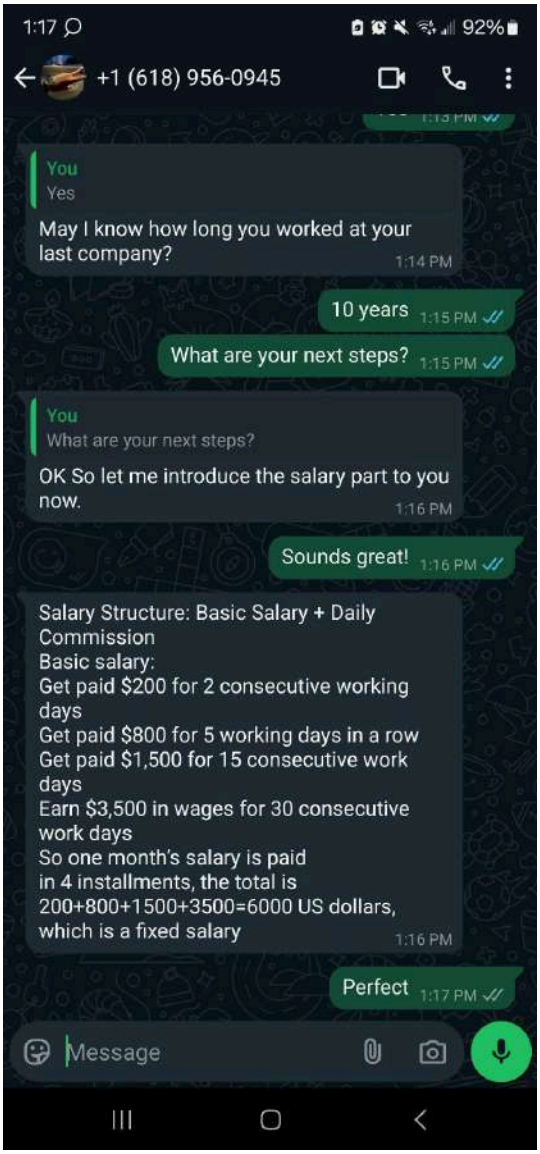

Figure 10: Emilia explains the salary structure

Figure 11: Emilia eases the user into the next stage

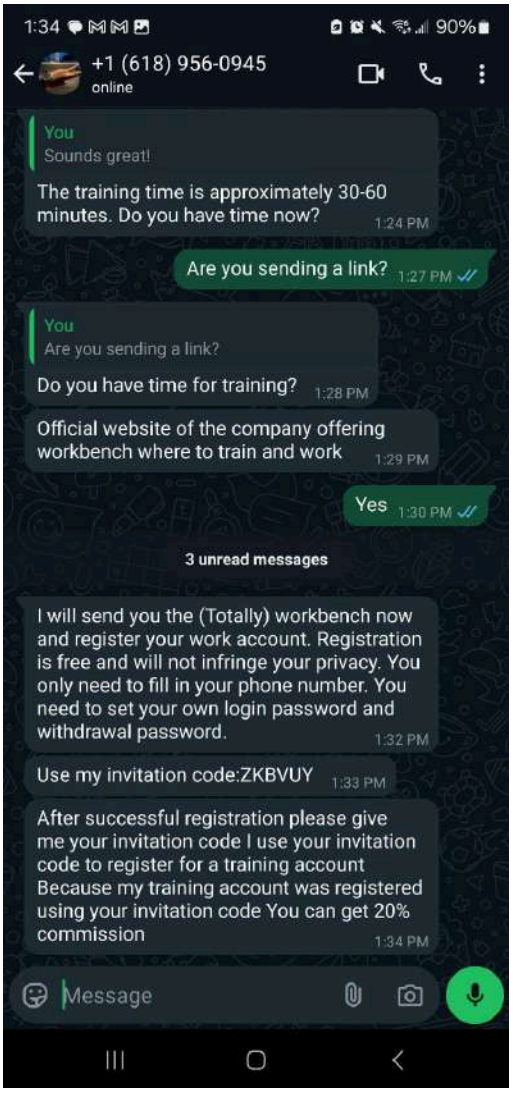

Figure 12: Emilia explains the training and the portal

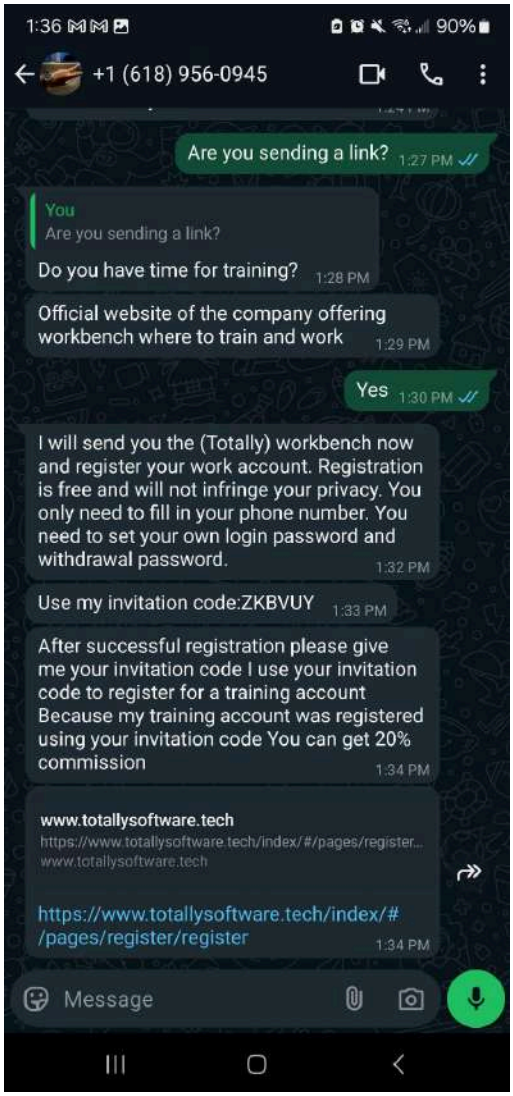

Figure 13: Invitation code and webpage

Red Flags to Note:

Red Flag #9: The scammer's WhatsApp profile lists the name as 'Evelyn,' but they present themself to potential victims as 'Emilia.'

Red Flag #10: The scammer and the website does not provide a clear and secure payment method.

Assessment of TotallySoftware[.]tech:

The domain TotallySoftware[.]tech was recently registered on 2024-08-12 with NameSilo LLC and is hosted on Cloudflare. On the surface, the website appears legitimate, presenting itself as a platform offering "app store boost services" designed to support startups and mid-sized applications. This aligns with the job description provided by Emilia.

Key Observations:

1. Account Registration: Access to the site requires account creation using a code provided by Emilia, a tactic designed to build trust and limit access to vetted targets.

2. Promotional Offers: After logging in, users are immediately presented with a pop-up promoting a "Limited Event." This offer promises:

- A 5% reward for deposits between $500 and $1,499.
- A 15% reward for deposits exceeding $10,000.

3. Communication Channels: The website prominently features customer support via **WhatsApp** and **Telegram**, platforms often favored by scammers due to their secure, anonymous nature.

Red Flags to Note:

Red Flag #11: Promises of high returns, such as a percentage reward for deposits, are classic tactics used in investment scams. These promises are designed to entice victims into making significant deposits under the guise of lucrative rewards.

Red Flag #12: The use of Telegram and WhatsApp as primary communication channels is another strong indicator of fraudulent activity. While these platforms offer privacy and encryption, they are frequently exploited by scammers to conceal their identities and evade detection.

This analysis underscores the deceptive nature of TotallySoftware[.]tech and highlights the various red flags that potential victims should be vigilant about. The combination of unrealistic

rewards, insecure payment methods, and unprofessional communication channels strongly suggests a sophisticated scam operation

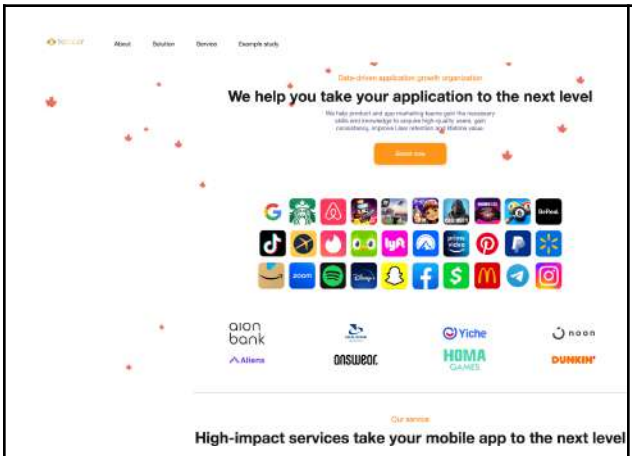

Figure 14: Screenshot of the Webpage

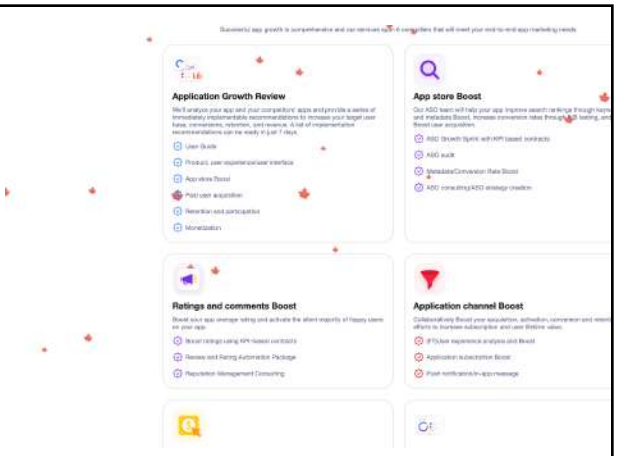

Figure 15: Screenshot of the Webpage

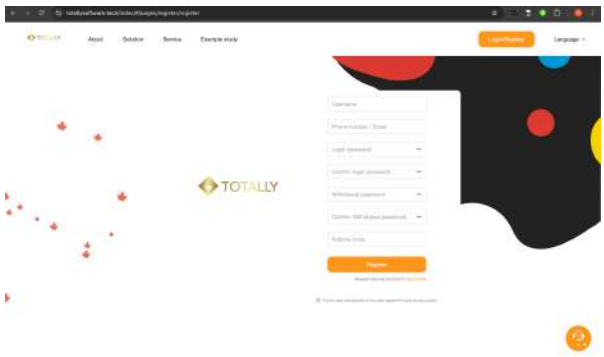

Figure 16: Registration webpage

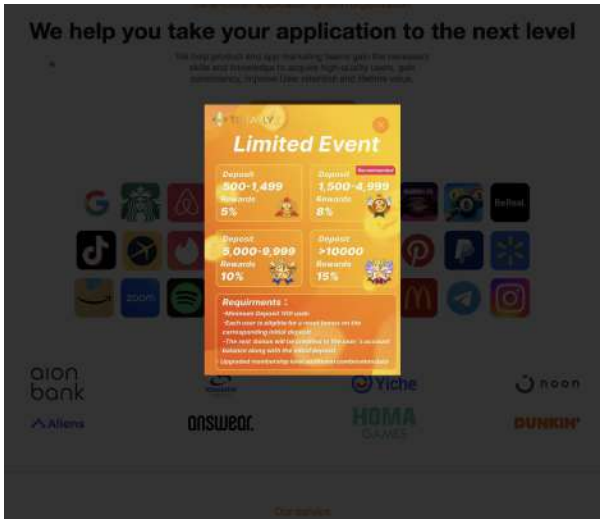

Figure 17: Lure message to create greed

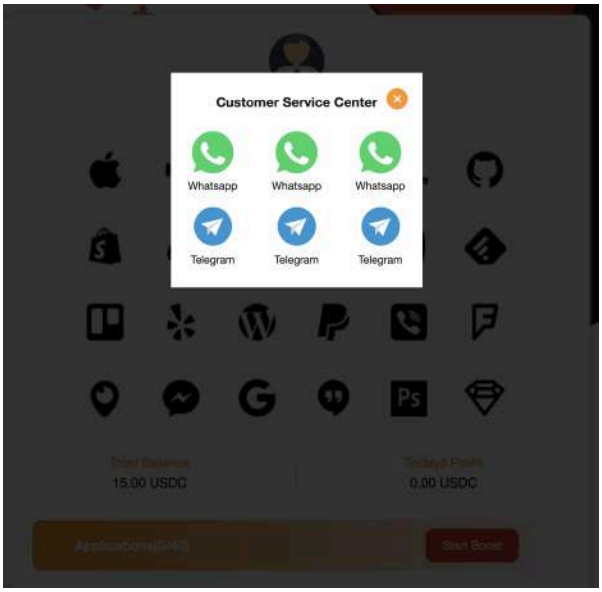

Figure 18: Customer Support page

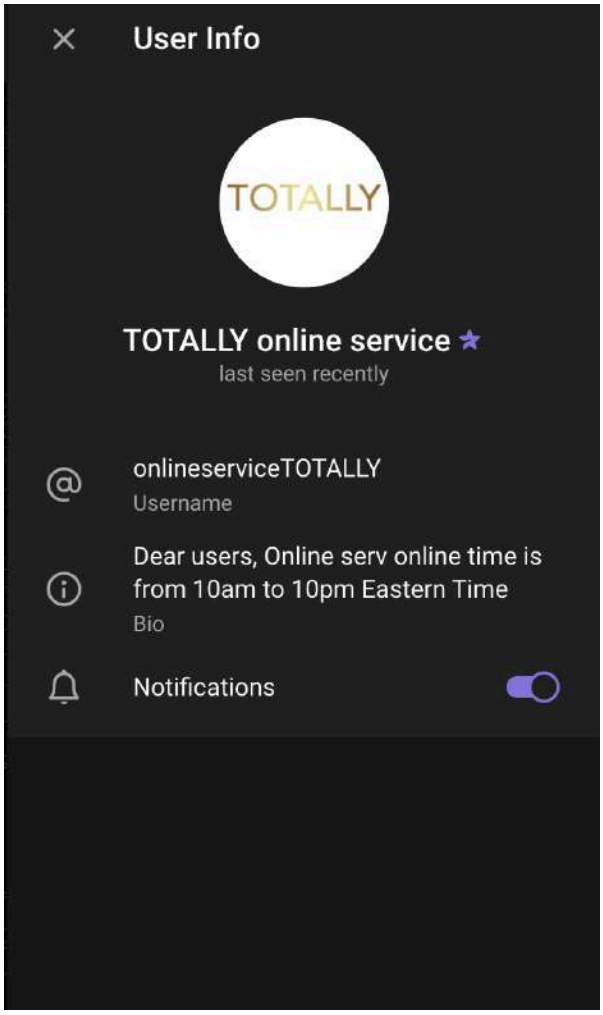

Figure 19: Customer Support Profile On Telegram

Red Flag #13: The "limited event" offering high returns within a short time frame in exchange for a deposit is a classic pressure tactic. This approach is designed to create a sense of urgency, compelling users to act quickly without fully considering the risks.

Technical Observations:

In the user profile interface, the platform displays both the total balance and total profit of the account. Within the wallet settings, users can input their preferred cryptocurrency wallet address for Bitcoin, or Ethereum. This wallet address is "bound" to the user's account for withdrawal purposes.

Upon further analysis of the network traffic, the following concerning behaviors were identified:

1. **API Data Handling**: User data is retrieved through an API, which returns a JSON document containing sensitive information. This document includes:
    - User details.
    - The linked cryptocurrency wallet address.
    - Total balance information.
    - Passwords stored in plain text.
2. **Language Indicators**: Certain status messages returned by the API were written in **Chinese**, potentially suggesting the geographical origin or affiliations of the cybercriminals operating the platform.

Red Flag #14: Storing passwords in plain text and transmitting them between the browser and web server is a glaring security vulnerability. This practice exposes sensitive user information to interception and exploitation, representing a significant breach of standard cybersecurity protocols.

Conclusion:

The combination of pressuring users with unrealistic return promises, insecure data handling practices, and potential foreign origins further underscores the fraudulent nature of this operation. These tactics, particularly the storage of sensitive information in plain text, highlight the high risks associated with engaging with this platform.

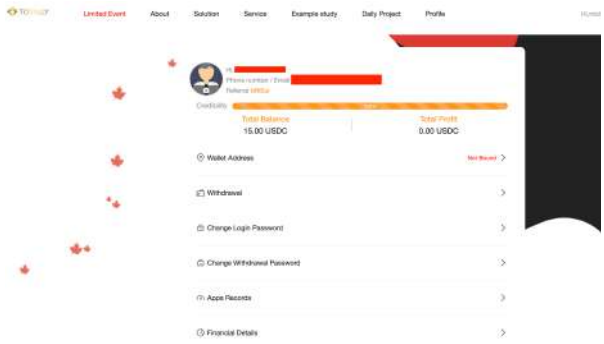

Figure 20: Initial Profile

Figure 21: Profile After Training

Figure 22: Profile with password in cleartext

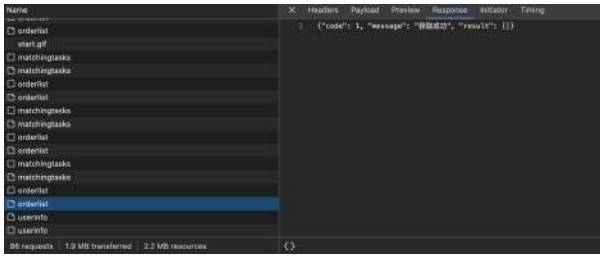

Figure 23: Status message respond from server is in Chinese

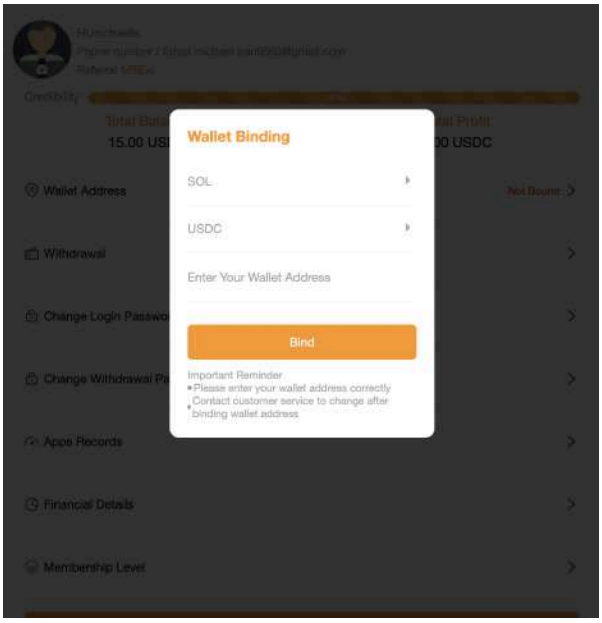

Figure 24: Wallet Binding Option

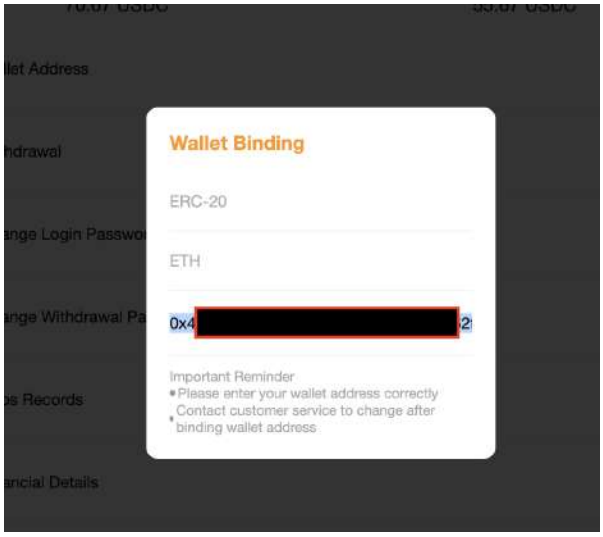

Figure 25: Binding wallet with Ethereum wallet

Step 3: Training / Set The Bait

Once the victim's account is registered and the scammer gauges sufficient interest, they introduce a separate "training account." This account serves as bait, displaying a balance supposedly deposited by the scammer to make the operation appear legitimate. The scammer then walks the victim through the platform, demonstrating how "easy" it is to earn money, further luring them into the scheme.

The Scam:

The scammer provides the victim with login credentials for the training account, claiming to have "deposited" $1,500 into it. They also mention that the platform credited an additional:

- $120 as a registration bonus.
- $15 as a special incentive, bringing the total balance to $1,635.

This setup is meticulously designed to impress the victim and establish trust by showcasing seemingly effortless earnings.

However, the scammer deliberately omits a critical detail: this "deposit" is actually the amount they expect the victim to contribute later under the guise of advancing their participation in the scheme. This omission is a calculated move to deceive the victim into believing the platform is both credible and profitable.

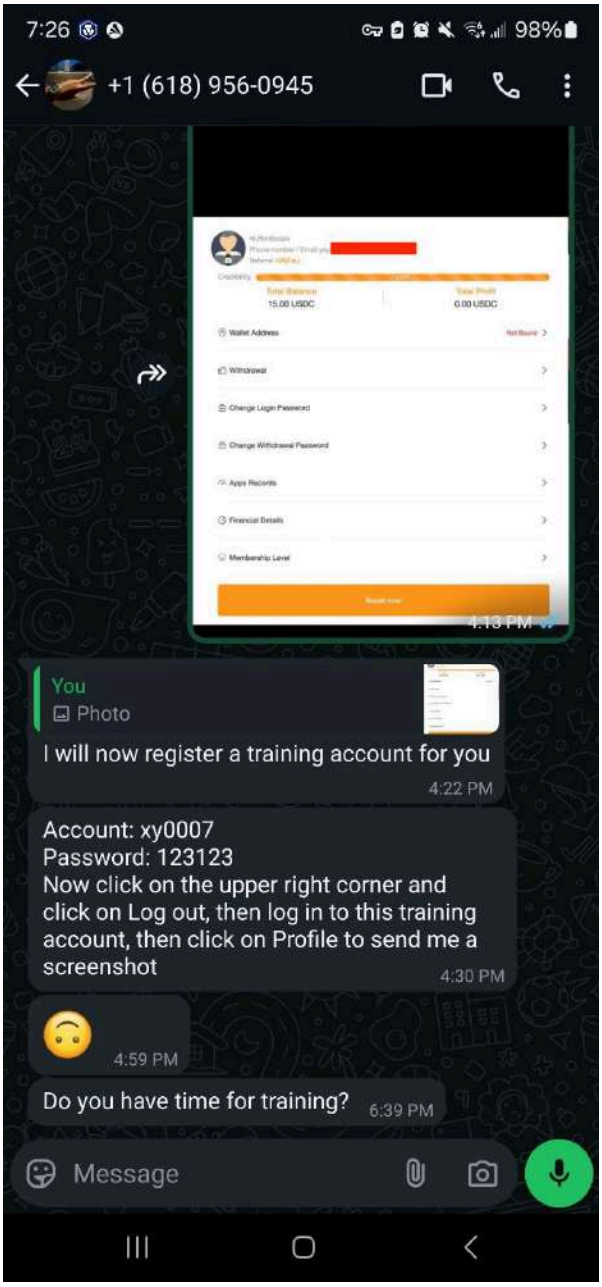

Figure 26: Train account

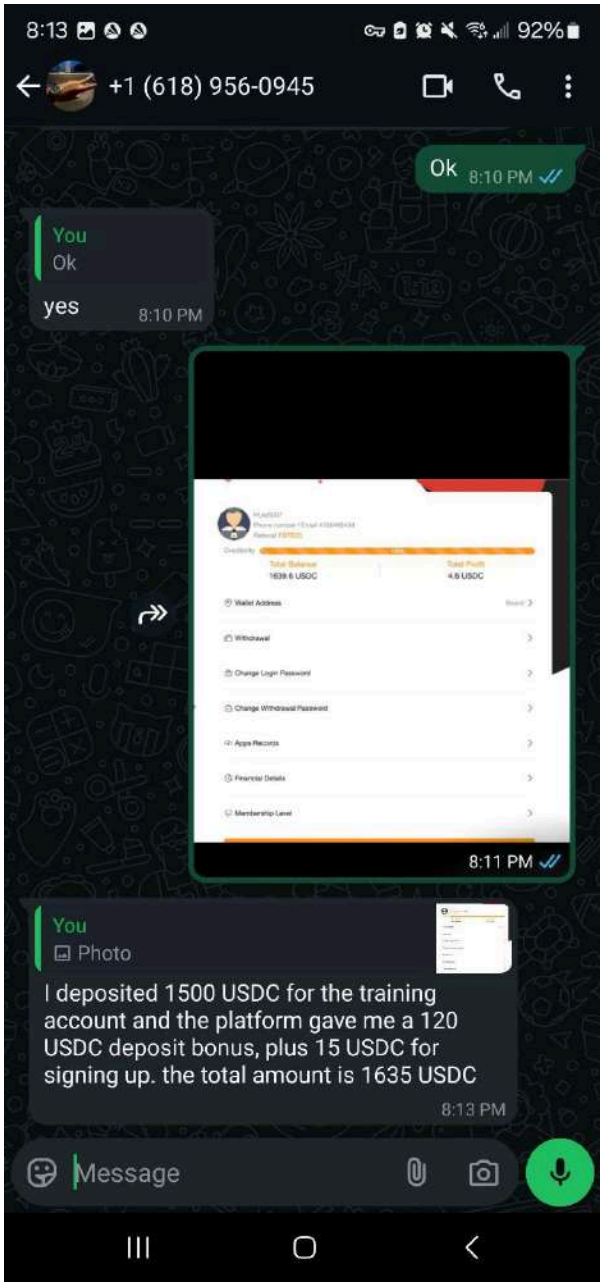

Figure 27: Emilia explains the fund deposit by her

Note: Emilia never mentioned that money must be deposited for the job.

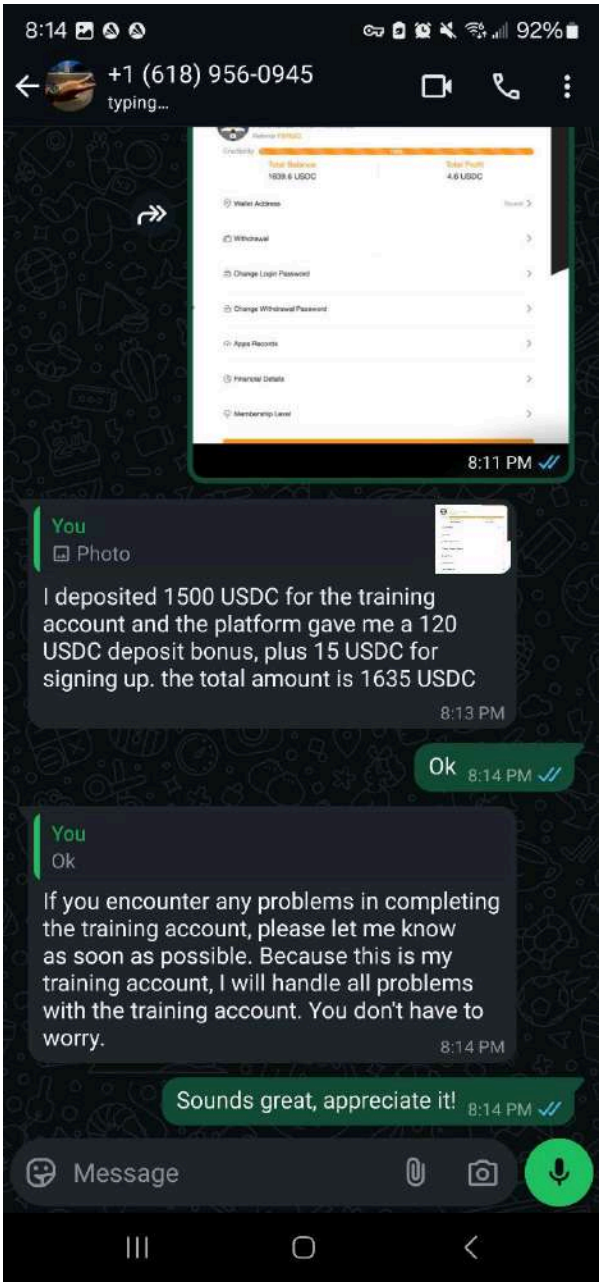

Figure 28: Emilia shows encouragement

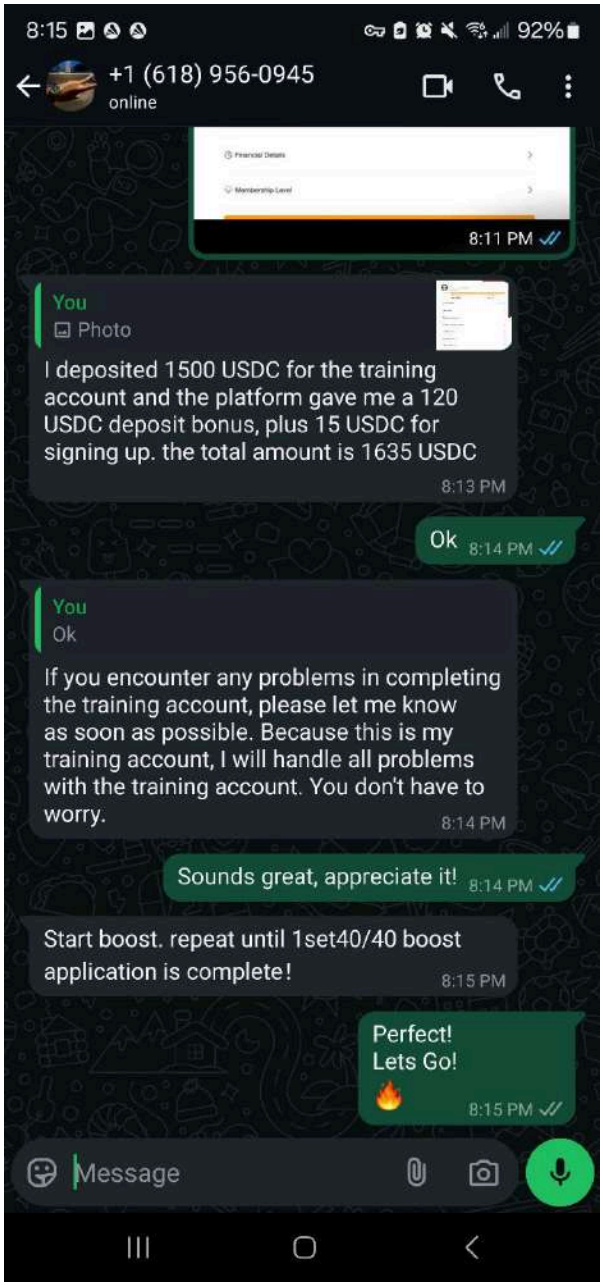

Figure 29: Emilia tell to start the job

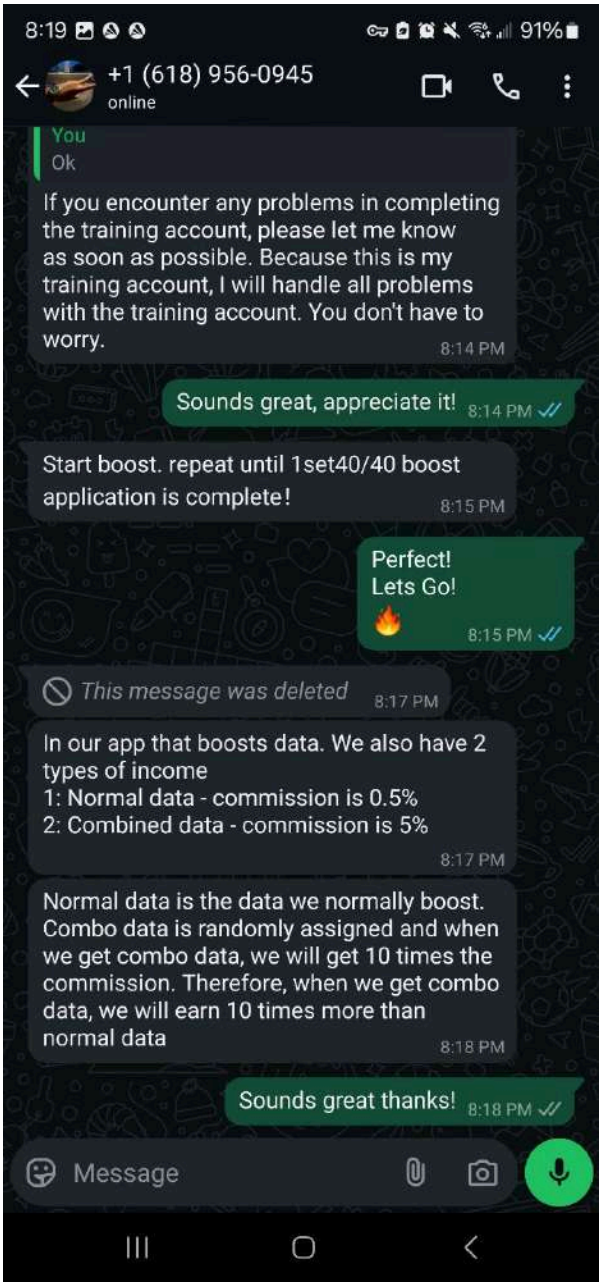

Figure 30: Emilia hinting the scam hook

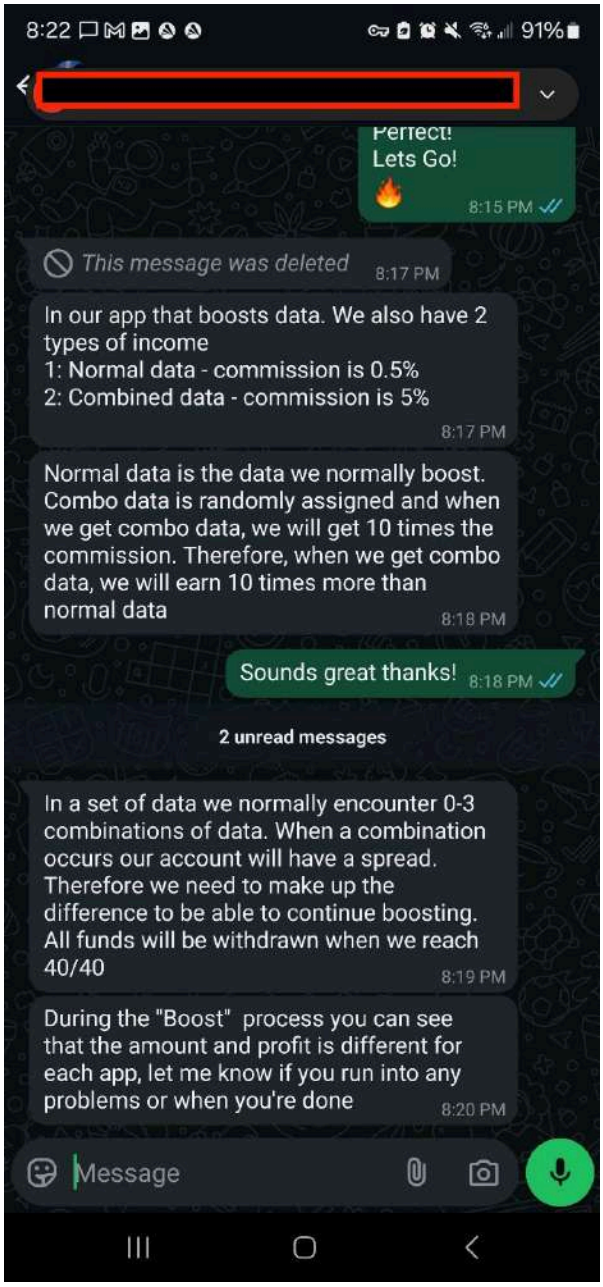

Figure 31: Emilia ease in how we make easy money but just hit the 'boost' button

The task assigned to the victim involves clicking a "boost" button, which supposedly generates income. In this scenario, each click is advertised as yielding a 0.05% return, translating to $2 to $6 per click.

Red Flag #15: The notion of being paid simply for pressing a button is a major red flag. Legitimate job opportunities require genuine effort, specific skills, or productive tasks that provide tangible value to the company or organization. This oversimplified task contradicts the expectations of legitimate work and is often a hallmark of scams.

Technical Analysis:

Upon inspecting the network traffic, no meaningful data was found being sent to the server to track or validate the user's actions. Instead, the server automatically updates the "profit" total displayed on the website, regardless of any real activity. This indicates that the earnings are entirely **fabricated**, designed to deceive the user into believing the platform is legitimate and profitable.

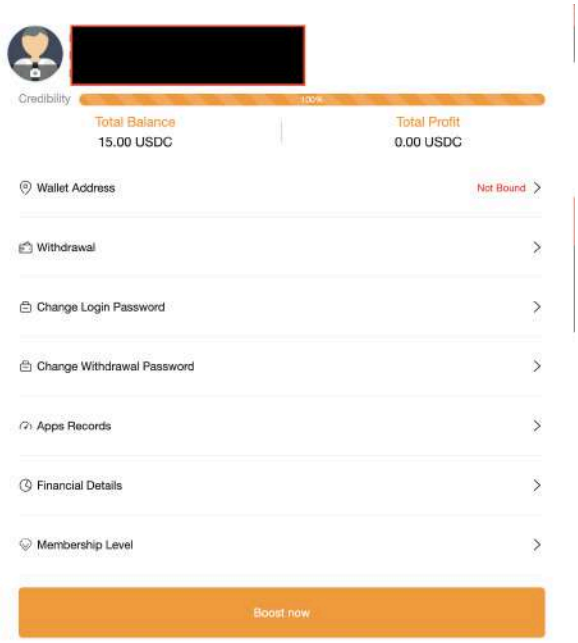

Figure 32: Screenshot of the “Boost” feature

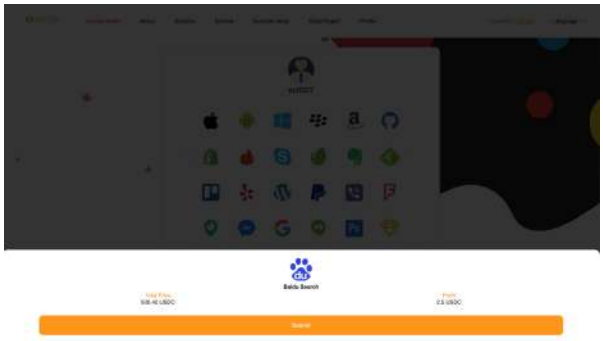

Figure 33: Screenshot shows the “boost” task. Users only need to press “Submit”

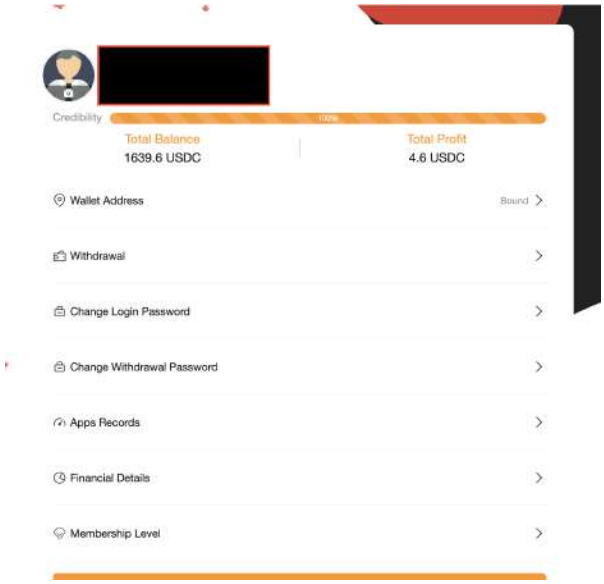

Figure 34: The profit get update once the users ‘submit’ the ‘boost’

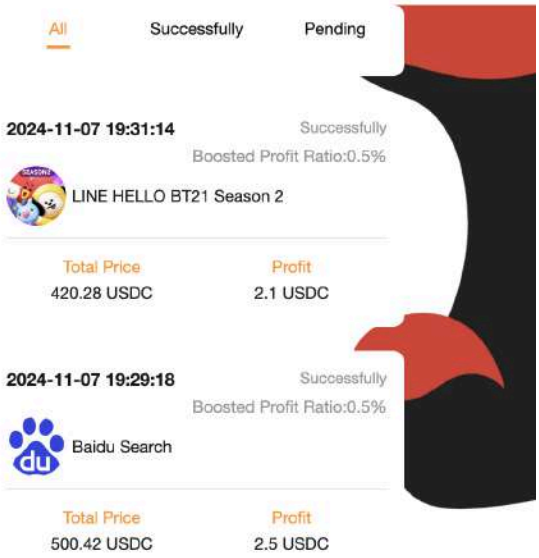

Figure 35: Apps Records page shows the activities (all fake)

Throughout the process, the scammer maintains frequent contact, checking in regularly to ensure the victim is completing the assigned tasks (e.g., reaching 40/40 clicks). They appear **attentive and supportive**, offering step-by-step guidance to address any issues. For example, when we encountered a problem at 30/40 clicks, the scammer promptly responded, explained the situation, and even "deposited" additional funds to help us complete the task.

This tactic is a deliberate attempt to build trust, showcasing the scammer's apparent dedication and willingness to assist. By reinforcing the illusion of a legitimate job and highlighting the victim's supposed "earnings," the scammer manipulates the victim into continuing their engagement. This psychological strategy increases the likelihood that the victim will overlook red flags and remain invested in the scheme.

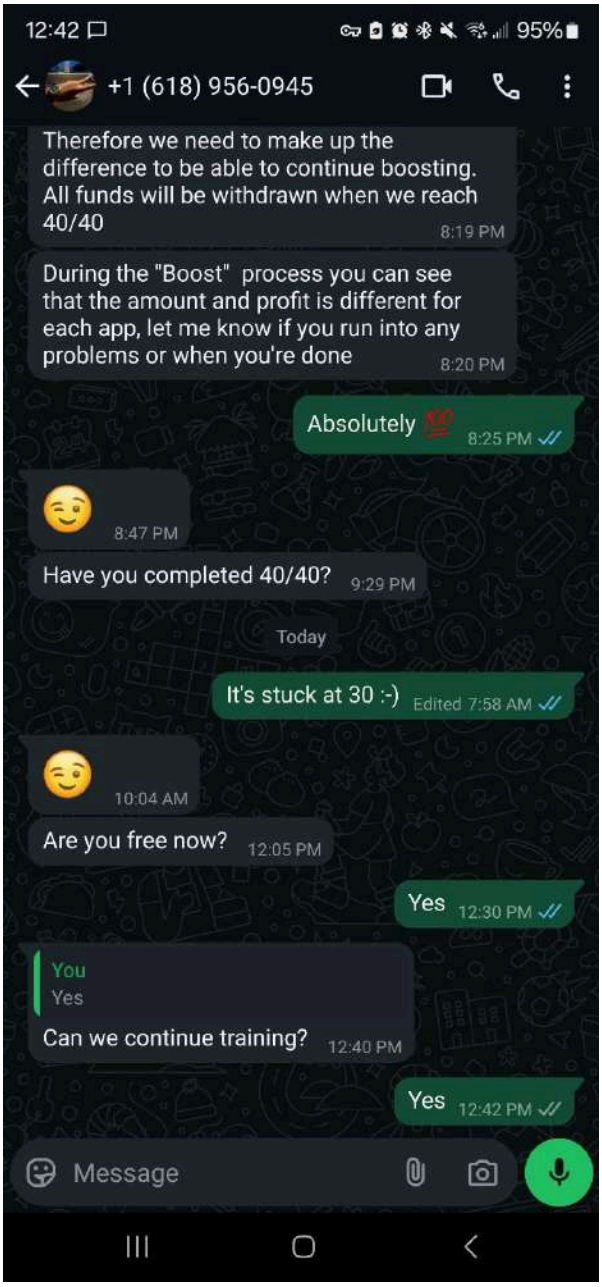

Figure 36: Emilia check up on the user

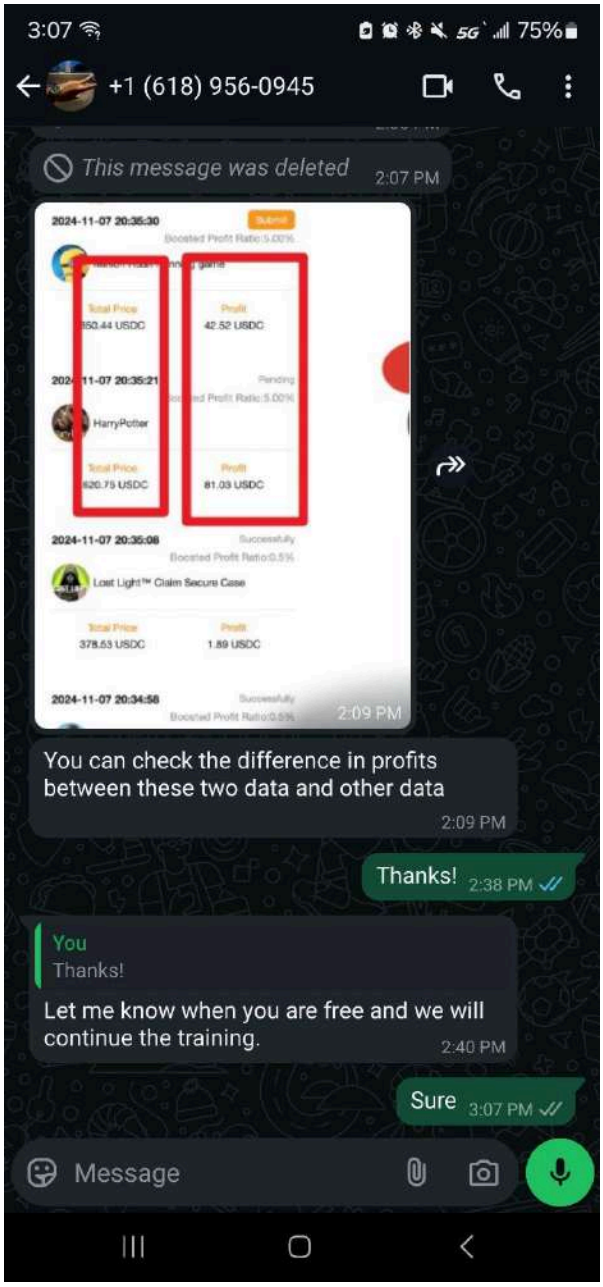

Figure 37: Emilia shows how much the user profit from the job so far

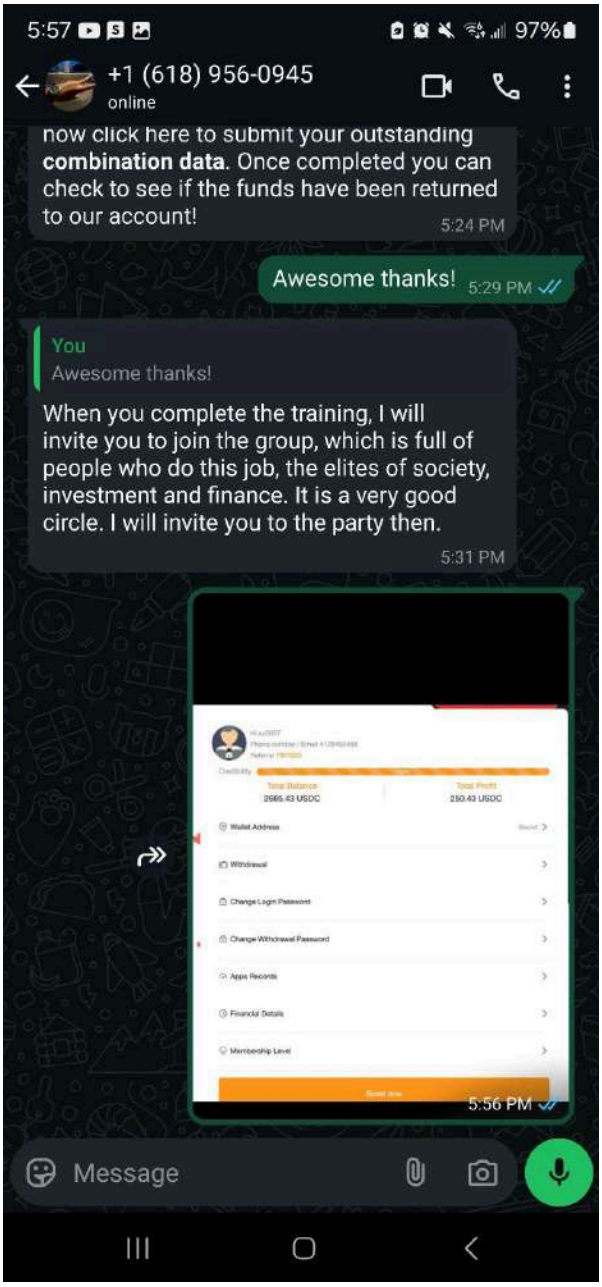

Figure 38: Emilia motivating the users to finish the training

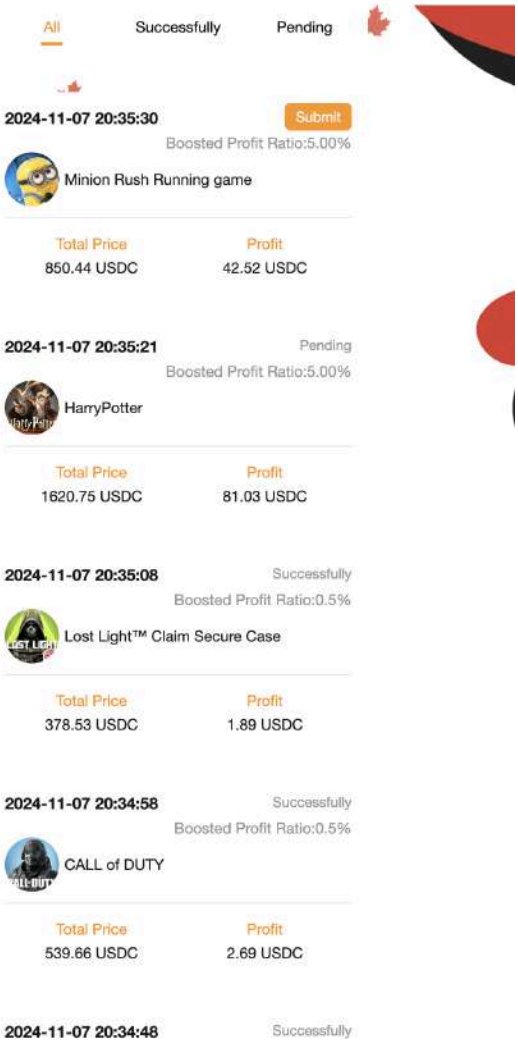

Figure 39: Fake activities shows the profits the user has gain

End of Training Session

At the conclusion of the training session, the account displayed a supposed profit of $250.

Step 4: The hook

After showcasing the victim's "earnings," the scammer sets the trap by convincing the victim that the money is real and theirs to keep. Following the training, the profit is transferred back to the victim's original account, and the scammer guides them step-by-step through the withdrawal process.

The Scam:

Upon completing our training, we returned to the real account, which now reflected a credit of $65—the "earnings" from the training session. Before initiating the withdrawal, the scammer explained two ways to make money through the platform:

1. **Salary-Based Earnings**: Fixed payouts for completing tasks.

2. **Personal Fund Investments**: Using personal funds to generate higher returns. As the scammer phrased it, "use money to make money."

This is the core of the scam—implanting the idea that significant profits can be made with minimal effort. The scammer demonstrated a deposit of $1,650, claiming that within 10 minutes of "work," a profit of $250 could easily be achieved. **By this point, the original concept of a simple online job had completely shifted into an investment scheme**.

Interestingly, the scammer did not apply aggressive pressure to deposit funds. Instead, they passively guided us through the process, giving no overt signs of deception. To build further trust, they walked us through the withdrawal process.

The Withdrawal Process:

The withdrawal involved cryptocurrency transactions, and the scammer inquired whether we had accounts with CashApp, PayPal, or MetaMask. They guided us in linking our public address through the platform’s "bind" option. After completing this step, we successfully withdrew $69 from the system.

Red Flags to Note:

Red Flag #16: The suggestion to use personal funds to generate returns is a significant warning sign, indicating a shift toward a financial investment scam.

Red Flag #17: Payments made exclusively through cryptocurrency without documentation (e.g., pay stubs or contracts) are a major red flag. Legitimate jobs provide clear paperwork and official payment records.

Red Flag #18: Advance payments, like the $69 withdrawal, are often indicative of an advance payment scam. These payouts are designed to build trust and reinforce the illusion of legitimacy, ensuring victims are more likely to make larger deposits in the future.

This tactic is calculated to foster confidence in the victim, making the operation seem credible and lucrative. By willingly allowing the withdrawal of $69, the scammer effectively plants the idea that the system works. However, this small payout pales in comparison to the significant sums they expect to extract from the victim in the later stages of the scheme.

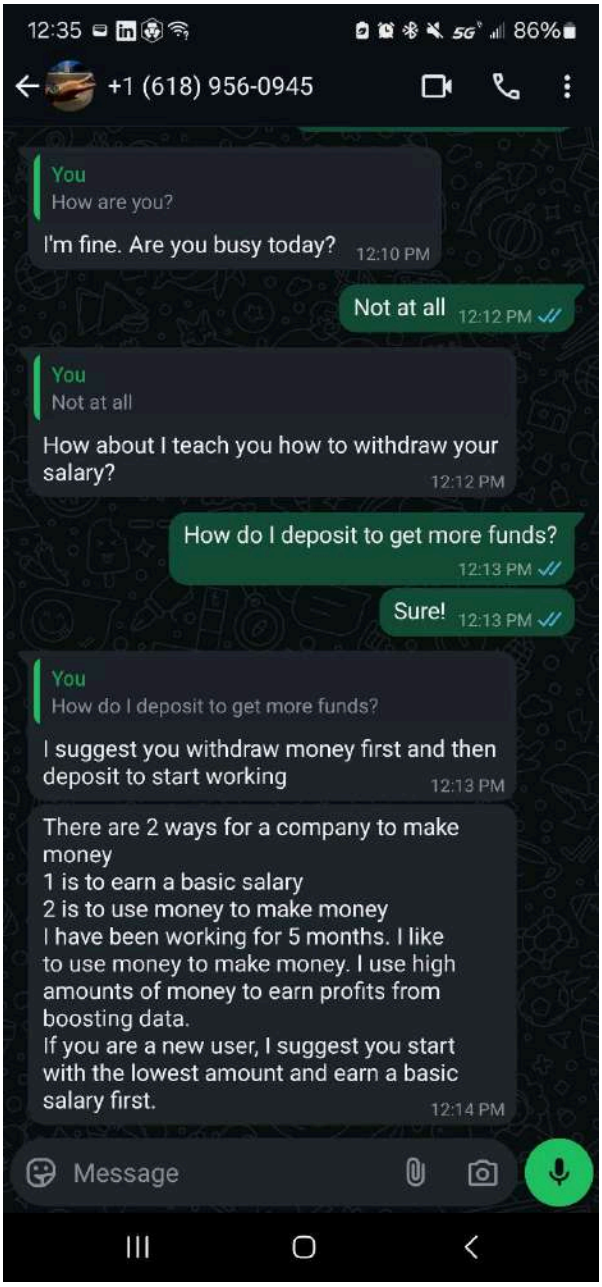

Figure 40: Emilia builds trust by mentioning that the user has already made money and needs to withdraw it.

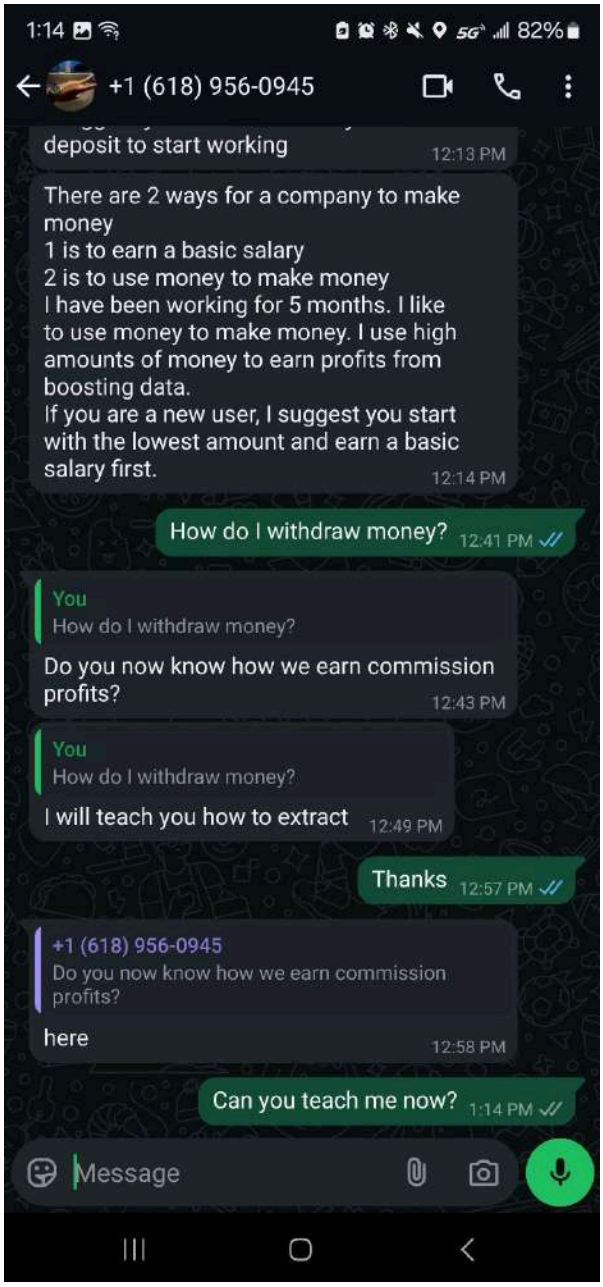

Figure 41: Emilia hinting the investment scam, “use money to make money”

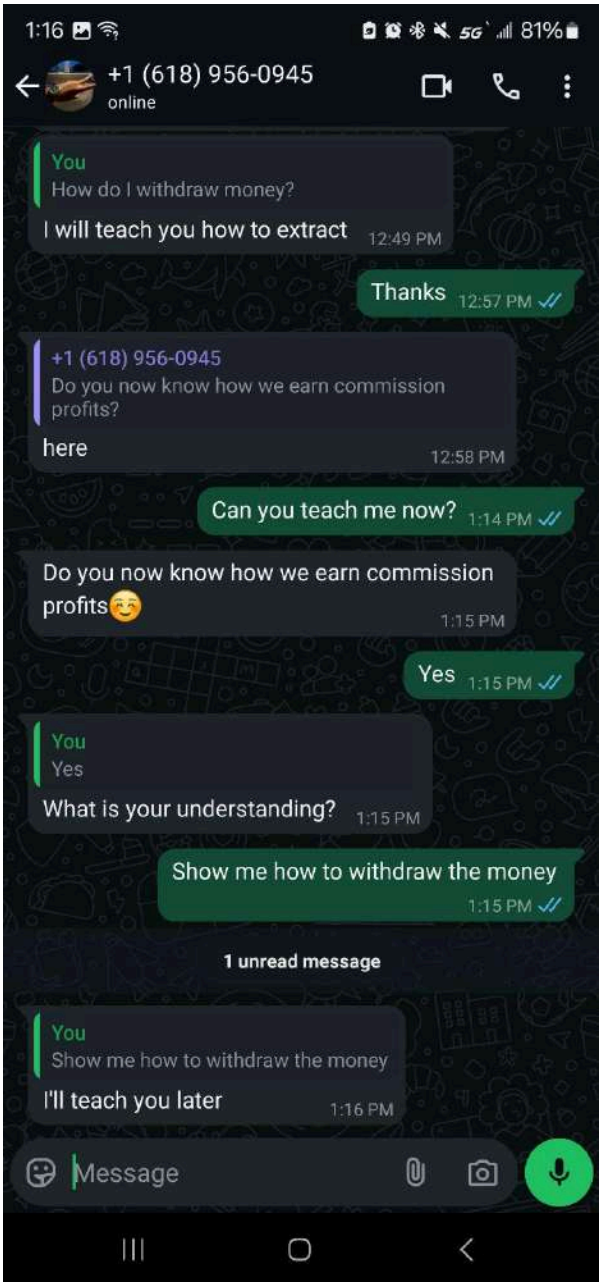

Figure 42: Emilia begins grooming the users by asking how they can earn a commission

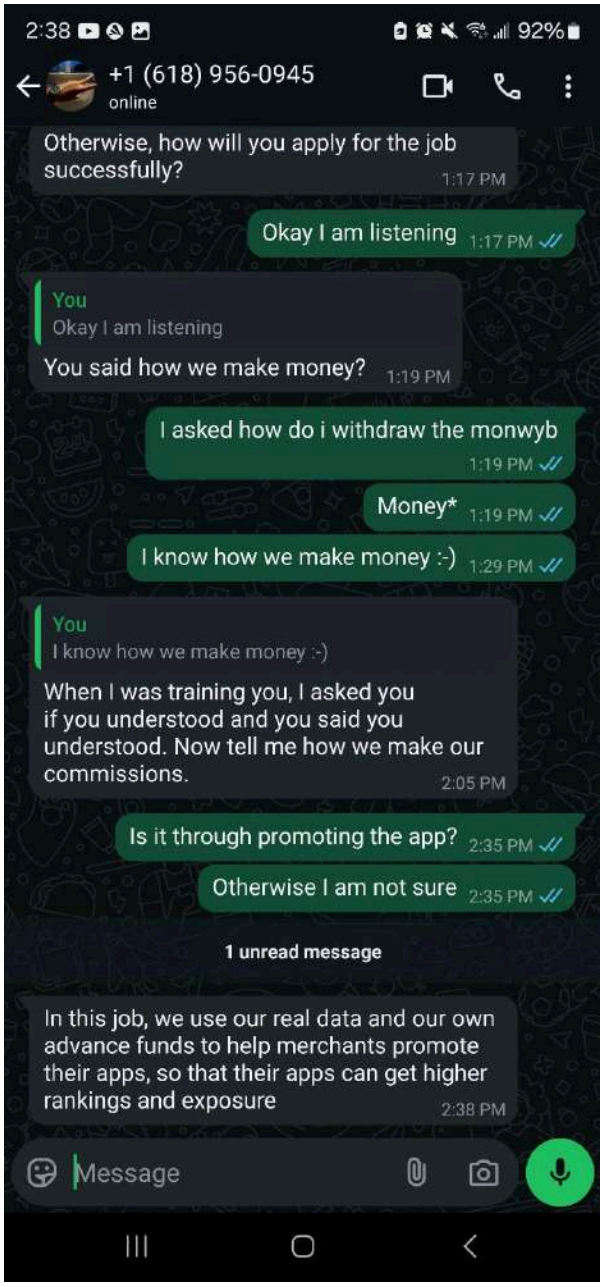

Figure 43: Emilia mentions we use “our own advance funds” to help merchants promote their apps.

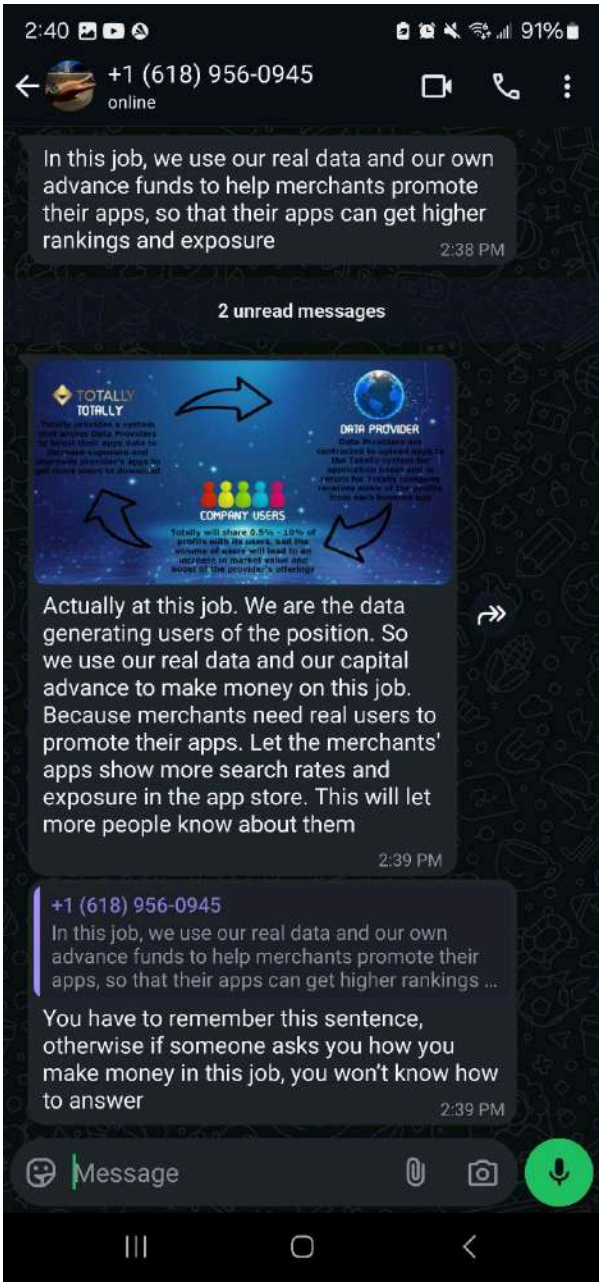

Figure 44: Emilia reiterates that they use their capital in advance to make money—a detail that was not explained earlier.

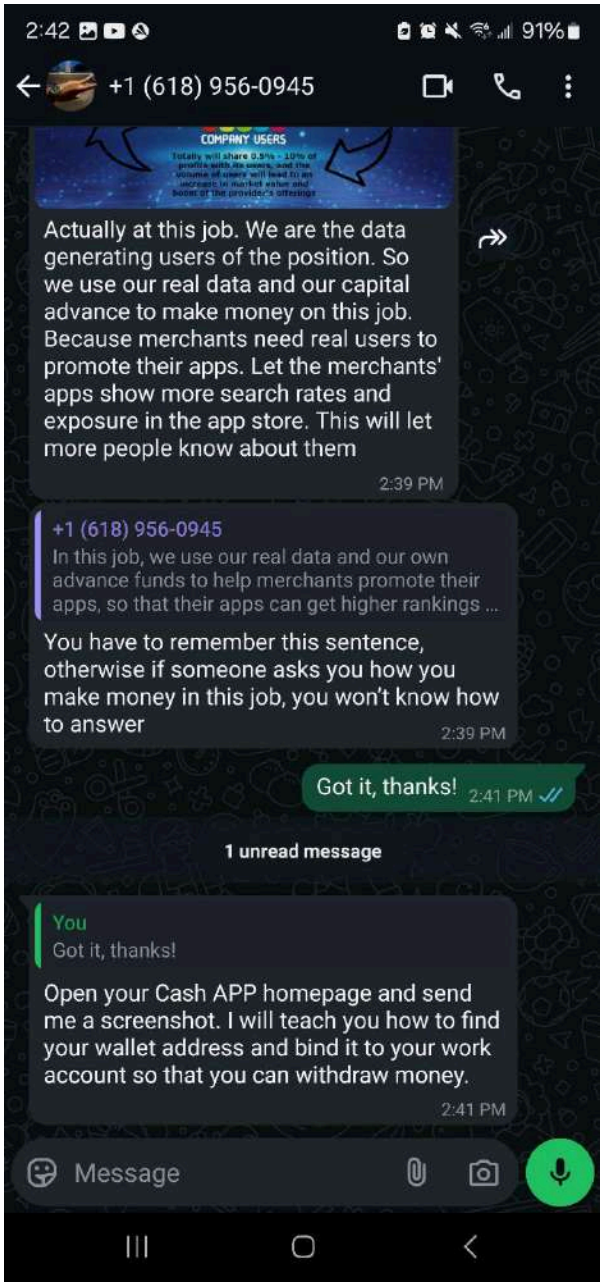

Figure 45: Emilia start explaining the withdraw methods with CashApp

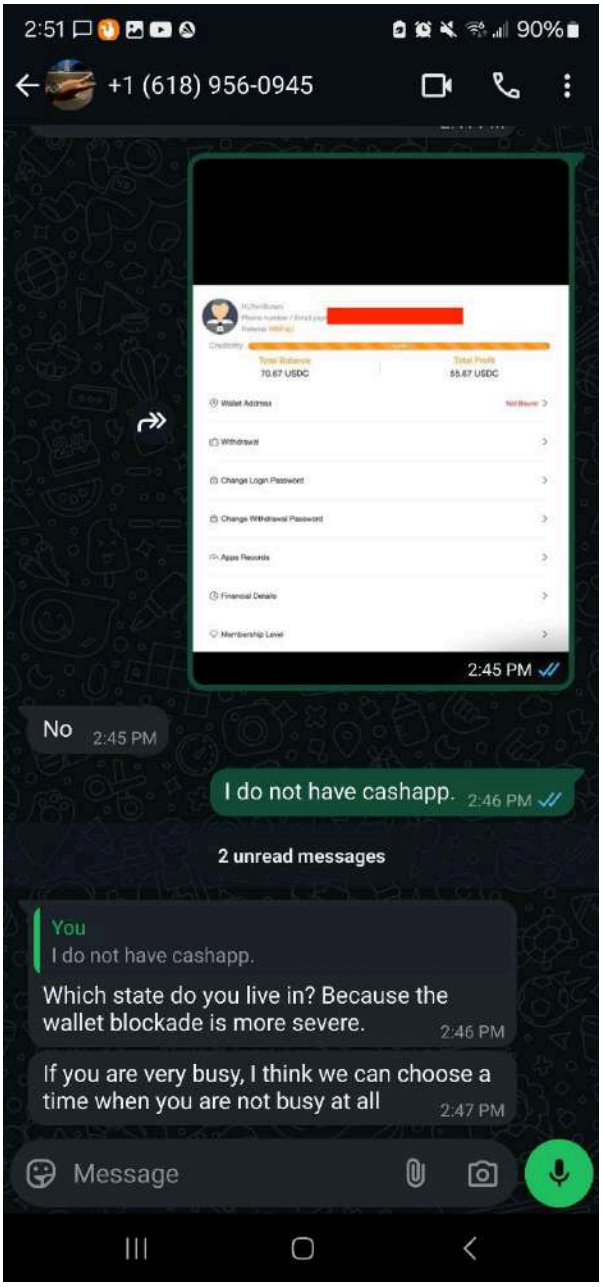

Figure 46: We asked for alternative option

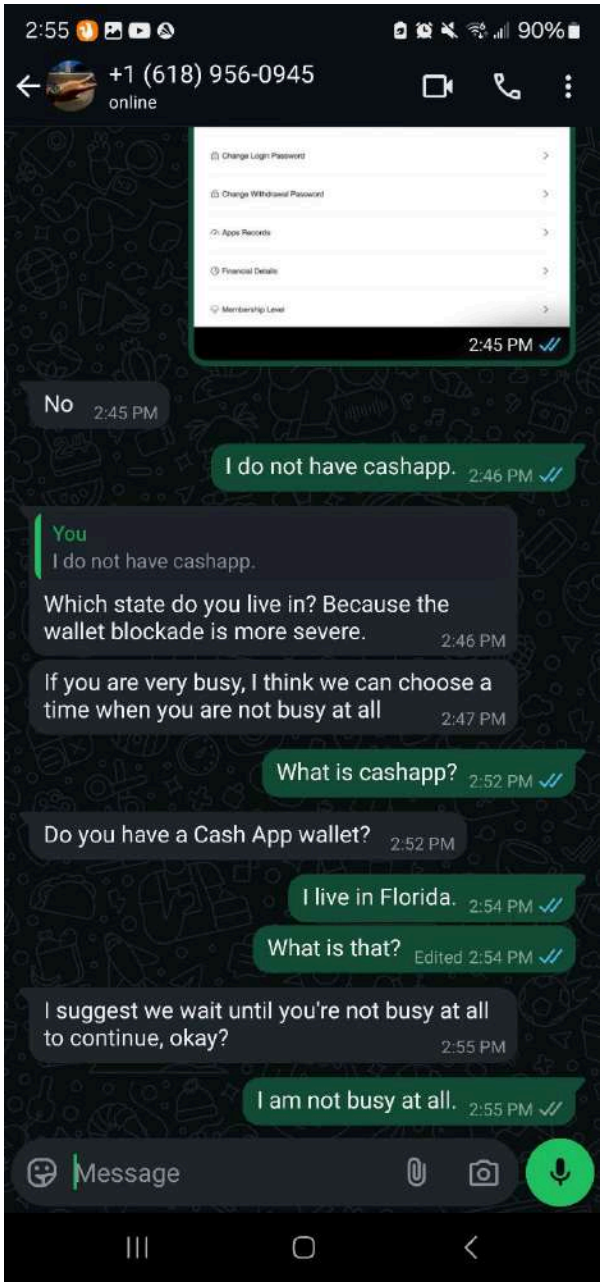

Figure 47: Emilia asks for Cashapp Wallet. Notice Emilia's tone is different today.

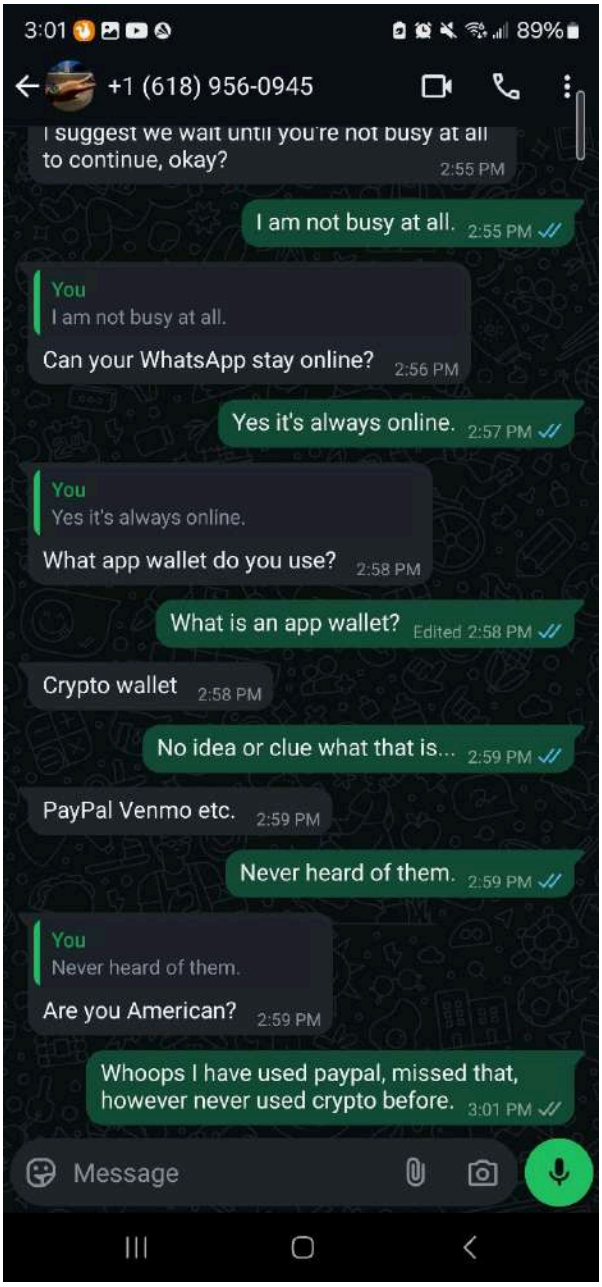

Figure 48: We try to gather more option to see their capability

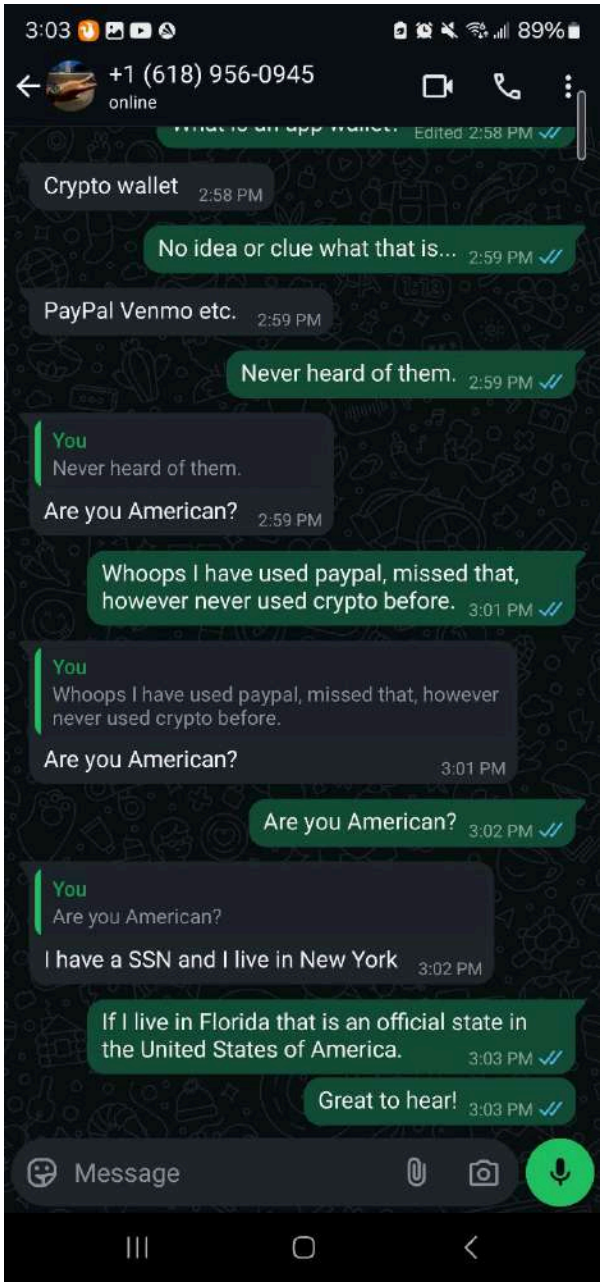

Figure 49: Emilia seems frustrated

Figure 50: Emilia asked us to download Metamask

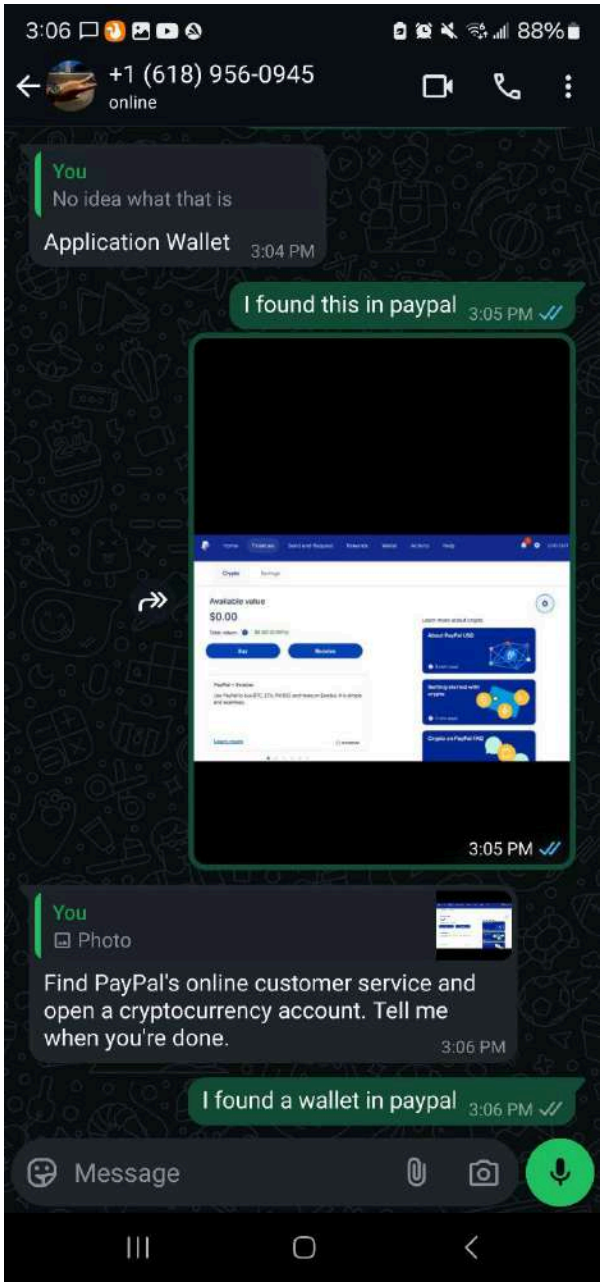

Figure 51: Emilia instruct us to get customer service to open a wallet on Paypal

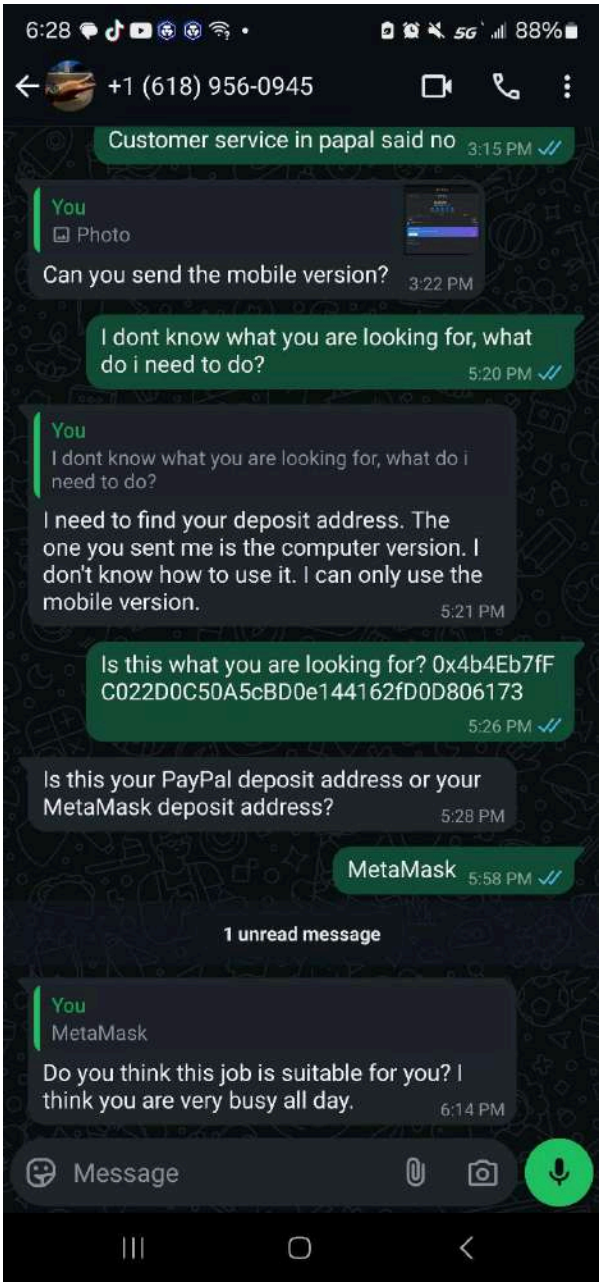

Figure 52: Notice the aggressiveness of this Emilia

Figure 53: “If you want this job, I suggest you to take the time to study seriously”

Figure 54: Notice the tone changed once we stop communicating with “Emilia”

Figure 55: This Emilia is softer and willing to guide us

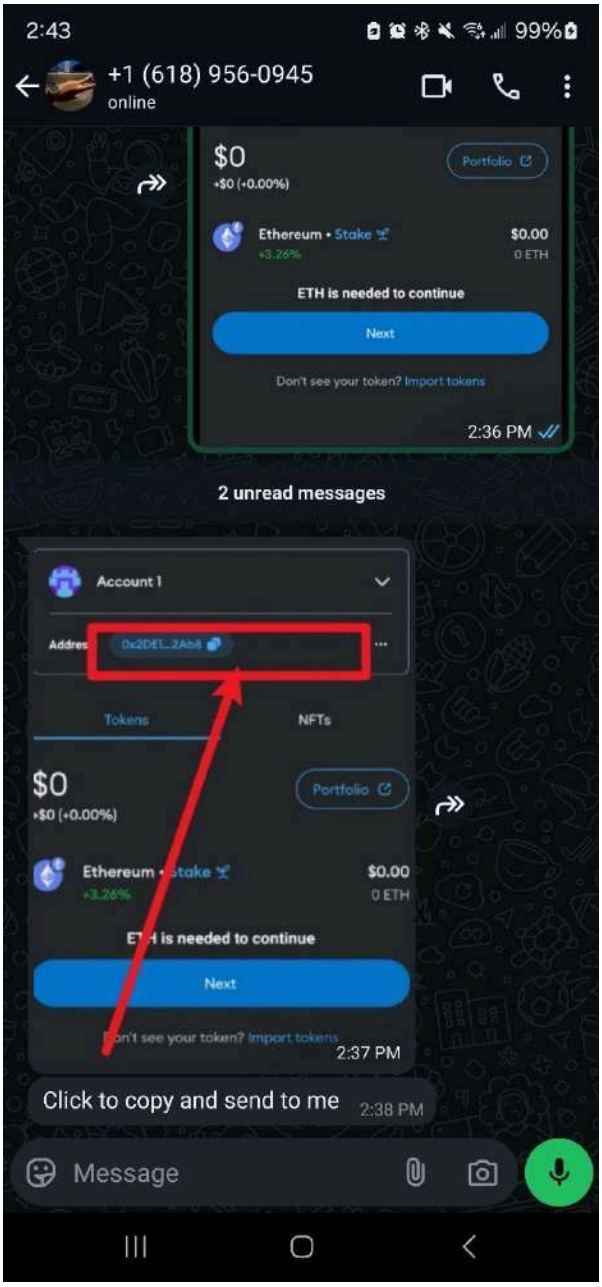

Figure 55: Emilia shows the how to copy the Metamask address

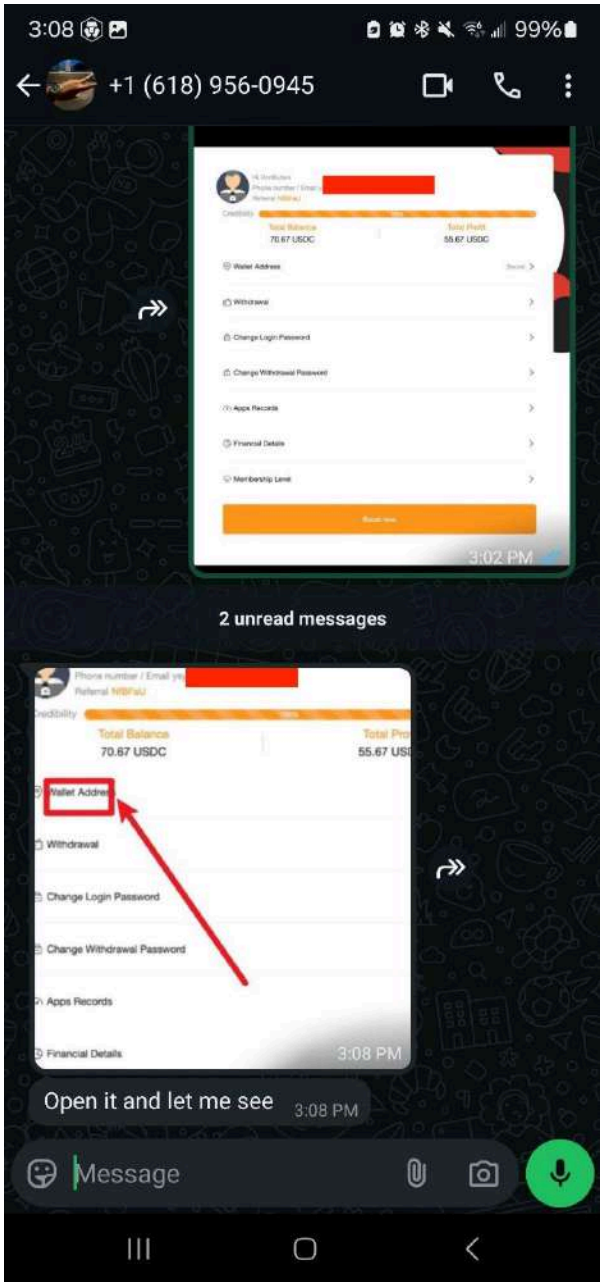

Figure 56: Emilia shows where to put the address

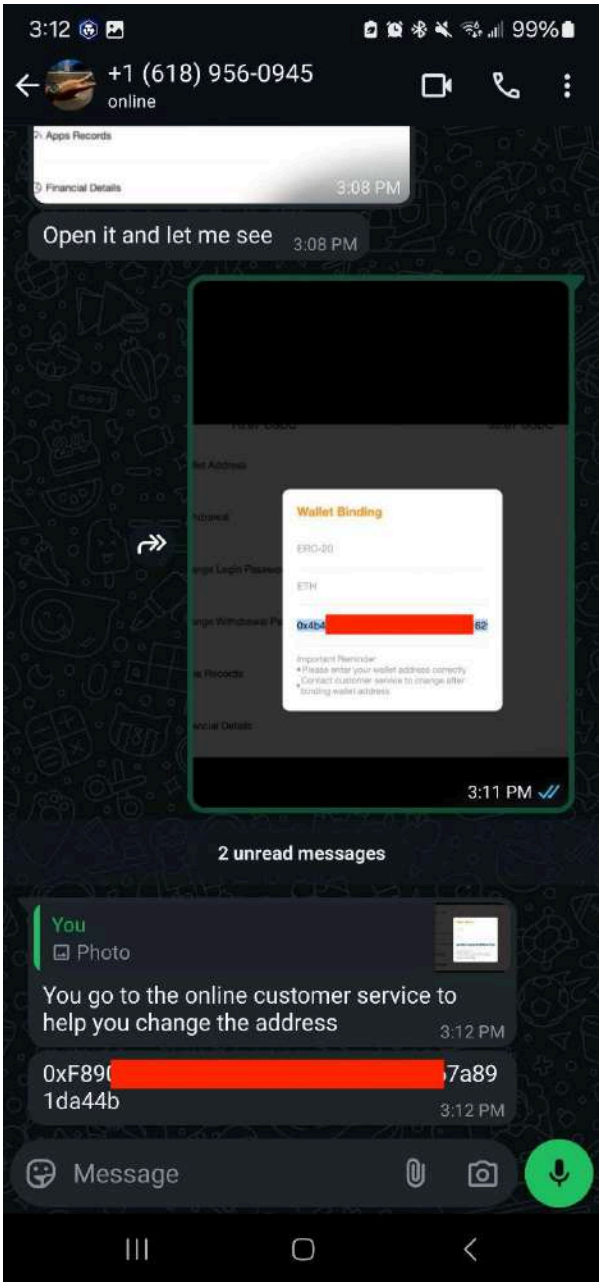

Figure 57: Since we put a wrong address, we couldn't change it. Emilia asked us to contact customer service

Figure 58: Emilia mentions that once the withdrawal is complete, we can join the working group.

Red Flag #19: Any business operating in the United States that does not request basic information such as your Social Security Number (SSN), full name, or address is likely not legitimate. Legitimate employers are required to collect this information for tax and employment compliance.

Step 5: Reel

The next phase of the scam is to persuade the victim to deposit money and start "working." Having built trust through earlier interactions, the scammer now expects the victim to take the bait and make a financial deposit.

However, the platform itself does not offer a direct way to deposit money. Instead, the scammer provides a cryptocurrency address (either Ethereum or Bitcoin) and instructs the victim to transfer funds to this address. To further cement the illusion of legitimacy, the scammer invites the victim to join a "working group" purportedly filled with other workers.

The Scam:

After we engaged with the scammer, they provided access to the working group, which turned out to be a WhatsApp group controlled by multiple individuals. The group showcased messages and screenshots of supposed earnings from other participants to convince us of the job's authenticity.

When we stopped responding, the scammer sent repeated follow-ups, asking if we were ready to start "working" and highlighting fabricated success stories from other "workers" in the group.

Red Flags to Note:

Red Flag #20: High-pressure tactics to start a job immediately—especially without a formal interview or contact with a human resources department—are strong indicators of a scam. Legitimate companies follow standard hiring procedures, including clear communication about job expectations, onboarding processes, and payment terms.

At this point, having gathered enough information to identify the scam, we chose to discontinue communication with the scammer.

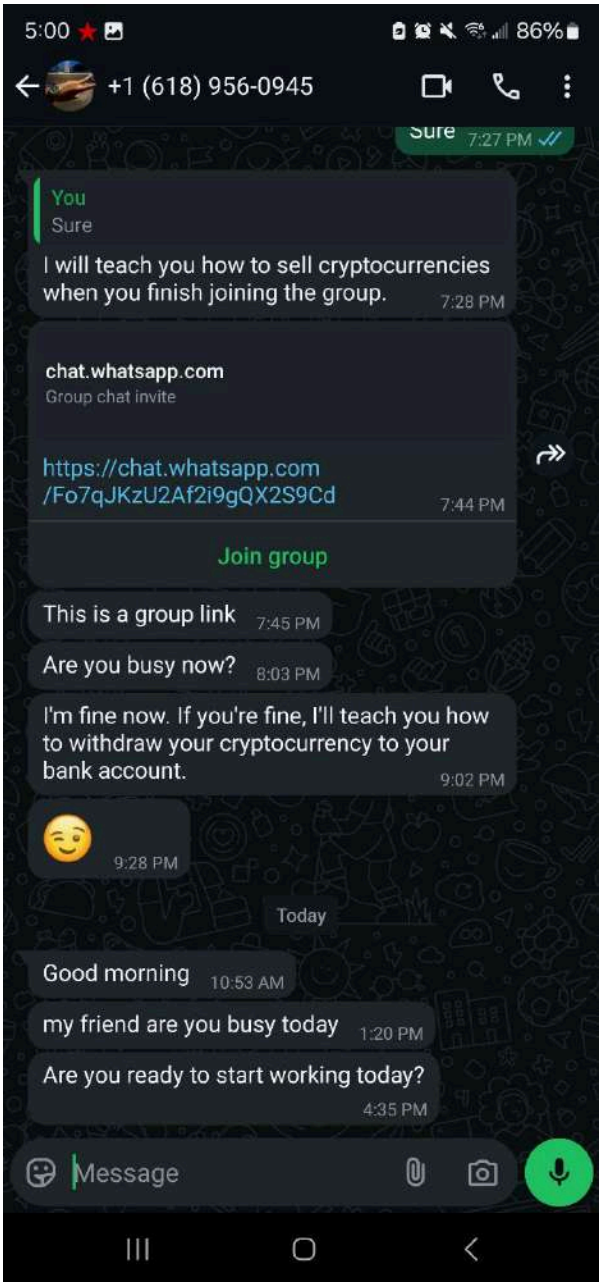

Figure 59: Emilia pushing us to join the group chat to finalize their scam process

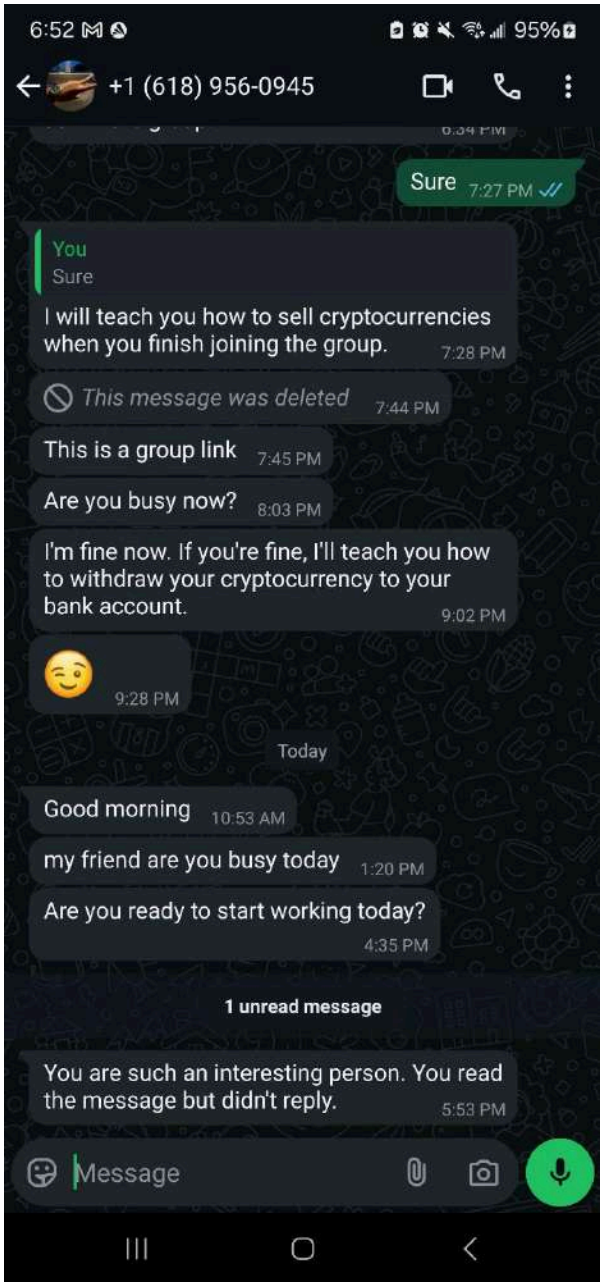

Figure 60: Notice the persistent from Emilia

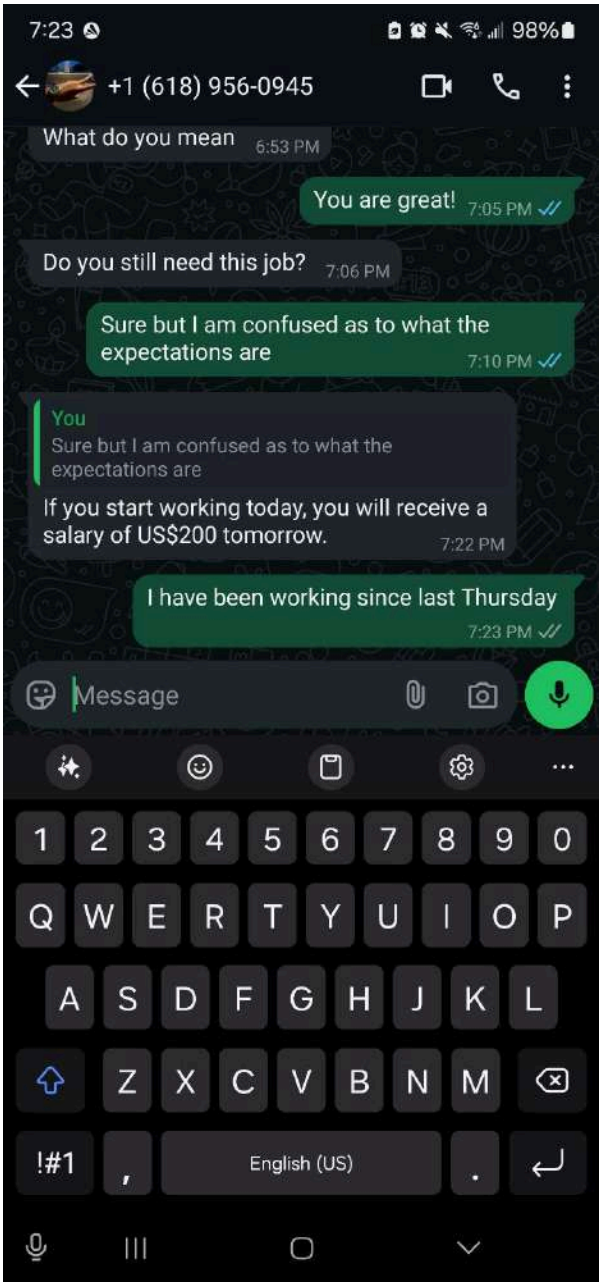

Figure 61: Emilia is pushing us to start to deposit the money to start to work

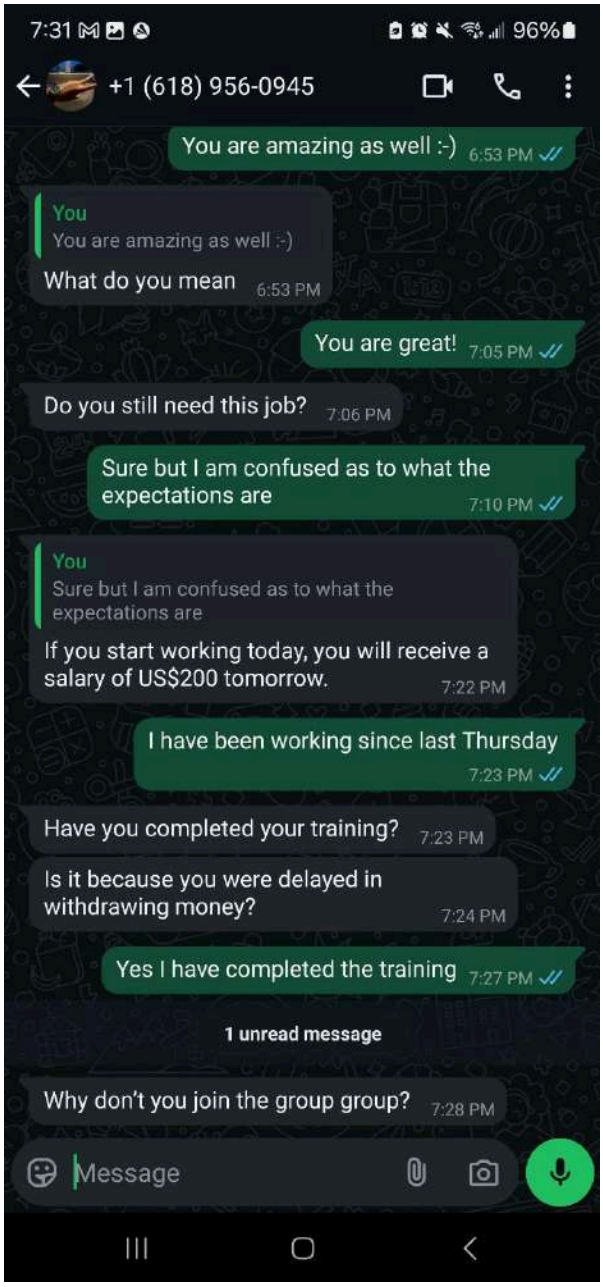

Figure 62: Persistent

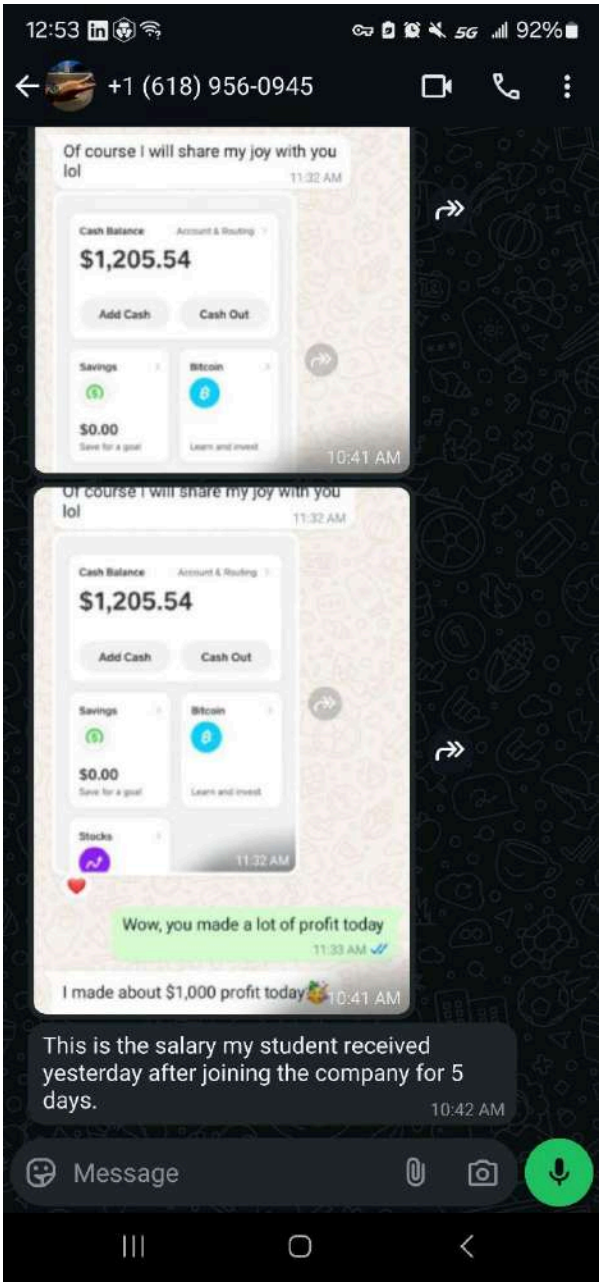

Figure 63: Emilia shows how much their student has made after five days, which contradicts the payout description provided in step 2.

The Scammer Working Group:

The scammer's working group, named "Dream Achievers," includes several administrators, including our recruiter, "Emilia." The group is moderated by an admin using the number (646) 577-8124, who actively blocks users not recognized as part of the group.

While it is unclear how many members are actual victims, the evidence strongly suggests that most participants are cybercriminals collaborating to create a convincing and supportive atmosphere designed to manipulate potential targets. Screenshots of the group and its members are provided below for reference.

Red Flag #21: Joining a group where member names or details are hidden is a significant warning sign. Legitimate professional groups are transparent about their members, roles, and purposes, unlike such covert setups designed to obscure fraudulent activities.

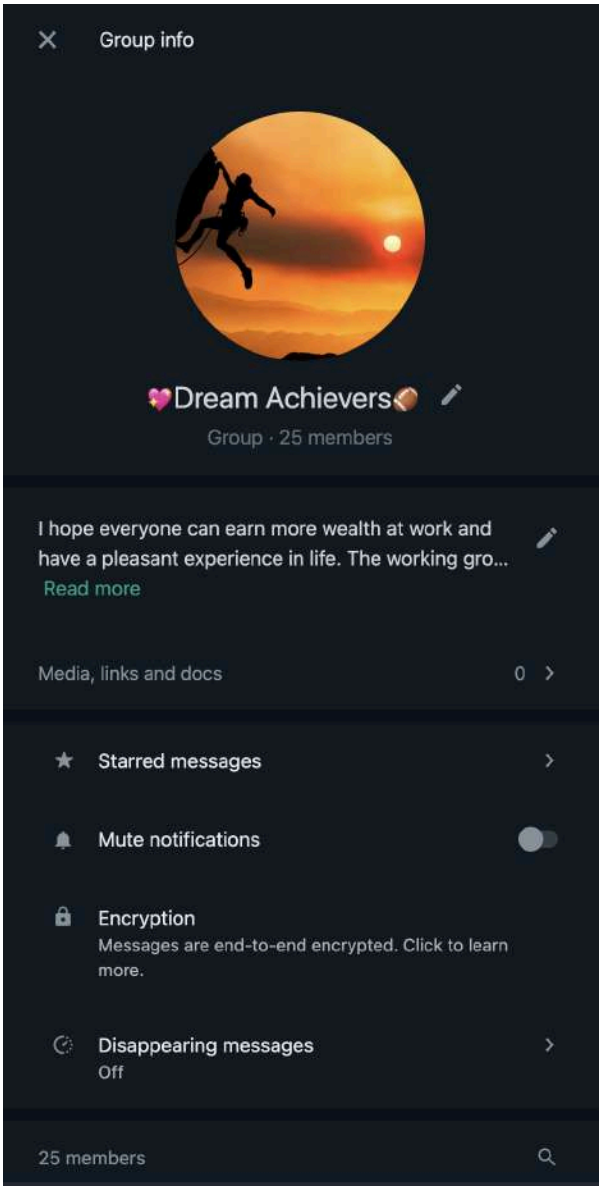

Figure 64: The working group profile

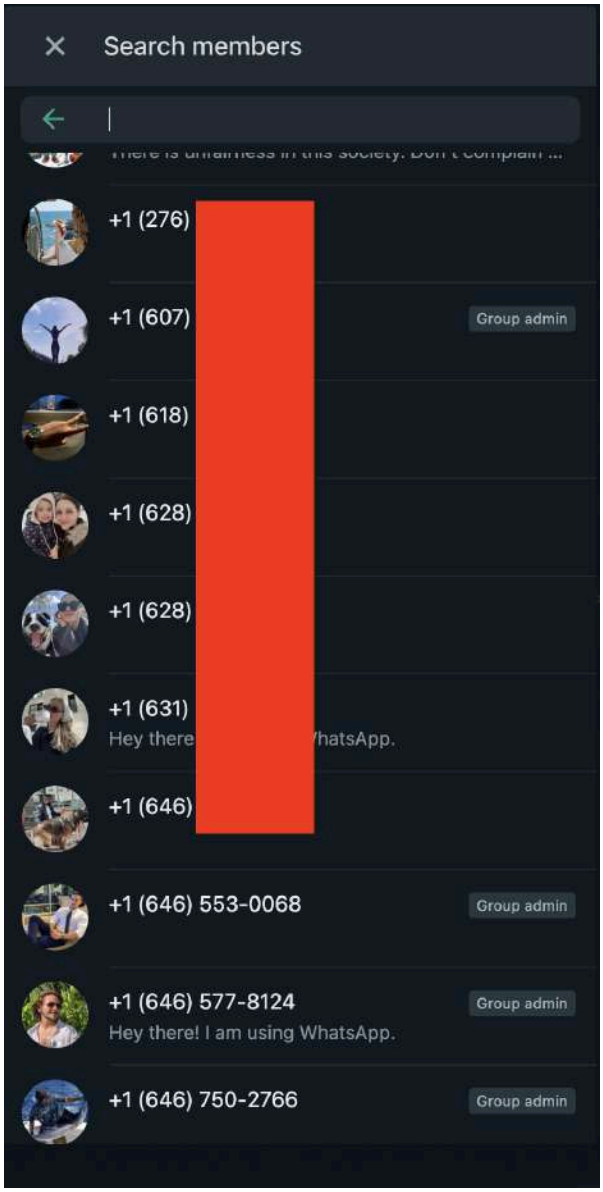

Figure 65: Admin in the working groups

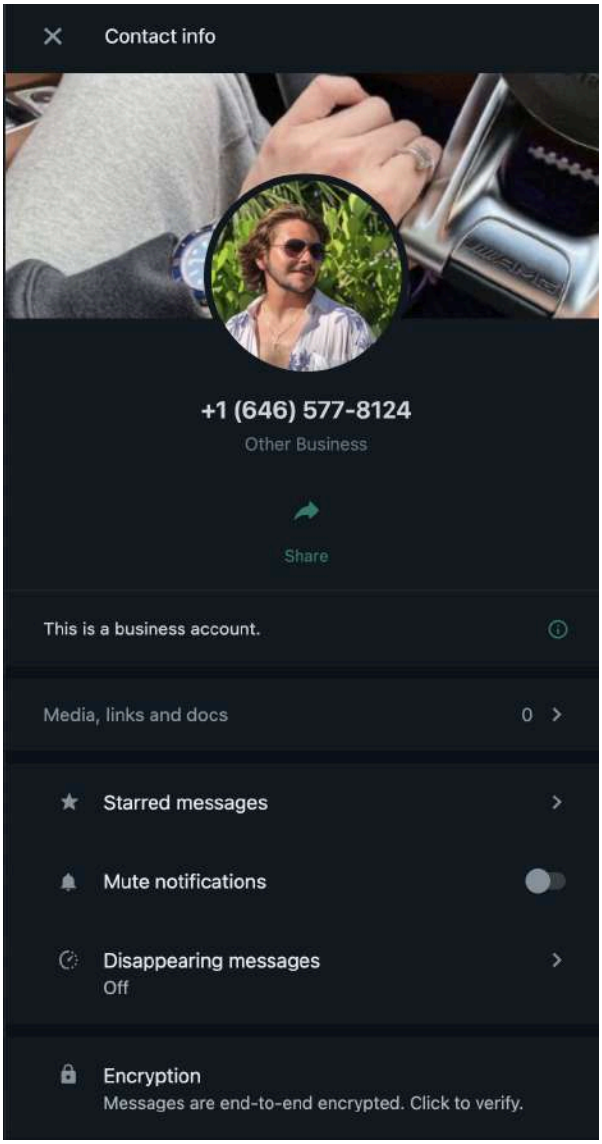

Figure 66: Whatsapp Group Admin

Step 6: Grab/Caught

In this phase, it is a critical moment where the scammer convinces the victim to deposit more money. This phase relies on manipulation and psychological tactics, exploiting trust, greed, or fear. Common techniques include:

1. **Showing Gains or Success**: The scammer often showcases fake profits or demonstrates an initial small payout to the victim. This builds trust and convinces the victim that their investment is legitimate and profitable.

2. **Limited-Time Offers**: The scammer may claim there is a "limited opportunity" or "urgent investment window" that requires the victim to act quickly. This creates a sense of urgency and prevents the victim from thinking critically.
3. **Emotional Manipulation**: Scammers might use emotional appeals, such as emphasizing the victim's potential financial success or their fear of missing out (FOMO), to compel action.
4. **Trust Building**: By portraying themselves as supportive and knowledgeable, the scammer positions themselves as an ally. They may even "invest" or "deposit" on behalf of the victim to make the process appear genuine.
5. **Problem-Solving Assistance**: If the victim encounters obstacles or expresses doubt, scammers offer solutions or additional "bonuses" to ease the victim's concerns, making them feel reassured.

These tactics combine to make victims feel obligated or motivated to deposit more money, deepening their entanglement in the scam. The scammers' ultimate goal is to draw the victim in repeatedly until they can extract the maximum possible financial gain.

The Scam:

Here's a real victim's story tied to this scam.

> In the beginning, someone reached out to me saying that I can make money quickly. At first I was suspicious and investigated. I asked if they have a website and everything and they do.
>
> But that still didn't stop me from being suspicious. So I entertained them a little by playing along.
>
> So they started messaging me through Whatsapp and walked me through the processes of making money through the website. They helped me create a crypto account.
>
> Once I finished
>
> We got started. They asked me to put in 100USD into the work account to do these

data clicks that helps apps get more exposure.

So I put in 100USD. After completing all my tasks, I would be able to withdraw my profits along with the 100USD I put in. That day, I made 214USD minus 100USD that put in. So I profitted 114USD.

I was like, "Oh, this is actually legit? I cant believe I made money this quickly."

This got me to actually trust them and I was blinded. So then, the next day I did my commissions as usual and profitted from it.

Then on my 3rd day. There was an event celebrating the company's 100,000 users. And that they give a 30% bonus to the amount you put into your asset balance.

And I was like, "hey if i put in 2000USD, I can get 600USD bonus."

Thats when it went downhill. There is this thing where as you are clicking each data, there is a chance that you will encounter a lucky data.

Lucky data turns your asset into negative and you would have to deposit the x negative amount thats in your asset balance. And in turn, you will get 10x the amount you profit from that single app.

So I did. And then I encountered 3 more lucky datas. By that point, I have no more money in my bank account.

I managed to complete all of my tasks.

But then when I tried to withdraw, I couldn't. Because I have to be a certain VIP to be able to withdraw a large sum.

As shown in the picture, I was at VIP 1. And VIP 1 - VIP 3 can only withdraw a max of 3000USD. And VIP 4 can withdraw an unlimited amount.

To activate VIP4, I have to deposit another 5000USD which at that point, I no longer have.

So now... I am here.

I just lost 12000USD which I have been saving for months. I can't get it back.

Ive fallen into Sunk Cost Fallacy by being in too deep to turn back and get my money back.

Source: https://www.reddit.com/r/Scams/comments/1fzj3x5/i_got_scammed_and_lost_12k/

Conclusion:

This paper has documented the progression of a sophisticated scam targeting individuals through a seemingly legitimate job opportunity. By analyzing the tactics employed by the fraud criminals—from initial recruitment through job descriptions to the eventual solicitation of deposits—we have outlined the various red flags and deceptive practices that characterize this fraudulent scheme. The use of fabricated websites, manipulation through psychological tactics, and the reliance on untraceable cryptocurrency transactions highlight the calculated nature of the scam.

Our investigation has revealed clear patterns and methods used by the fraud criminals to build trust, deceive targets, and ultimately profit from their financial contributions. By identifying the Ethereum and Bitcoin deposit addresses and analyzing the transactions associated with them, we estimate that several targets fallen for the scam, with substantial amounts of money deposited into the scammer-controlled wallets.

This analysis serves as a cautionary tale for potential targets of similar scams and emphasizes the need for vigilance when encountering unsolicited job offers, especially those involving unusual payment methods or requests for personal financial deposits. Awareness and education on these tactics are essential in preventing further victimization and minimizing the impact of such scams.