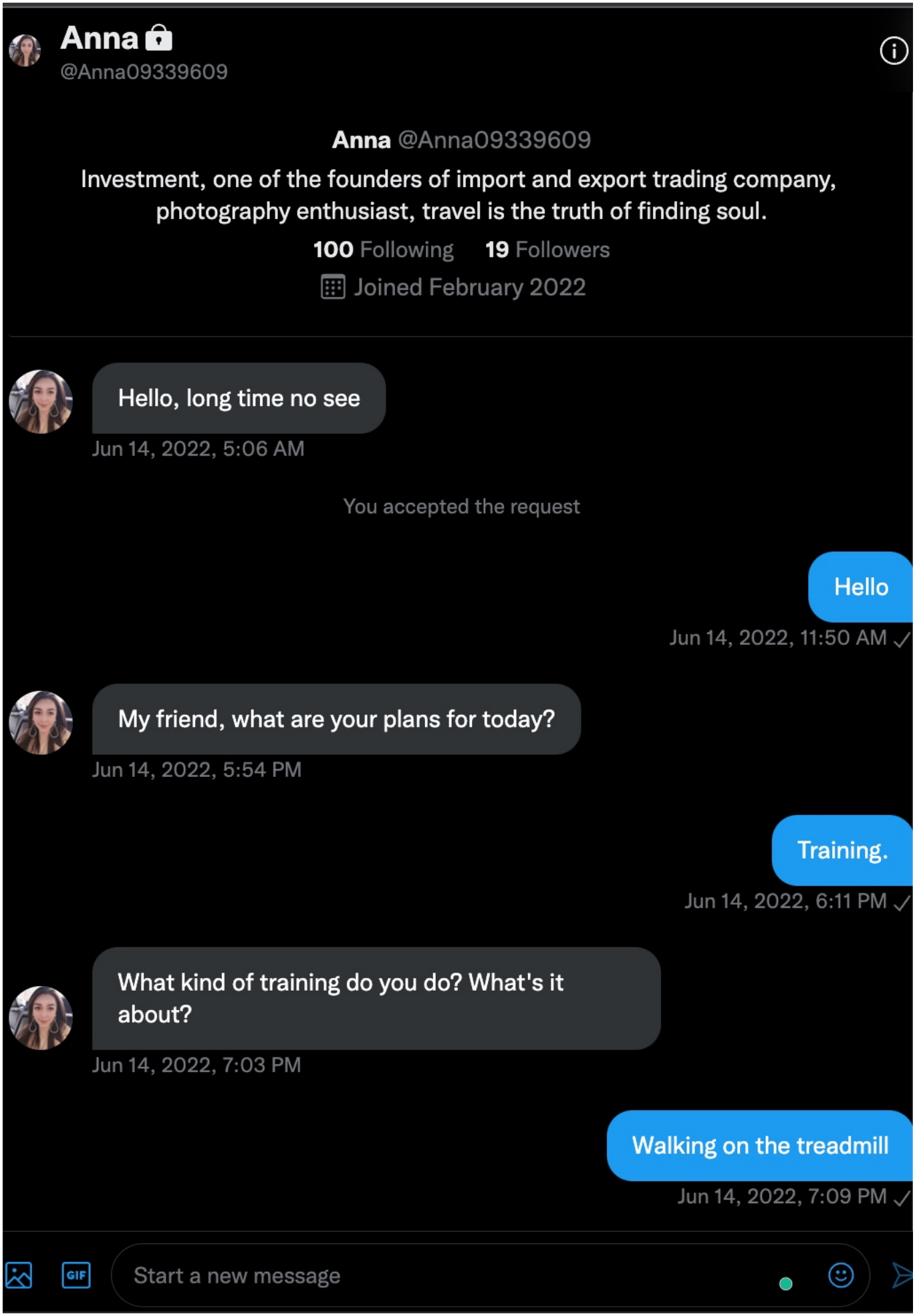
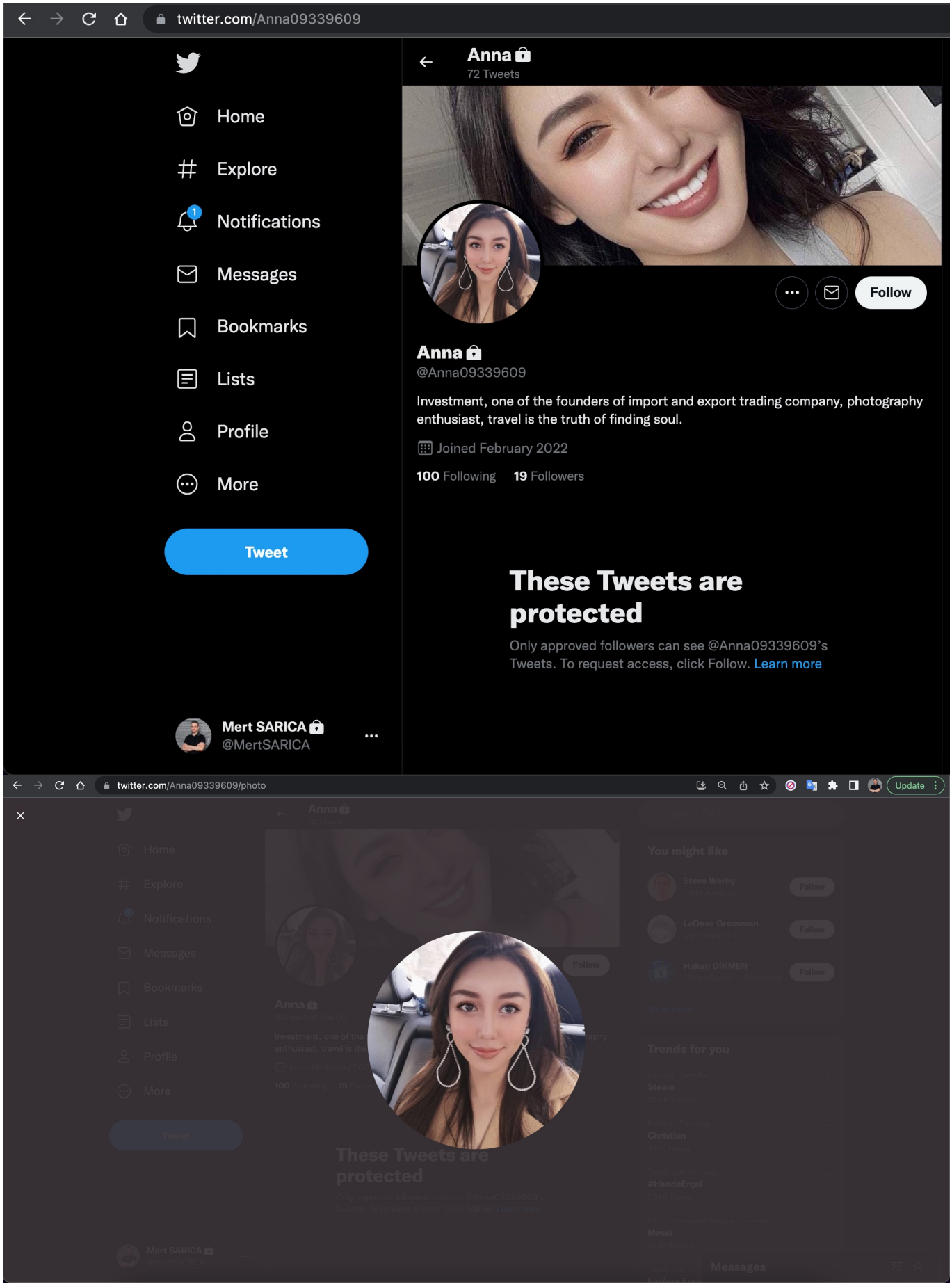
Exposing Pig Butchering Scam

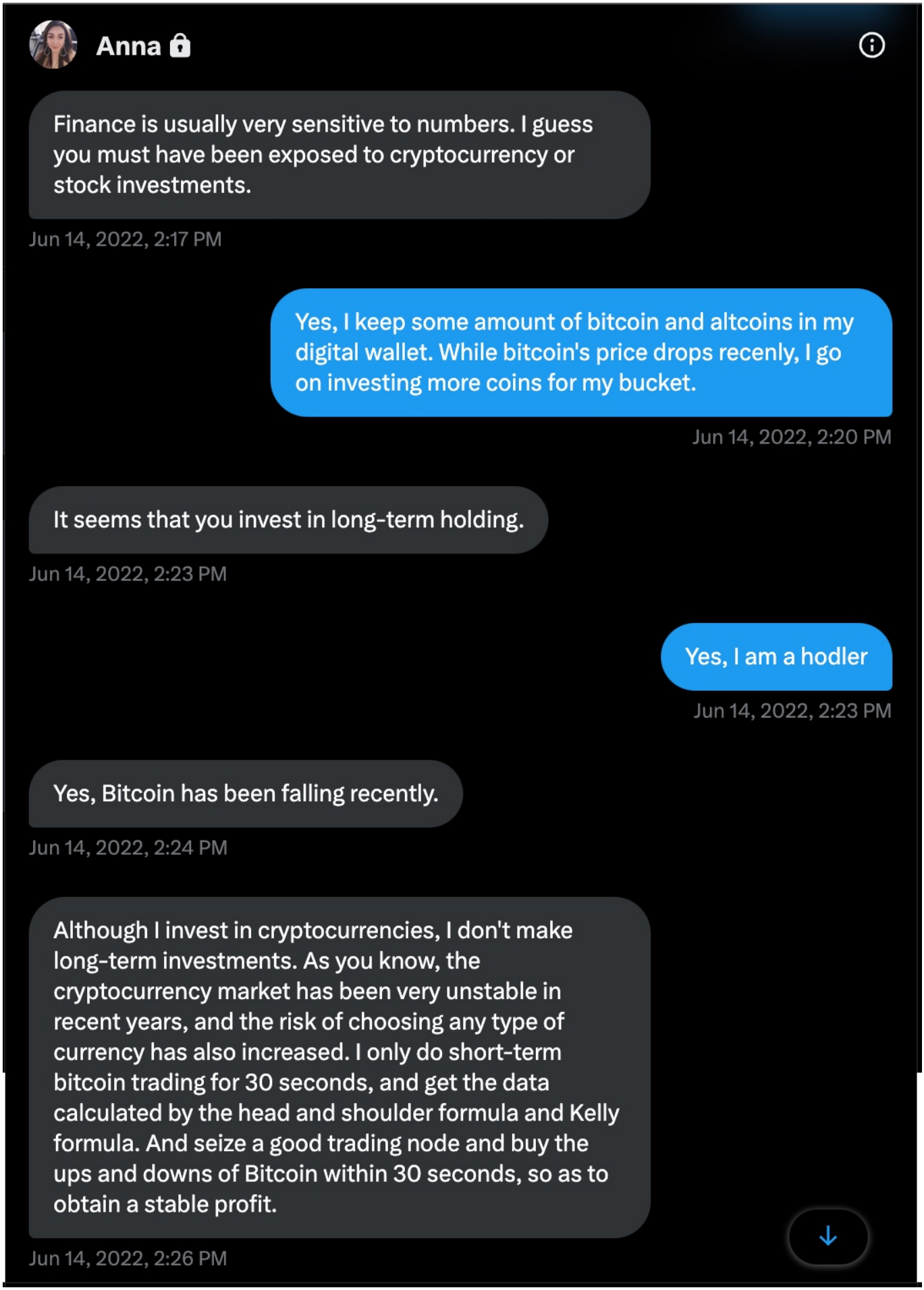
written by Mert SARICA | 1 March 2023

Over the years, as I have been targeted sometimes directly (LinkedIn Scammers, Sponsored Scamming) and sometimes indirectly (Who Viewed My Profile?) by scammers, I have made it my duty to write about these attempts in blog posts and warn those around me about them. At times, I have even received messages about scams from my spouse, friends, and close ones and have tried to write about them (Instagram Scammers) whenever I get the chance. And now, I am here again with a new scam attempt to expose.

As I announced through my Twitter account in June 2022, this attempt started with a message from a protected Twitter account named Anna on June 14, 2022. In this message, Anna started the conversation by talking about how she hasn’t seen me in a long time. After learning my name (Mark *fake*), where I live (a Belgian living in Turkey *fake*), and what I do (CFO of a FinTech company *fake*), the topic shifted to where I invest my money and the loss of value of Bitcoin cryptocurrency at that time.

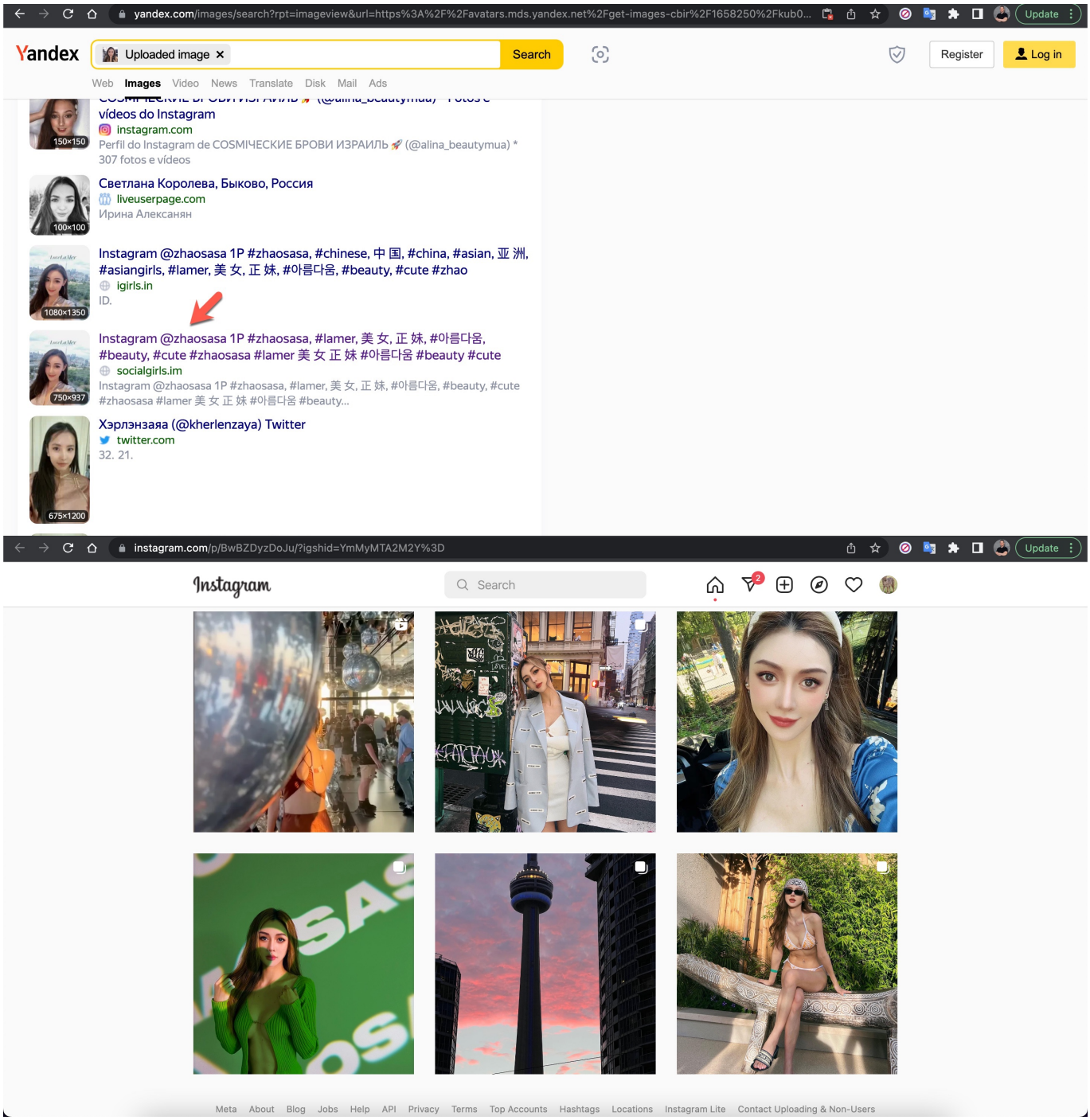

Anna
@Anna09339609
Anna @Anna09339609
Investment, one of the founders of import and export trading company, photography enthusiast, travel is the truth of finding soul.
100 Following 19 Followers
Joined February 2022
Hello, long time no see
Jun 14, 2022, 5:06 AM
You accepted the request
Hello
Jun 14, 2022, 11:50 AM
My friend, what are your plans for today?
Jun 14, 2022, 5:54 PM
Training.
Jun 14, 2022, 6:11 PM
What kind of training do you do? What's it about?
Jun 14, 2022, 7:03 PM
Walking on the treadmill
Jun 14, 2022, 7:09 PM
GIF
Start a new message

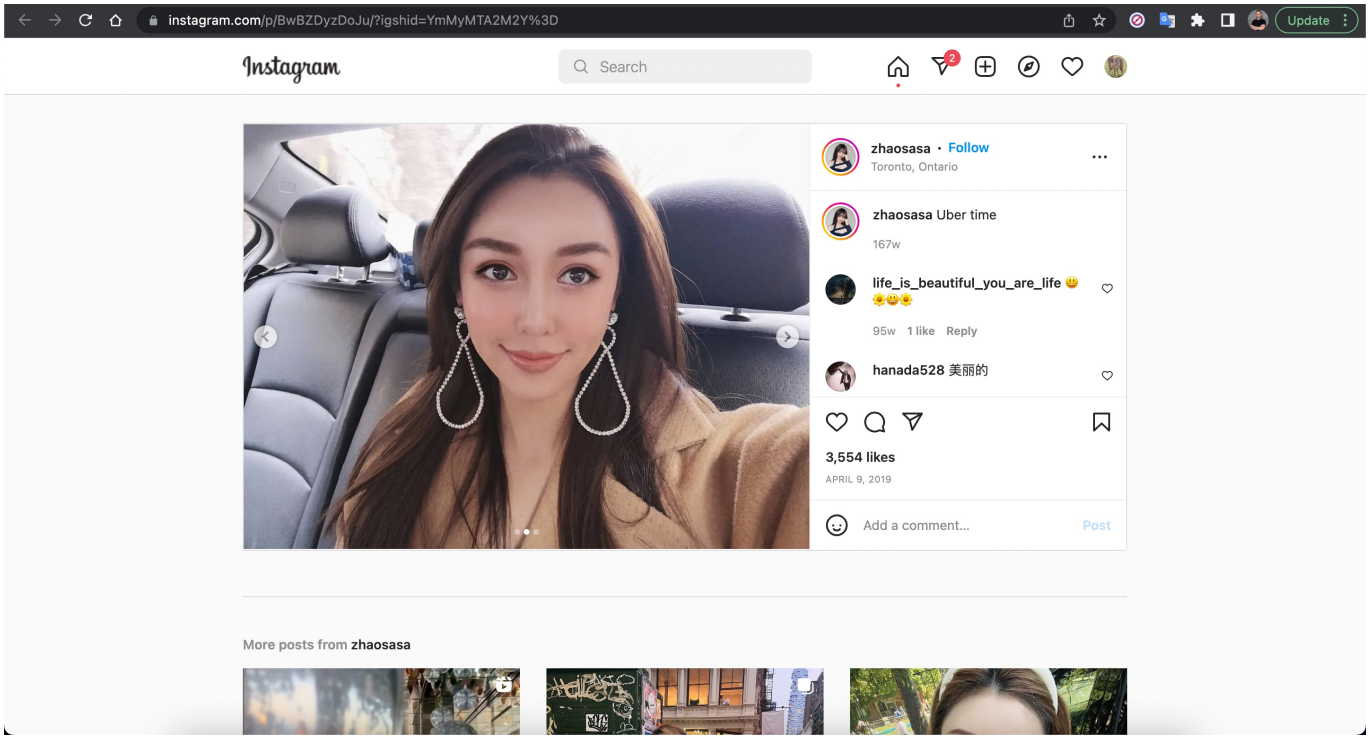

twitter.com/Anna09339609
Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet
Mert SARICA
@MertSARICA
Anna
72 Tweets
Follow
Anna
@Anna09339609
Investment, one of the founders of import and export trading company, photography enthusiast, travel is the truth of finding soul.
Joined February 2022
100 Following
19 Followers
These Tweets are protected
Only approved followers can see @Anna09339609's Tweets. To request access, click Follow. Learn more
twitter.com/Anna09339609/photo
Update



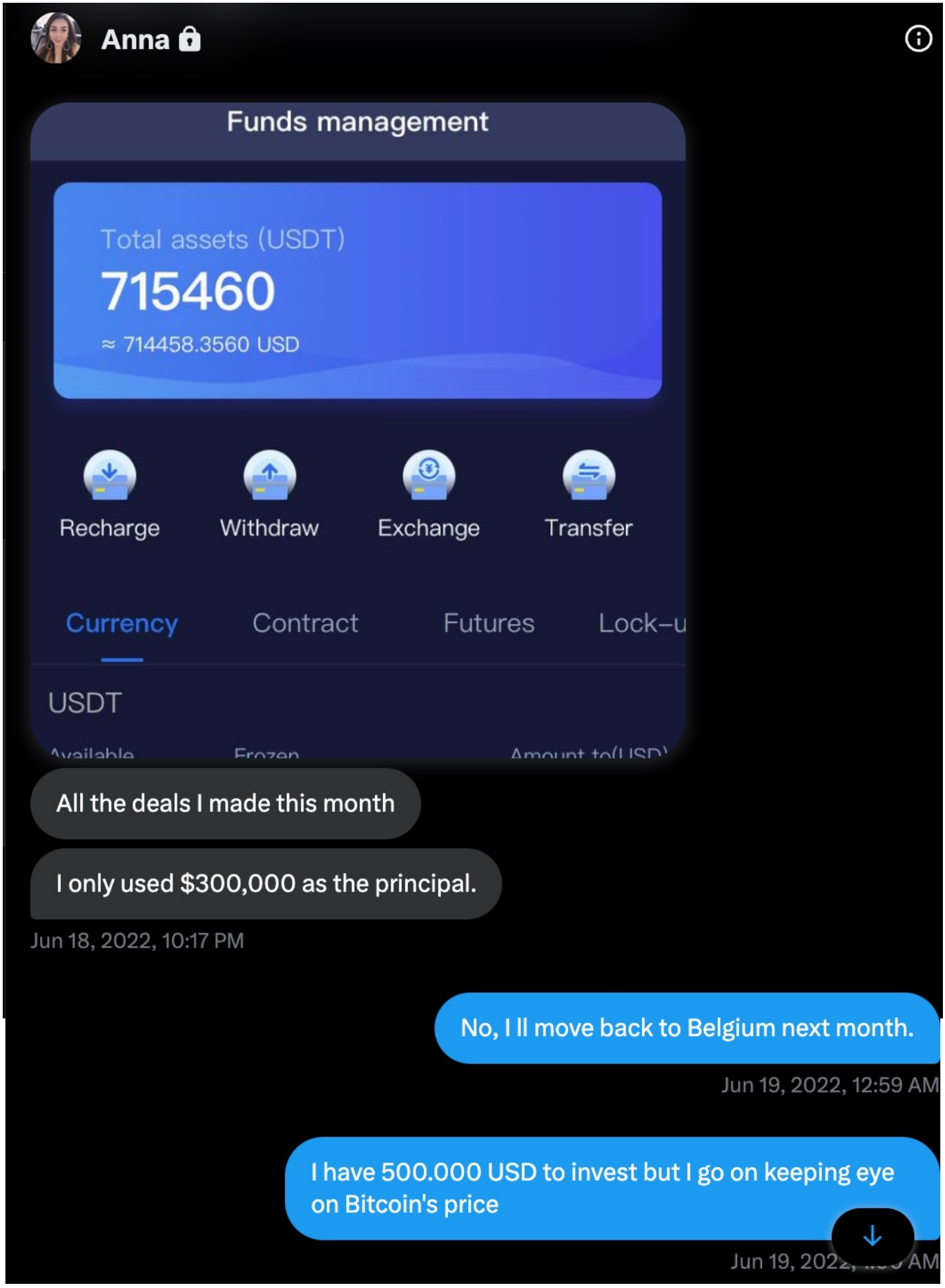
I took a break from the conversation and decided to find out who the photo on

Anna’s profile really belonged to, as I suspected it was fake. To do this, I used the Visual Search feature of the Yandex search engine and discovered that the profile photo belonged to a Chinese person named Shasha Zhao. When I looked at the photos shared on Shasha’s profile, I found the exact photo on Anna’s profile.



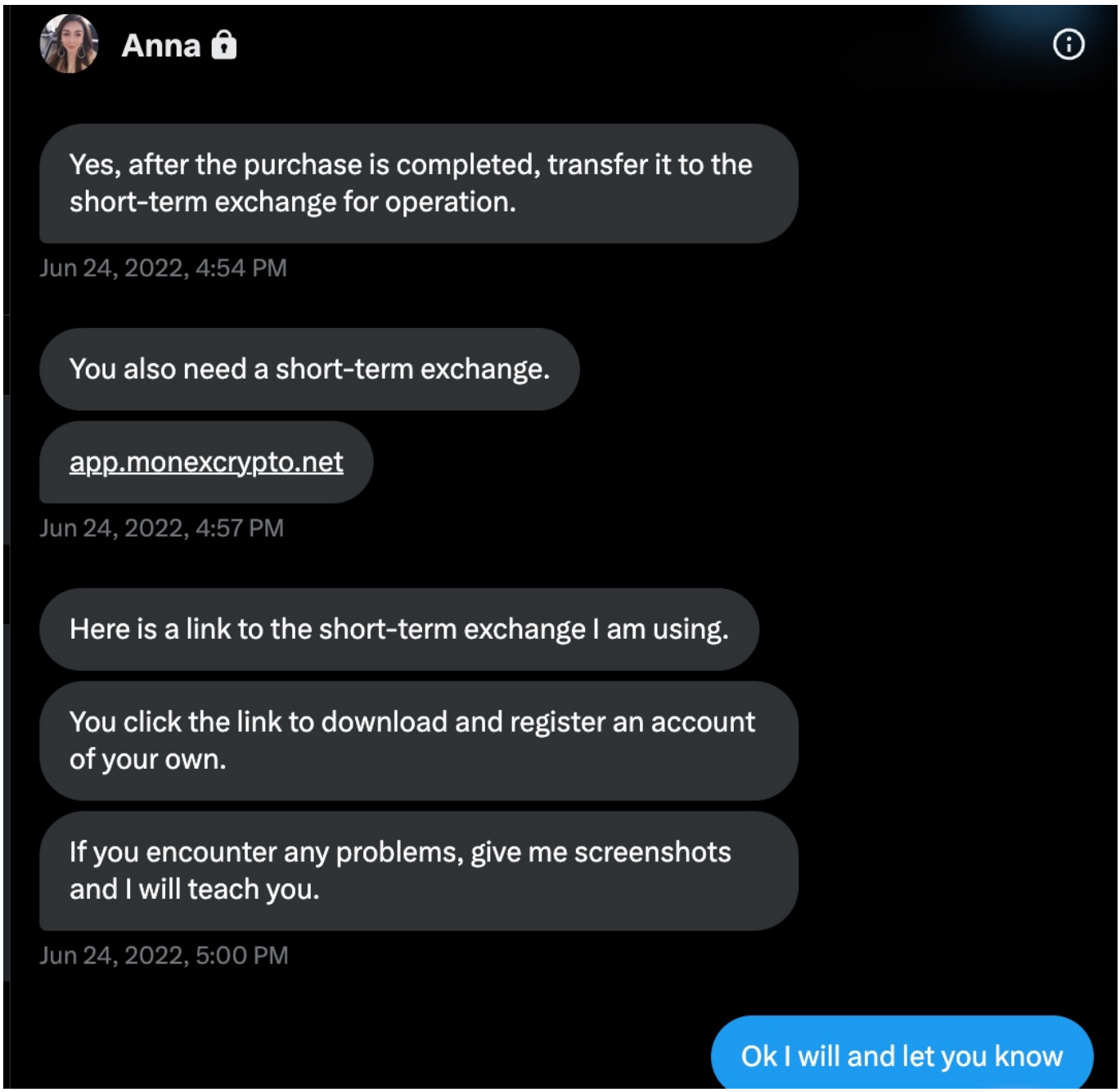


Anna, who initially claimed to live in Singapore and founder of a garment import and export trading company, asked to continue the conversation on WhatsApp and shared a US phone number (+19295654212) with me. When I questioned her about using a US phone number, she changed her story, saying she lived in the US for business reasons. To pique my interest, she then claimed to have made a profit of around $715,000 from a crypto investment of $300,000. I informed her that I was considering investing $500,000 to see her tactics for quickly making a profit.

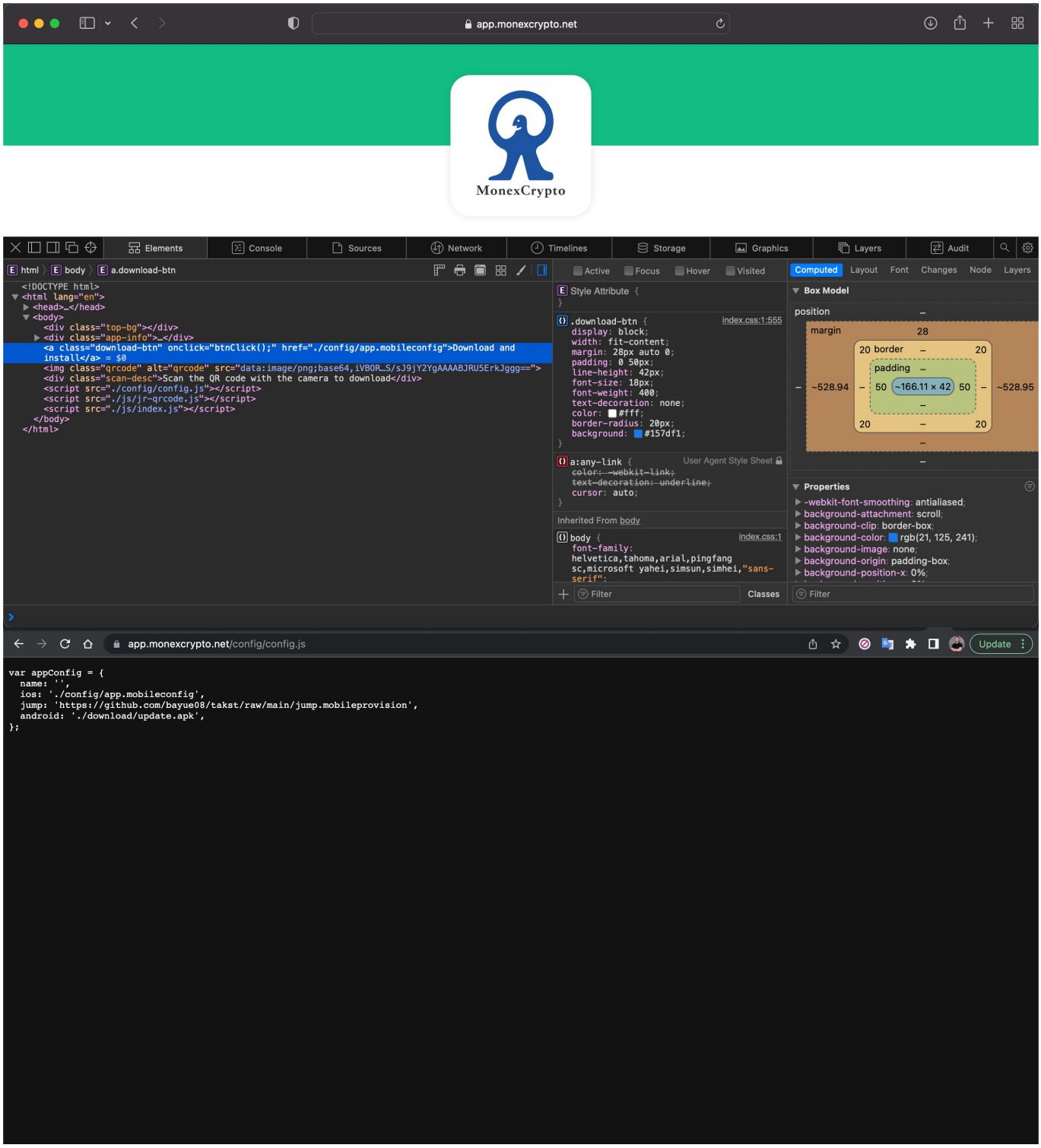


After sharing that I consider her to be a very good investor and want to invest with her, she told me that I need to enter the MonexCrypto platform

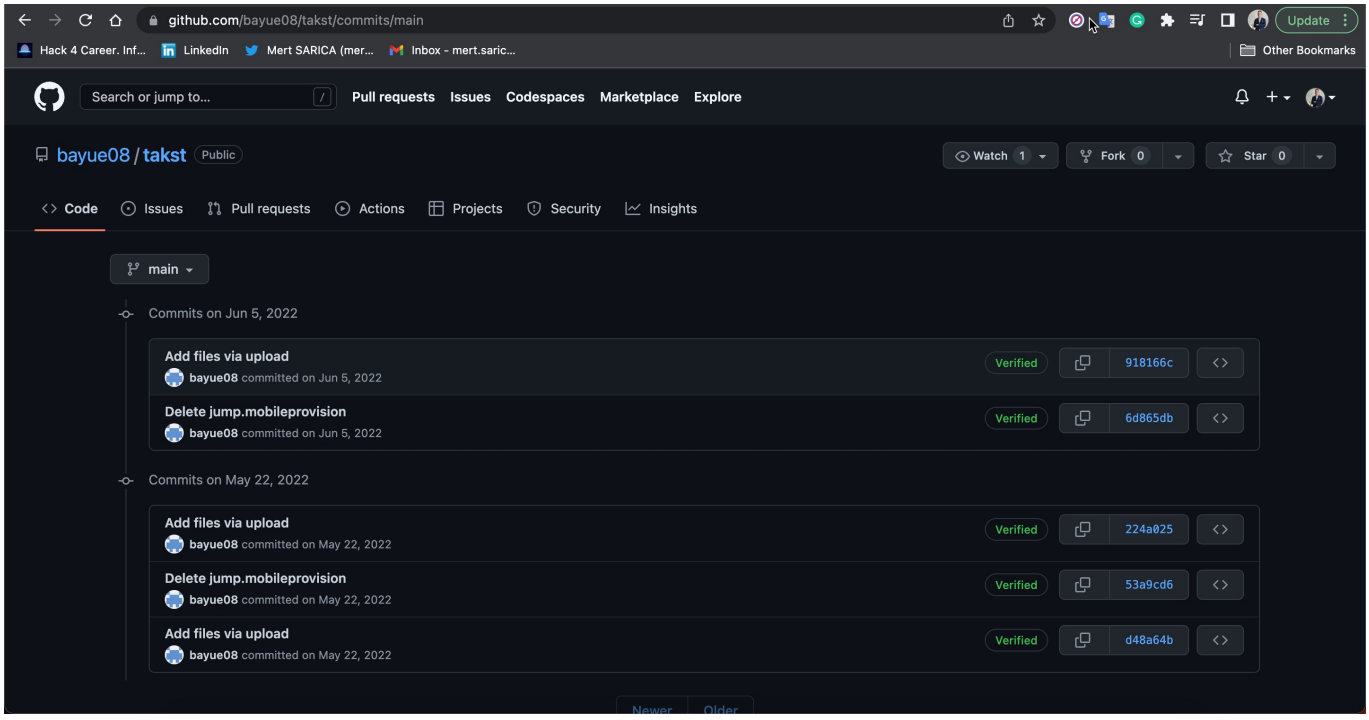
for short-term investments. She also shared that I need to visit the https://app[.]monexcrypto[.]net address, download the mobile application, and register.



I went to the website to download the mobile application and when I looked at the source code of the webpage, I found out that there was both an Android (update.apk) and an iOS version of the app. After uploading the Android app to VirusTotal and Pithus, a mobile threat intelligence platform, and quickly checking the somewhat suspicious results, I decided to thoroughly examine the version developed for the iOS operating system.


app.monexcrypto.net
MonexCrypto
Elements
Console
Sources
Network
Timelines
Storage
Graphics
Layers
Audit
<!DOCTYPE html>
<html lang="en">
<head>…</head>
<body>

…
Download and install = $0
<img class="qrcode" alt="qrcode" src="…S/sJ9jY2YgAAAABJRU5ErkJggg==">
Scan the QR code with the camera to download
<script src="./config/config.js"></script>
<script src="./js/jr-qrcode.js"></script>
<script src="./js/index.js"></script>
</body>
</html>
.download-btn { index.css:1:555
display: block;
width: fit-content;
margin: 28px auto 0;
padding: 0 50px;
line-height: 42px;
font-size: 18px;
font-weight: 400;
text-decoration: none;
color: #fff;
border-radius: 20px;
background: #157df1;
a:any-link { User Agent Style Sheet
color: -webkit-link;
text-decoration: underline;
cursor: auto;
Inherited From body
body { index.css:1
font-family:
helvetica,tahoma,arial,pingfang sc,microsoft yahei,simsun,simhei,"sans-serif";
Box Model
position
margin 28
~528.94
20 border 20
padding
50 ~166.11 × 42 50
~528.95
Properties
-webkit-font-smoothing: antialiased;
background-attachment: scroll;
background-clip: border-box;
background-color: rgb(21, 125, 241);
background-image: none;
background-origin: padding-box;
background-position-x: 0%;
app.monexcrypto.net/config/config.js
Update
var appConfig = {
name: '',
ios: './config/app.mobileconfig',
jump: 'https://github.com/bayue08/takst/raw/main/jump.mobileprovision',
android: './download/update.apk',
};



After seeing that the mobileprovision file, which enables third-party applications to run on the iOS operating system, is stored on GitHub, I viewed the information about the developer/company (QuanLi Network Technology Co., Ltd. (SRD7J8LLBV)) registered in the Apple Developer Program.

jump.mobileprovision.2205.2022-2.mobileprovision

Open with Xcode

wql220604

Expired 7 months ago

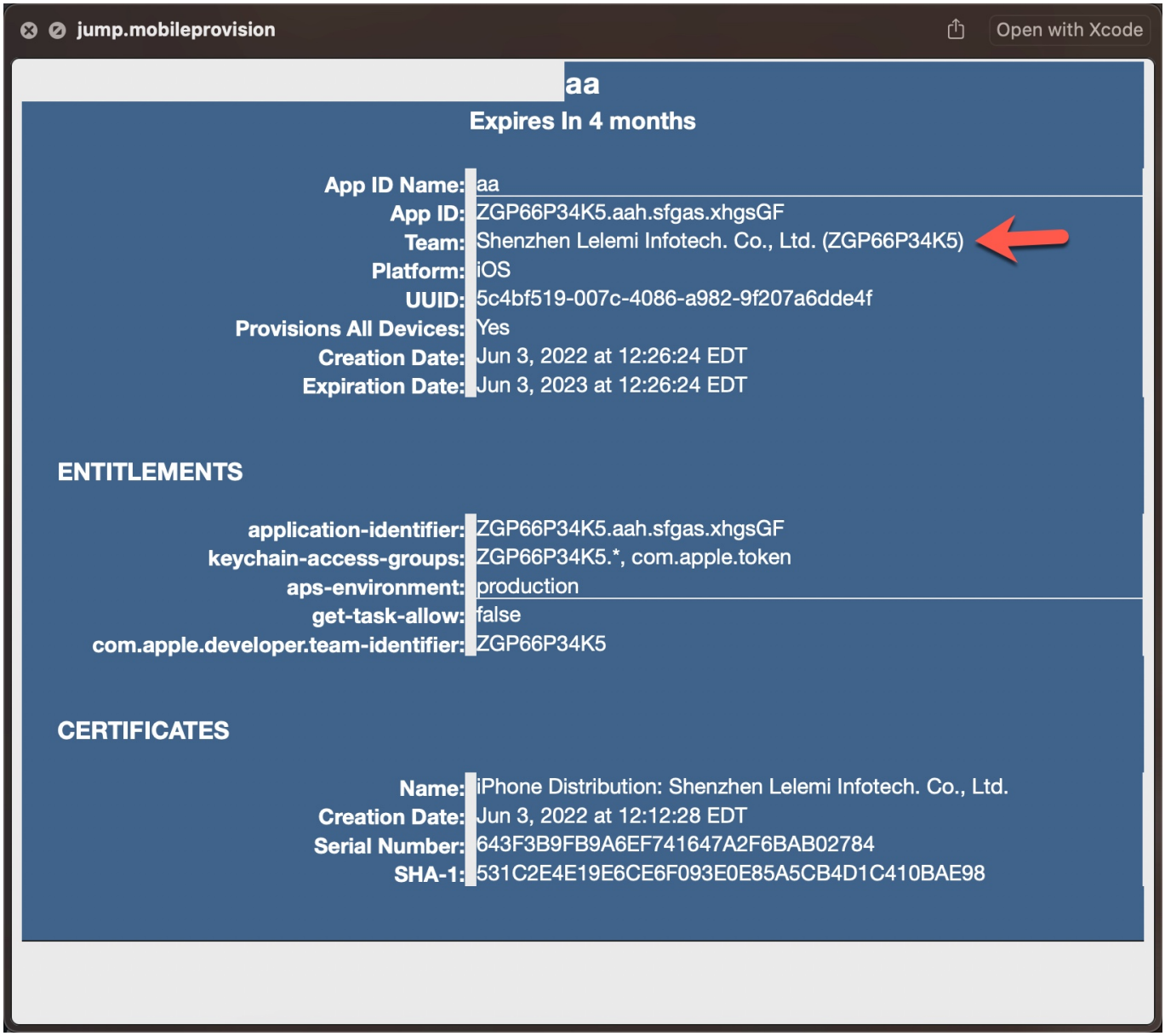
App ID Name:	iosplayer
App ID:	SRD7J8LLBV.com.weiquanli.iosplayer
Team:	QuanLi Network Technology Co., Ltd. (SRD7J8LLBV)
Platform:	iOS
UUID:	f464148a-77ac-4a72-a15e-f1ed214212f8
Provisions All Devices:	Yes
Creation Date:	Jun 4, 2021 at 03:02:28 EDT
Expiration Date:	Jun 4, 2022 at 03:02:28 EDT

ENTITLEMENTS

keychain-access-groups:	SRD7J8LLBV.*, com.apple.token
com.apple.external-accessory.wireless-configuration:	true
com.apple.developer.healthkit.access:	health-records
com.apple.developer.ubiquity-container-identifiers:	SRD7J8LLBV.*
get-task-allow:	false
com.apple.developer.default-data-protection:	NSFileProtectionComplete
com.apple.developer.healthkit:	true
com.apple.developer.associated-domains:	*
com.apple.developer.team-identifier:	SRD7J8LLBV
com.apple.security.application-groups:	Unknown
application-identifier:	SRD7J8LLBV.com.weiquanli.iosplayer
com.apple.developer.ubiquity-kvstore-identifier:	SRD7J8LLBV.*
com.apple.developer.homekit:	true

CERTIFICATES

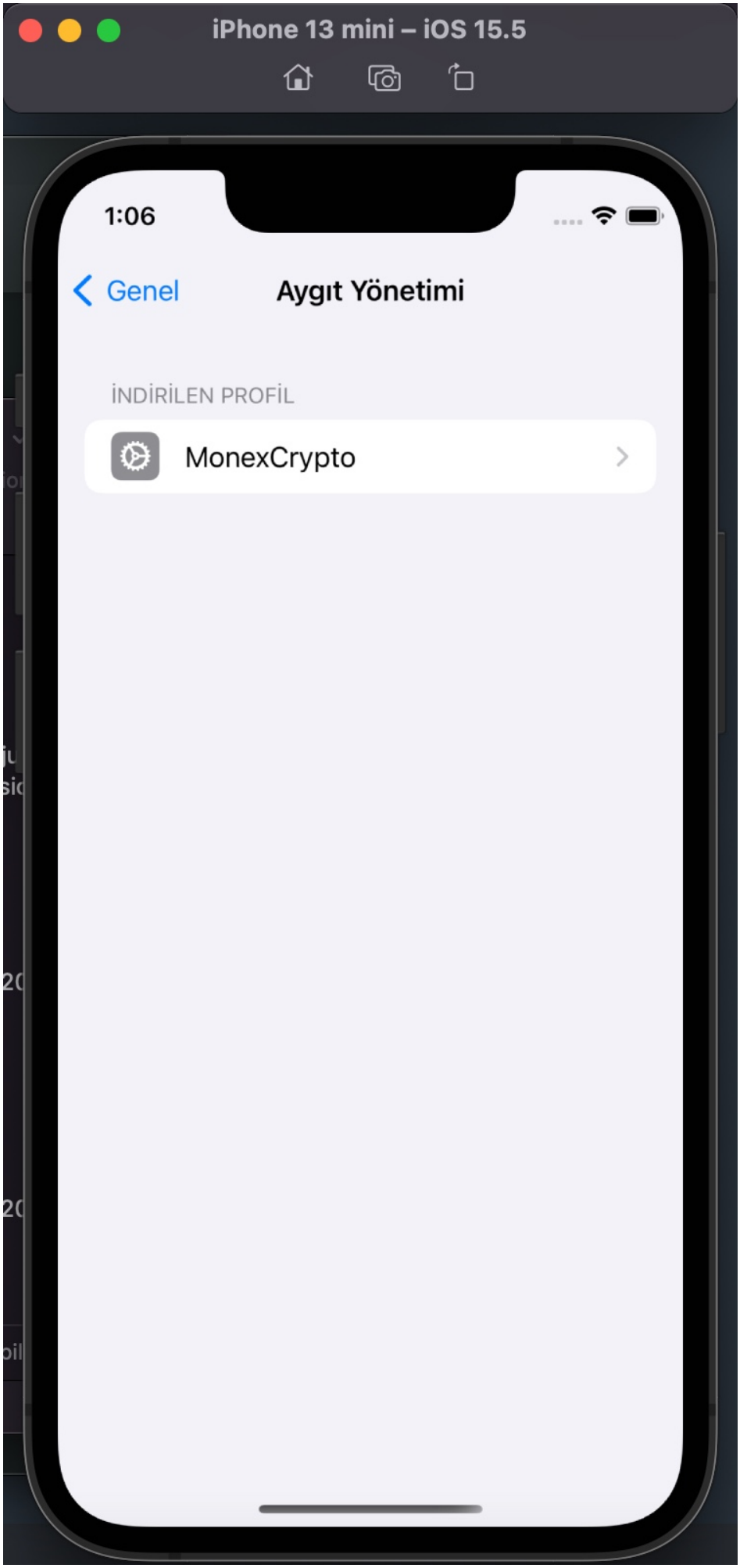
Name:	iPhone Distribution: QuanLi Network Technology Co., Ltd.
Creation Date:	Apr 9, 2020 at 10:39:23 EDT
Serial Number:	04F4A485C1B2F933
SHA-1:	F4AD79B2285828A32B124AC7EB4D664013F8CCC5

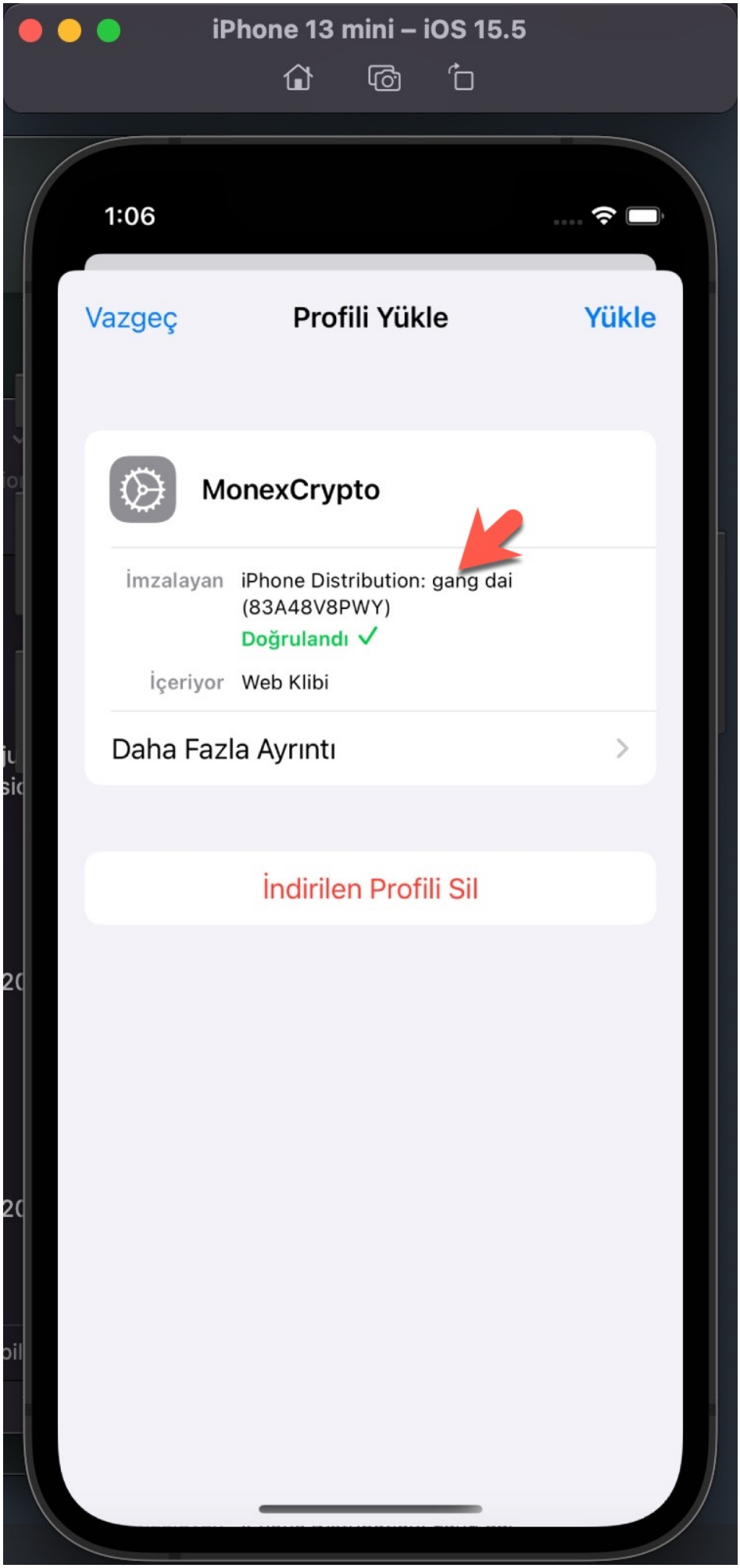


I examined the app.mobileconfig XML file, consisting of payloads that load settings and authorization information onto Apple devices. When I ran the file in the Simulator application located in Xcode, I learned that it is a Web Clip (WebClip) that opens the https://www.monexcrypto.net web page and is signed by a developer named Gang Dai.

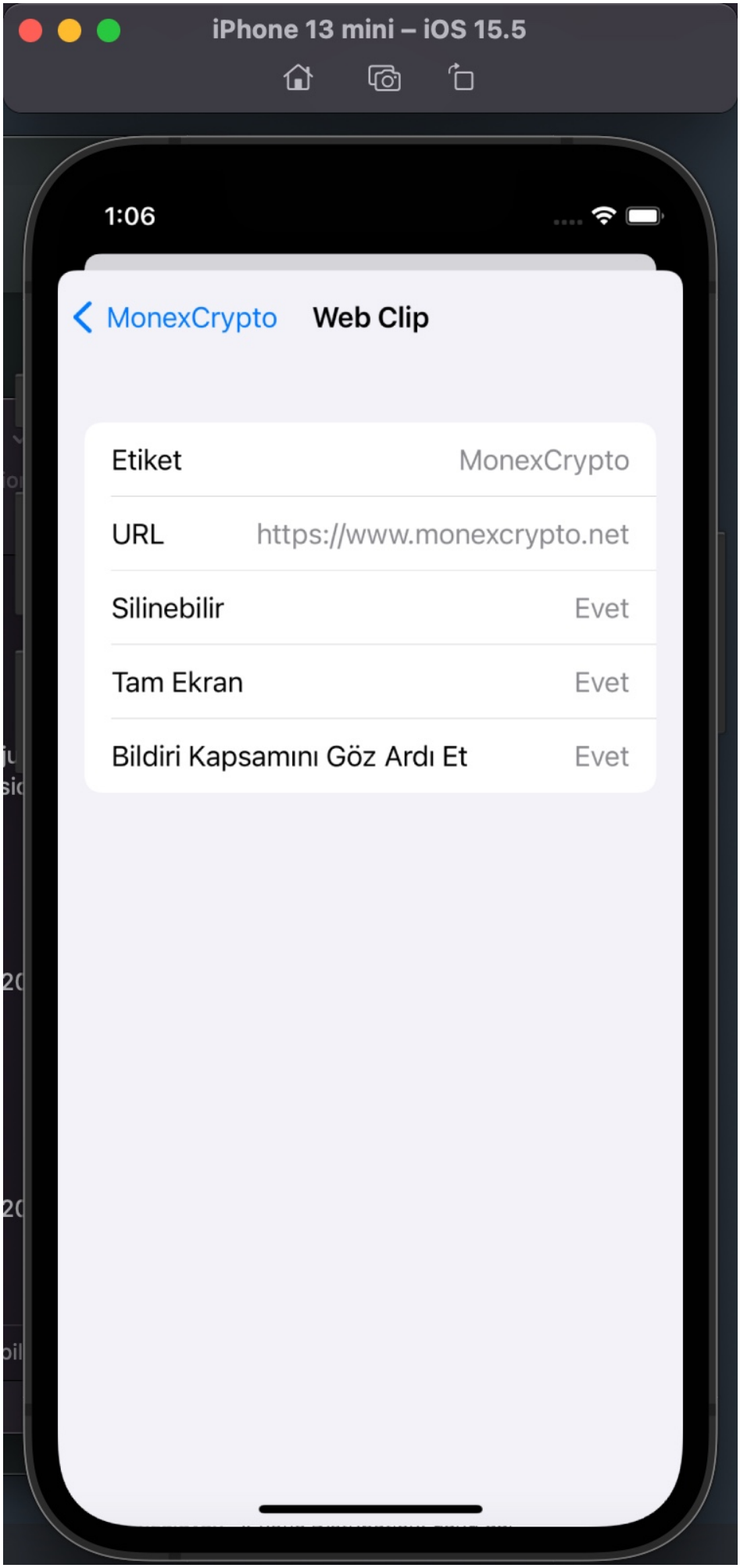
Web clips: A web clip is an icon on the device Home screen that links to a website or URL. Web clips can optionally launch full-screen web apps and can run offline using HTML5 local storage. Configuration profiles can include web clips that use a custom title and icon, and can optionally be nonremovable. Web clips can point students to specific websites for educational purposes. For more information about configuring web clips on a device, see WebClip profile page in Apple Developer documentation.

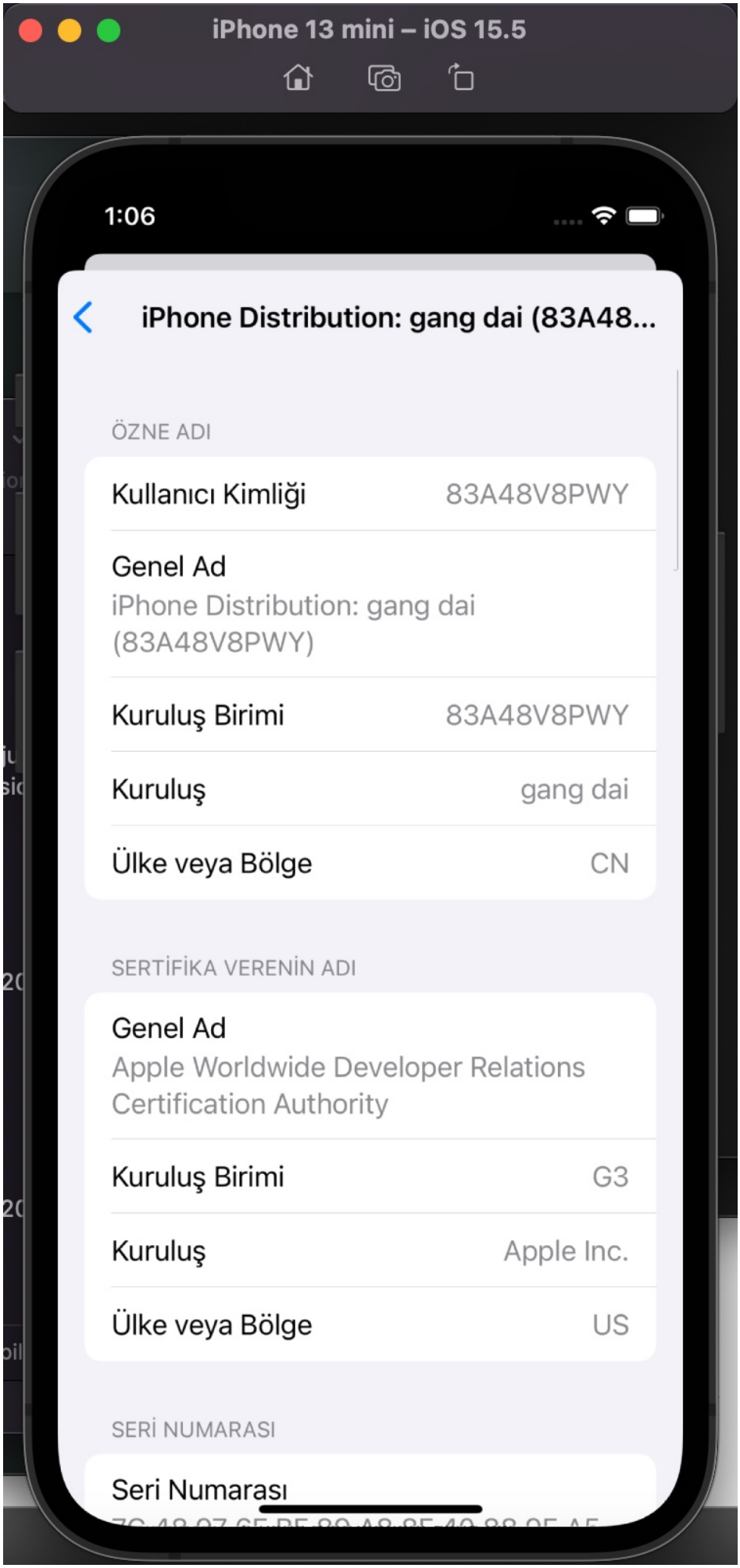
iPhone 13 mini – iOS 15.5
1:05
Bu web sitesi bir konfigürasyon profili göstermek istiyor. İzin vermek istiyor musunuz?
Yok Say
İzin Ver
p/YeniYazi/Monex/app.mobileconfig

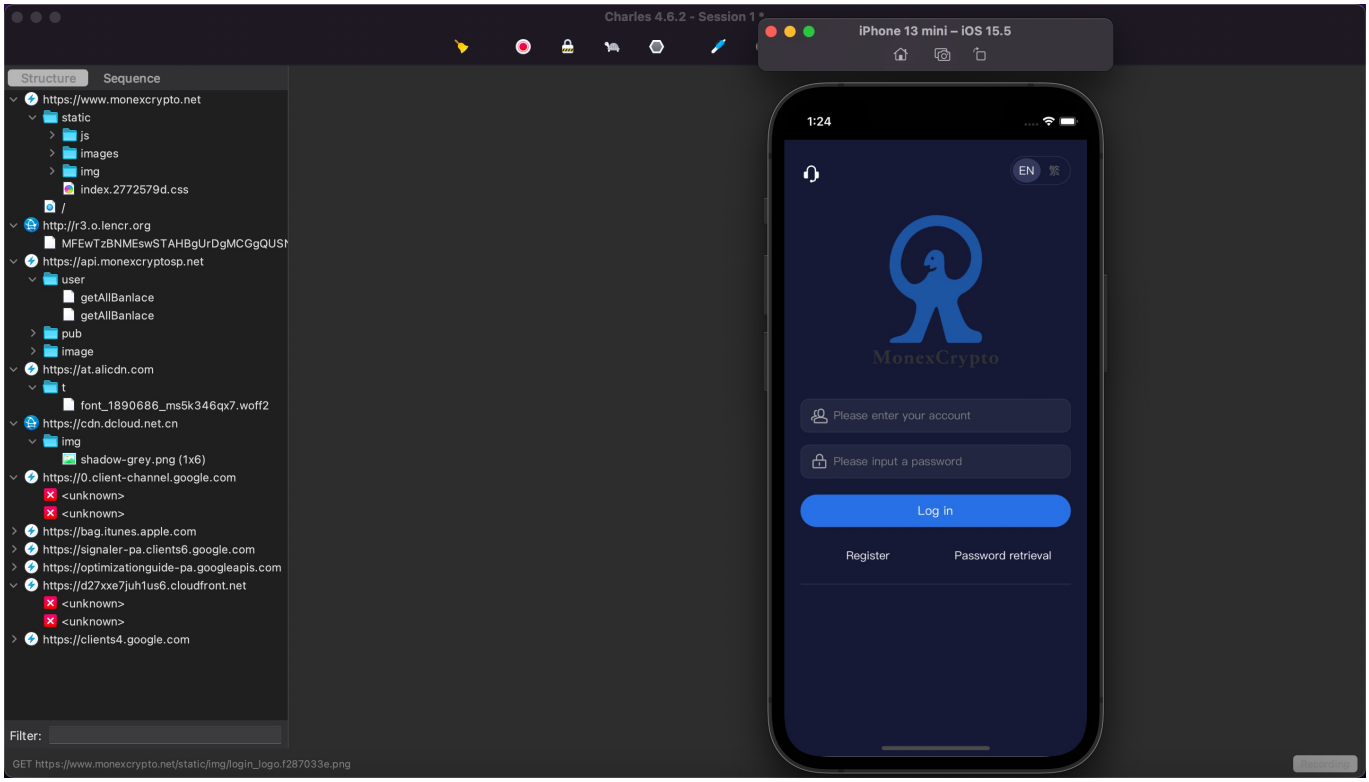

iPhone 13 mini – iOS 15.5
1:06
Genel
Aygıt Yönetimi
İNDİRİLEN PROFİL
MonexCrypto


iPhone 13 mini – iOS 15.5
1:06
Vazgeç
Profili Yükle
Yükle
MonexCrypto
İmzalayan
iPhone Distribution: gang dai
(83A48V8PWY)
Doğrulandı
İçeriyor
Web Klibi
Daha Fazla Ayrıntı
İndirilen Profili Sil

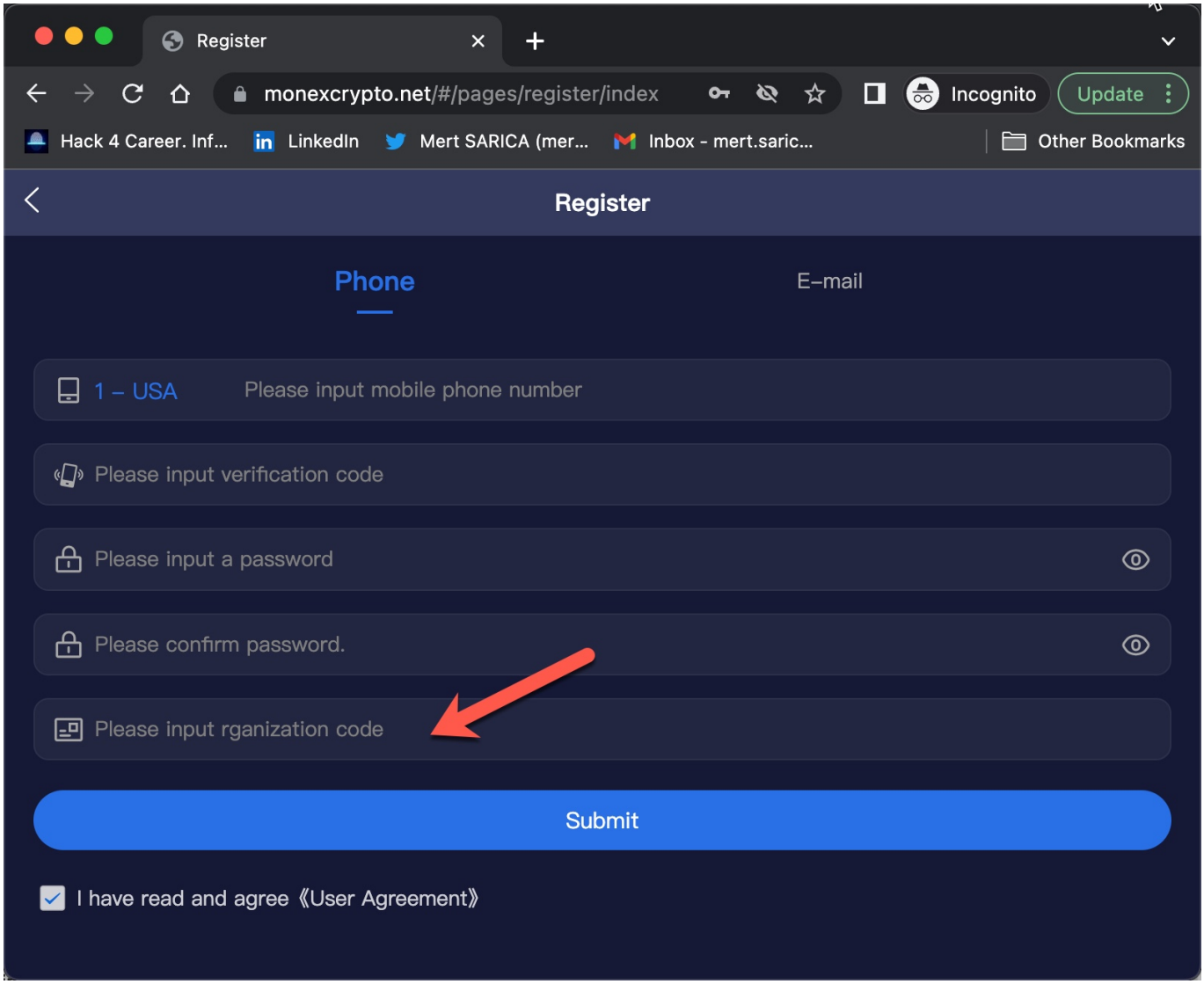
iPhone 13 mini – iOS 15.5
1:06
Profili Yükle
MonexCrypto
WEB KLİBİ
Web Klibi
URL: https://www.monexcrypto.net
Etiket: MonexCrypto
İMZALAMA SERTİFİKALARI
iPhone Distribution: gang dai (83A48V8PWY)
Sertifika Veren: Apple Worldwide Developer Relations Certification Authority
Bitiş: 11 Mart 2023
Apple Worldwide Developer Relations Certification Authority
Sertifika Veren: Apple Root CA
Bitiş: 20 Şubat 2030


iPhone 13 mini – iOS 15.5
1:06
MonexCrypto
Web Clip
Etiket
MonexCrypto
URL
https://www.monexcrypto.net
Silinebilir
Evet
Tam Ekran
Evet
Bildiri Kapsamını Göz Ardı Et
Evet

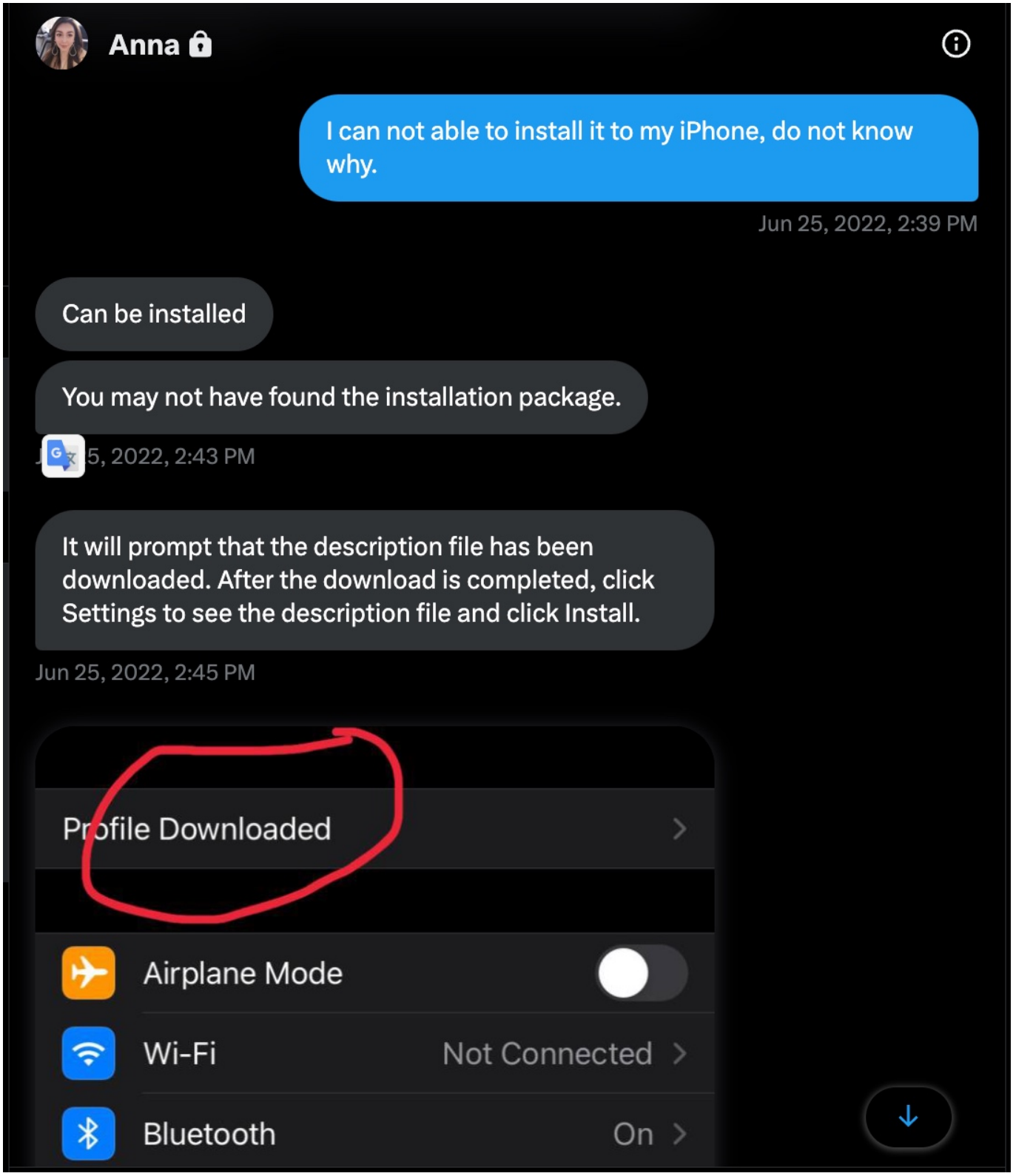

iPhone 13 mini – iOS 15.5
1:06
iPhone Distribution: gang dai (83A48...
ÖZNE ADI
Kullanıcı Kimliği
83A48V8PWY
Genel Ad
iPhone Distribution: gang dai (83A48V8PWY)
Kuruluş Birimi
83A48V8PWY
Kuruluş
gang dai
Ülke veya Bölge
CN
SERTİFİKA VERENİN ADI
Genel Ad
Apple Worldwide Developer Relations Certification Authority
Kuruluş Birimi
G3
Kuruluş
Apple Inc.
Ülke veya Bölge
US
SERİ NUMARASI
Seri Numarası

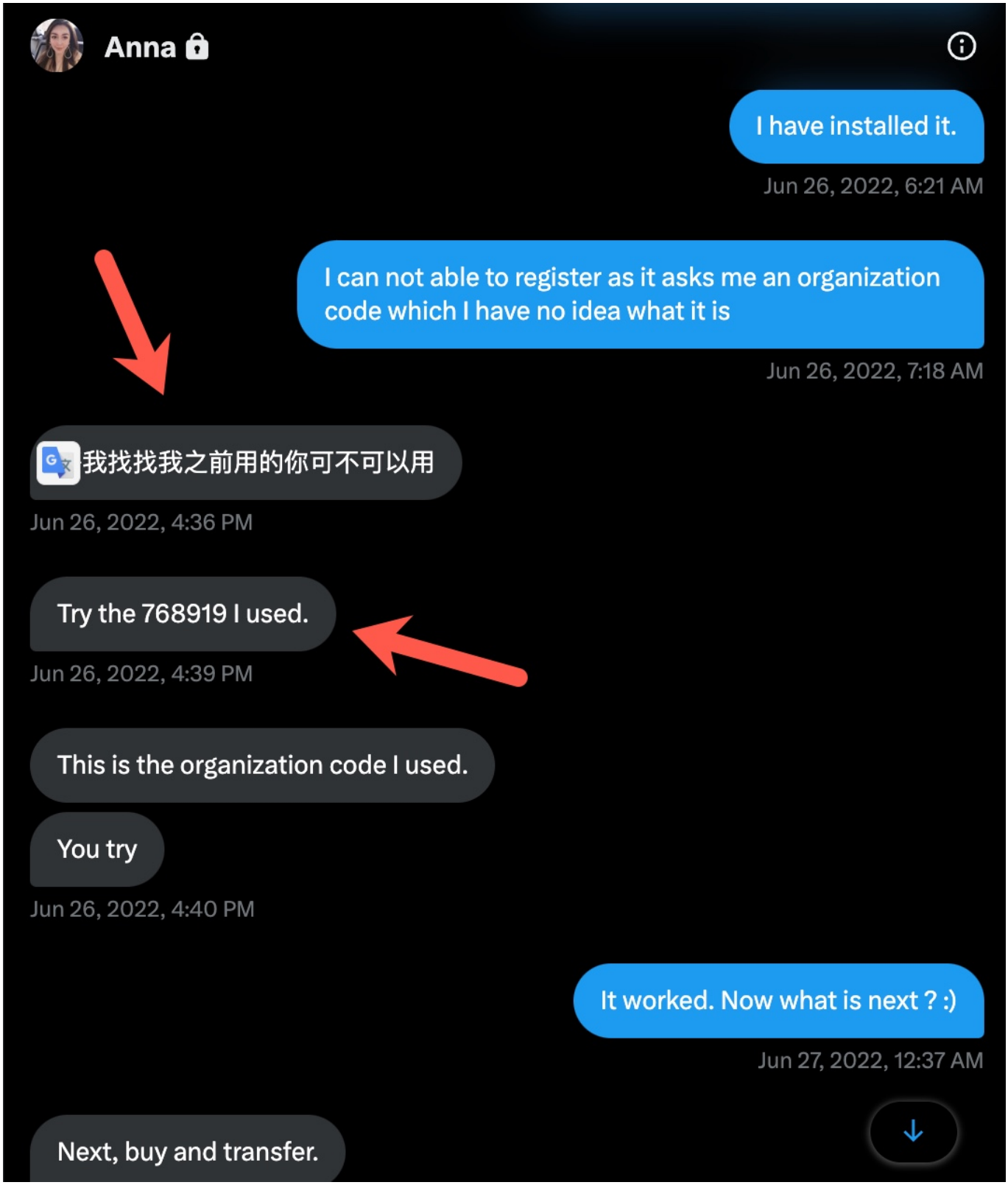


When I tried to register on the website, I was expected to enter an Organization Code in the registration form. The purpose of placing such a code in the form by scammers was probably to prevent cyber security researchers and/or cyber security vendors from detecting this page and collecting information, and they had been successful until now. Whenever I told Anna that I was having issues in the app installation, she kindly did everything she could to help me with screenshots. So I decided to ask Anna for help one more time in finding out the organization code. :)

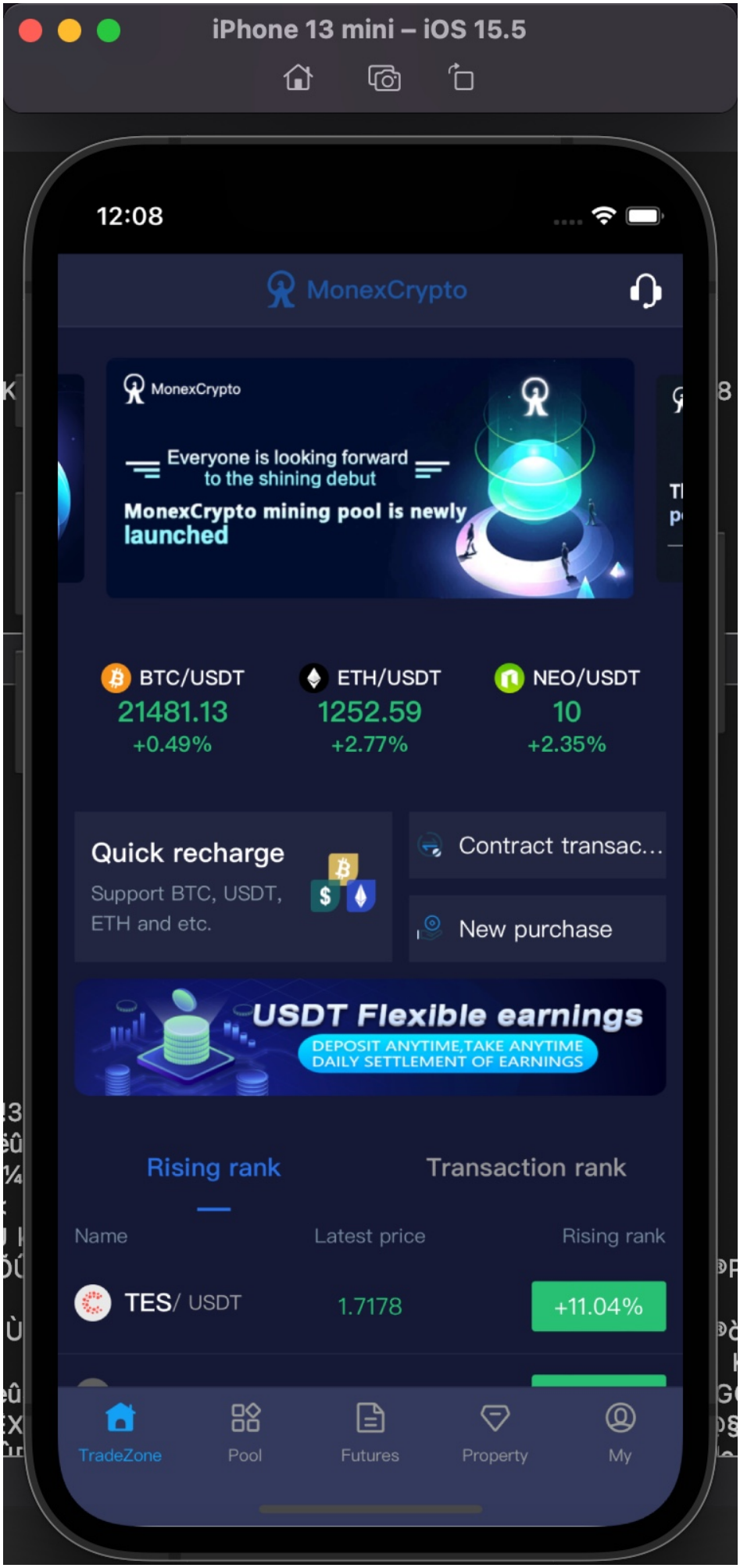


When I asked her the organization code, she first wrote Chinese words (probably she was communicating with me using a Chinese-English translation service), then she shared with me the code (768919) that I needed to enter into the form.

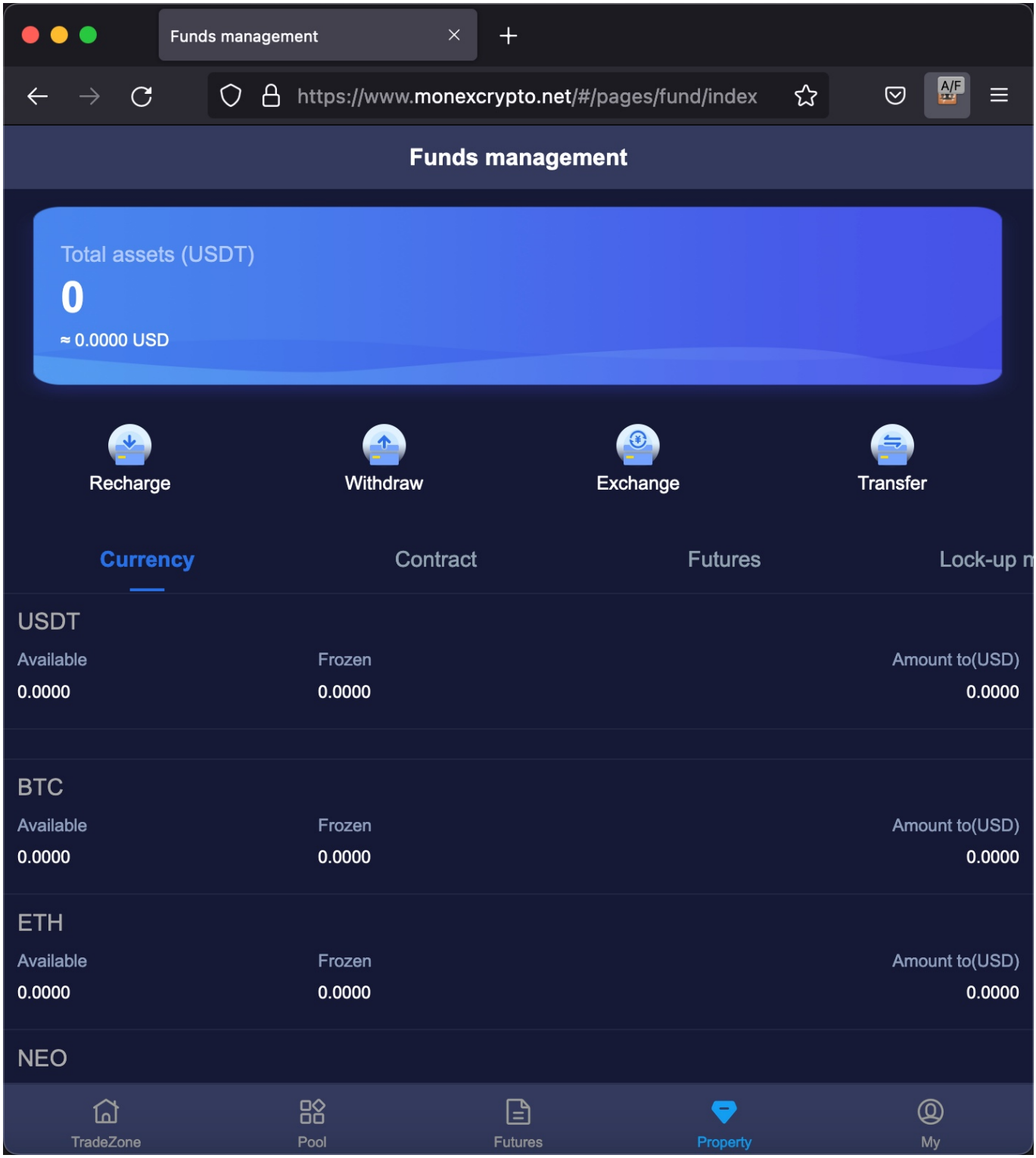

Anna
I can not able to install it to my iPhone, do not know why.
Jun 25, 2022, 2:39 PM
Can be installed
You may not have found the installation package.
5, 2022, 2:43 PM
It will prompt that the description file has been downloaded. After the download is completed, click Settings to see the description file and click Install.
Jun 25, 2022, 2:45 PM
Profile Downloaded
Airplane Mode
Wi-Fi
Not Connected
Bluetooth
On

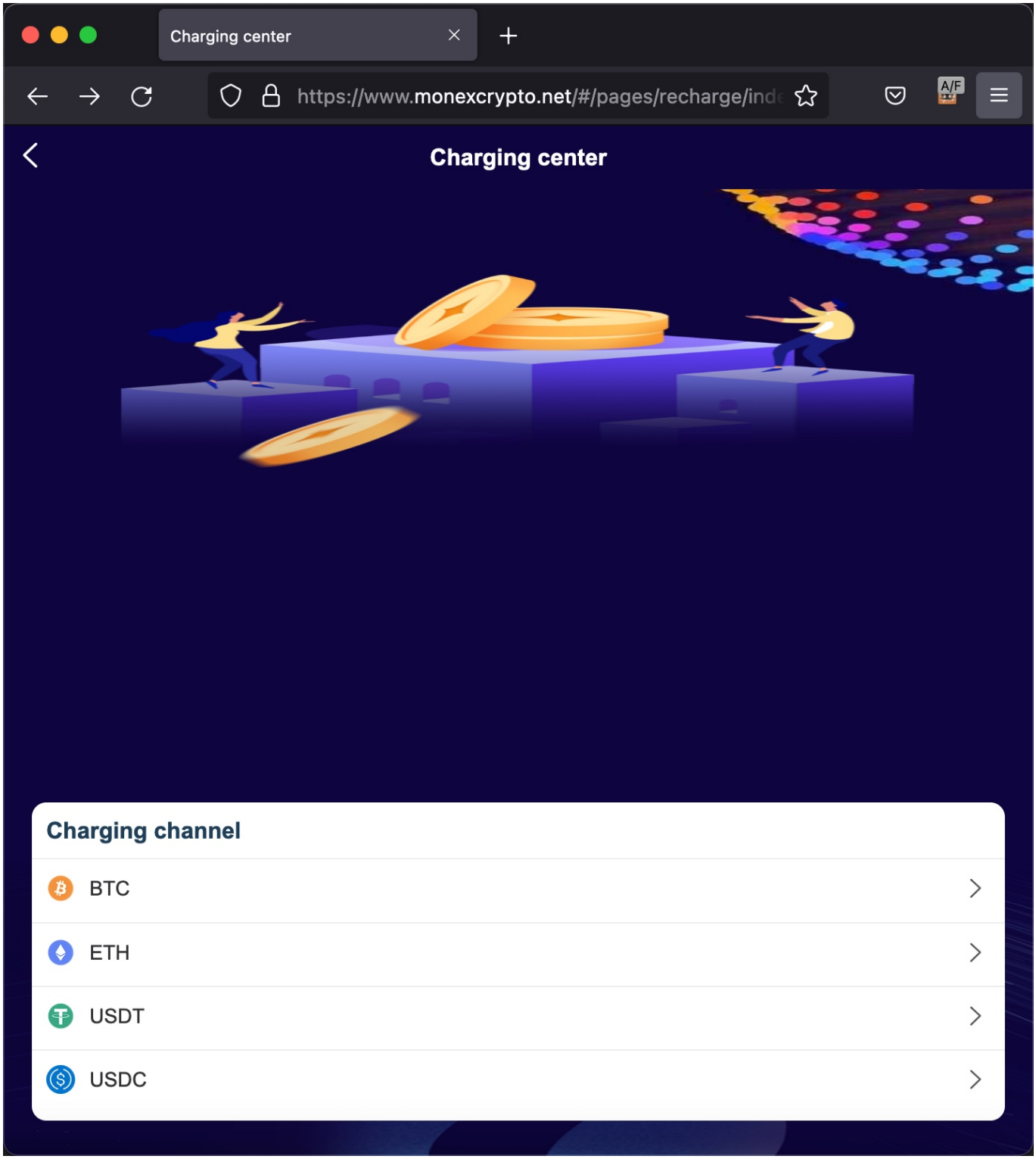

Anna
I have installed it.
Jun 26, 2022, 6:21 AM
I can not able to register as it asks me an organization code which I have no idea what it is
Jun 26, 2022, 7:18 AM
我找找我之前用的你可不可以用
Jun 26, 2022, 4:36 PM
Try the 768919 I used.
Jun 26, 2022, 4:39 PM
This is the organization code I used.
You try
Jun 26, 2022, 4:40 PM
It worked. Now what is next ? :)
Jun 27, 2022, 12:37 AM
Next, buy and transfer.

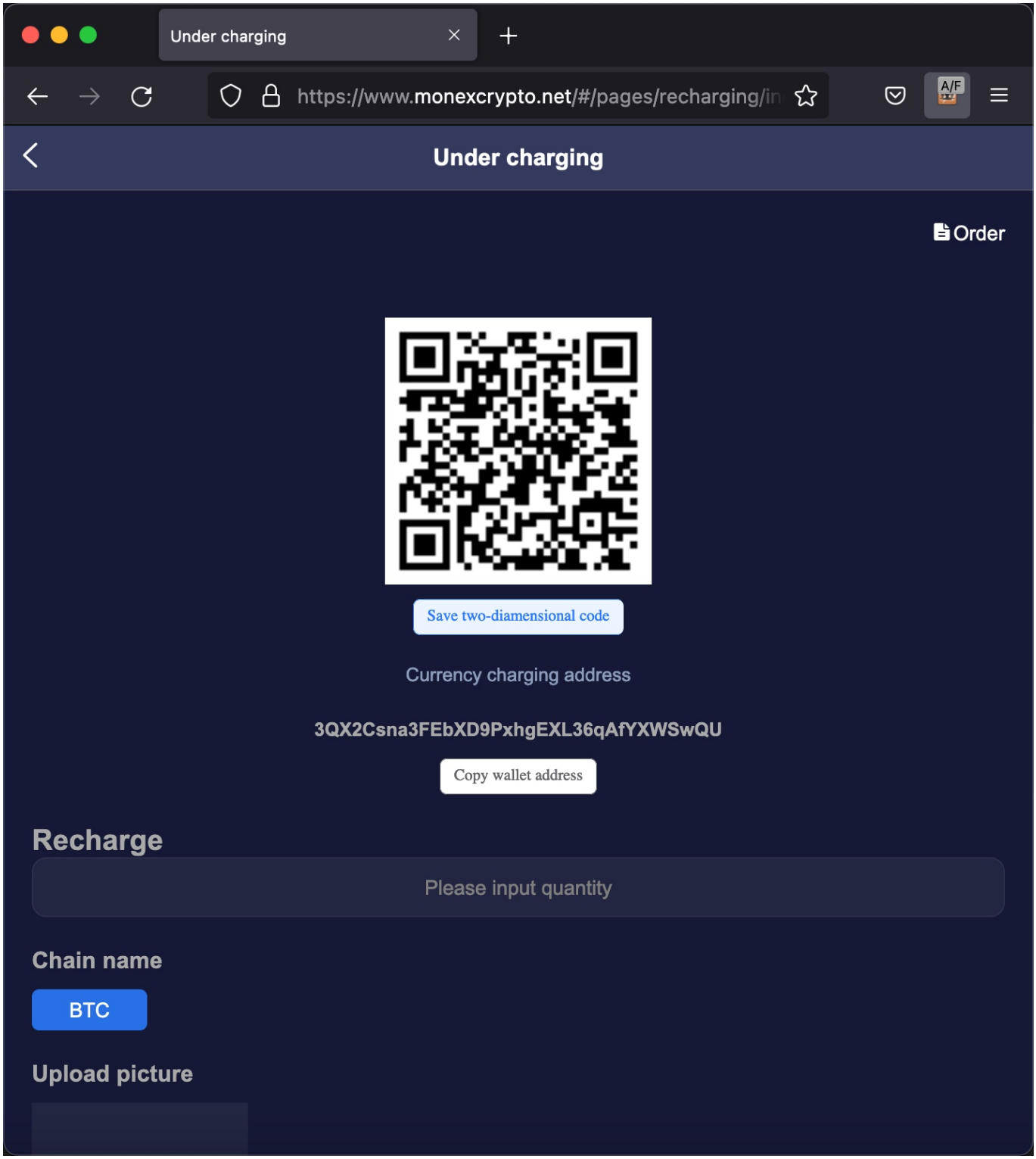
When I successfully registered and started browsing the website with Web Clip, I saw pages and menus about real-time market tracking, depositing money into the wallet, withdrawal, etc.

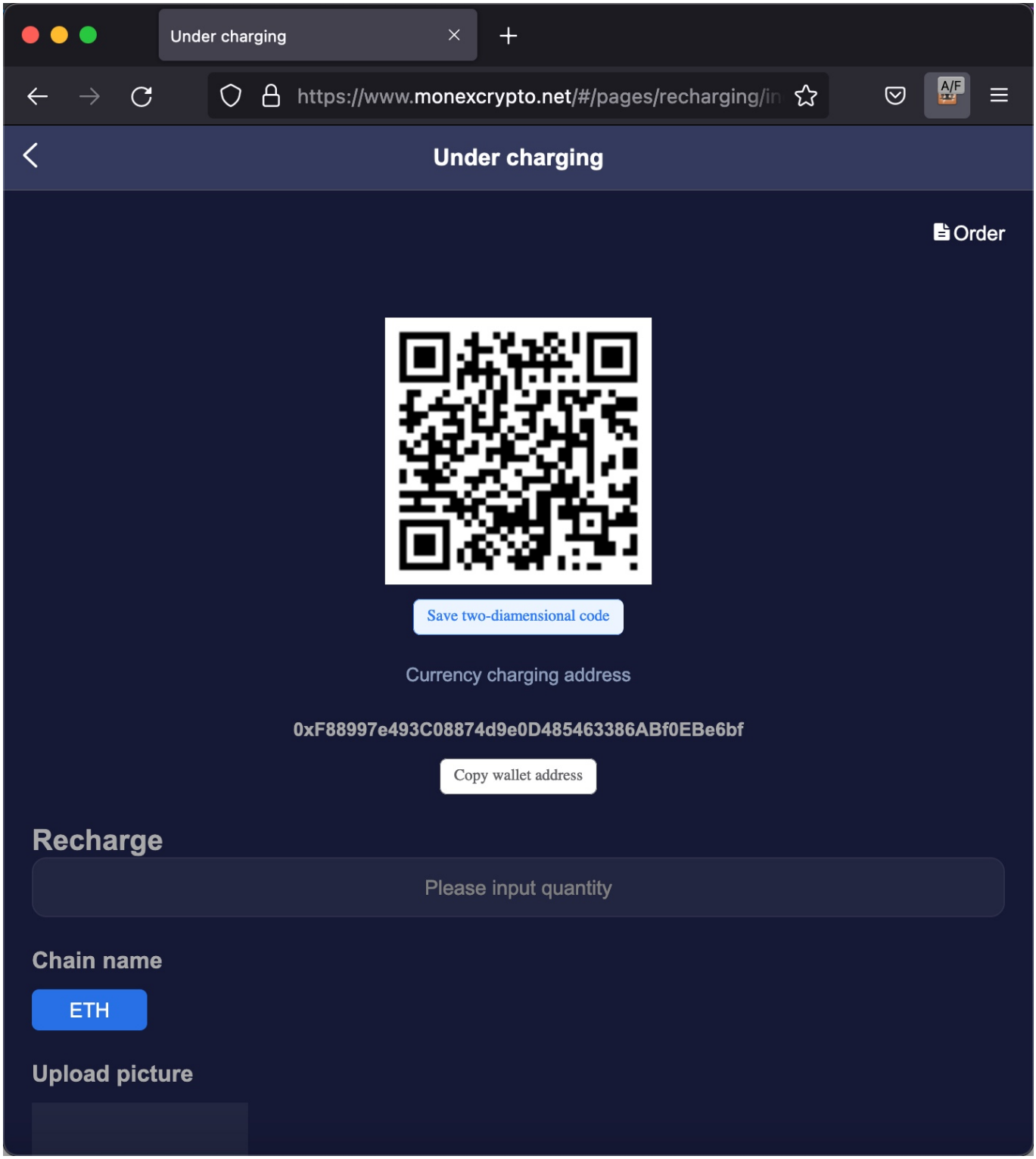

iPhone 13 mini – iOS 15.5
12:08
MonexCrypto
MonexCrypto
Everyone is looking forward to the shining debut
MonexCrypto mining pool is newly launched
BTC/USDT
21481.13
+0.49%
ETH/USDT
1252.59
+2.77%
NEO/USDT
10
+2.35%
Quick recharge
Support BTC, USDT, ETH and etc.
Contract transac...
New purchase
USDT Flexible earnings
DEPOSIT ANYTIME,TAKE ANYTIME
DAILY SETTLEMENT OF EARNINGS
Rising rank
Transaction rank
Name
Latest price
Rising rank
TES/ USDT
1.7178
+11.04%
TradeZone
Pool
Futures
Property
My

Later, I visited the Recharge page, which I thought could be the ideal place for scammers to trap their victims, as the page for depositing and withdrawing cryptocurrency. Like other exchanges and platforms, when I visited, I was presented with the addresses of my cryptocurrency wallets.

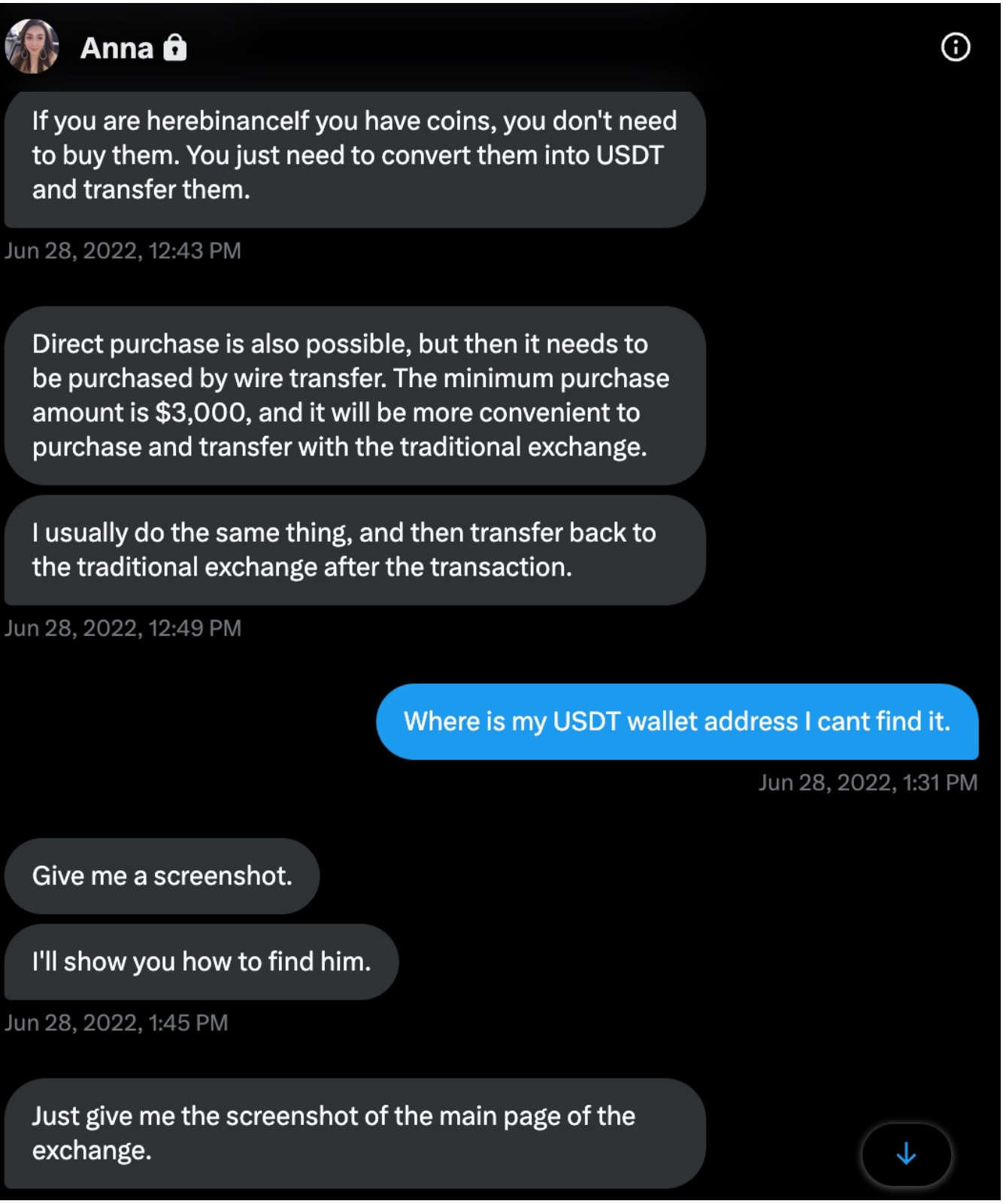



Charging center
https://www.monexcrypto.net/#/pages/recharge/inde
Charging center
Charging channel
BTC
ETH
USDT
USDC


Under charging
https://www.monexcrypto.net/#/pages/recharging/in
Under charging
Order
Save two-diamensional code
Currency charging address
3QX2Csna3FEbXD9PxhgEXL36qAfYXWSwQU
Copy wallet address
Recharge
Please input quantity
Chain name
BTC
Upload picture



On June 28, 2022, Anna realized she was very close to scamming me, began directing me on how to send cryptocurrency (USDT) via a cryptocurrency exchange named Binance to my wallet.

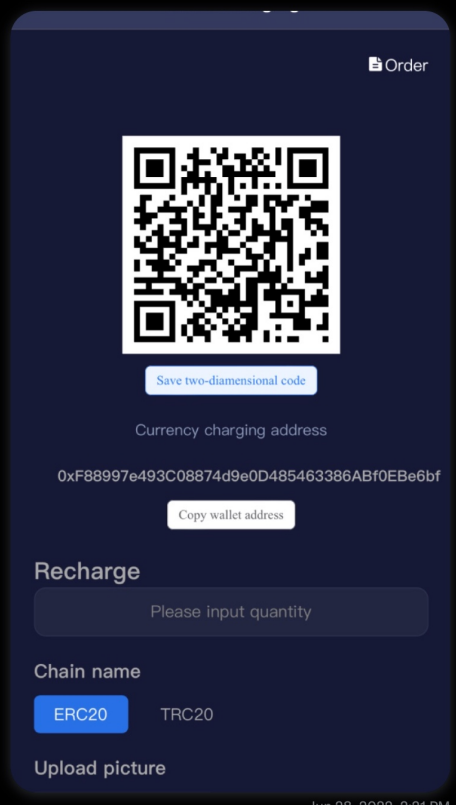

Anna
If you are herebinanceIf you have coins, you don't need to buy them. You just need to convert them into USDT and transfer them.
Jun 28, 2022, 12:43 PM
Direct purchase is also possible, but then it needs to be purchased by wire transfer. The minimum purchase amount is $3,000, and it will be more convenient to purchase and transfer with the traditional exchange.
I usually do the same thing, and then transfer back to the traditional exchange after the transaction.
Jun 28, 2022, 12:49 PM
Where is my USDT wallet address I cant find it.
Jun 28, 2022, 1:31 PM
Give me a screenshot.
I'll show you how to find him.
Jun 28, 2022, 1:45 PM
Just give me the screenshot of the main page of the exchange.

Anna

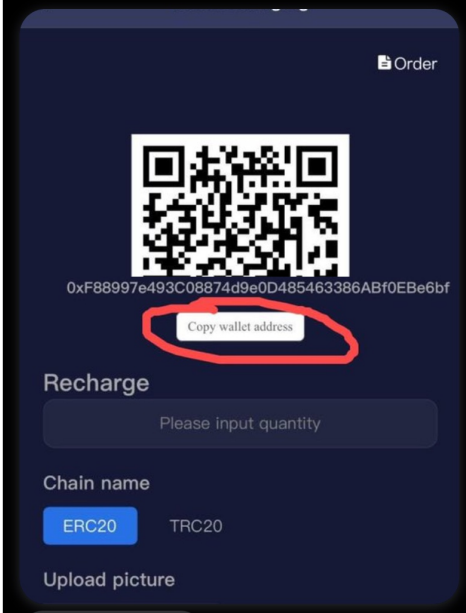
Click on it and give me a screenshot.

I'll teach you the next step

Jun 28, 2022, 2:08 PM



Jun 28, 2022, 2:21 PM



Copy wallet address

Jun 28, 2022, 2:26 PM

Got it.

Jun 28, 2022, 2:27 PM

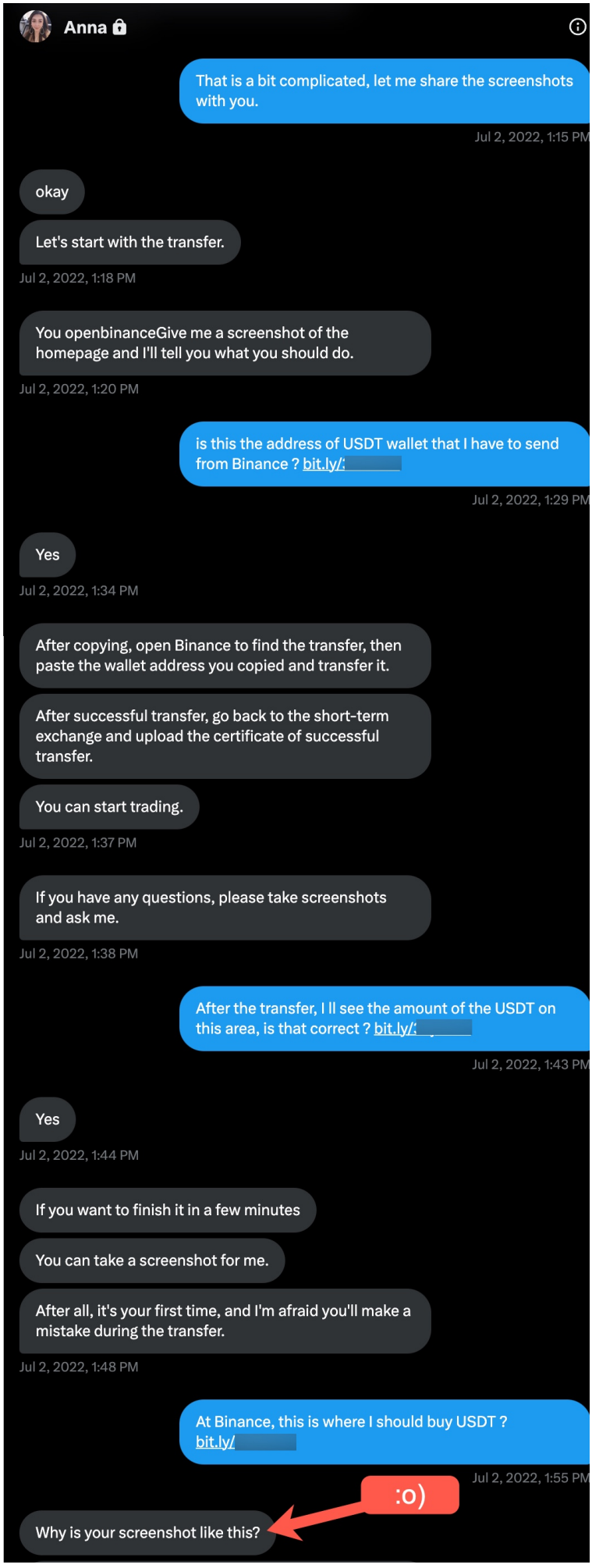
Then open your Binanec screenshot and send it to me,
I will teach you how to transfer the injected funds

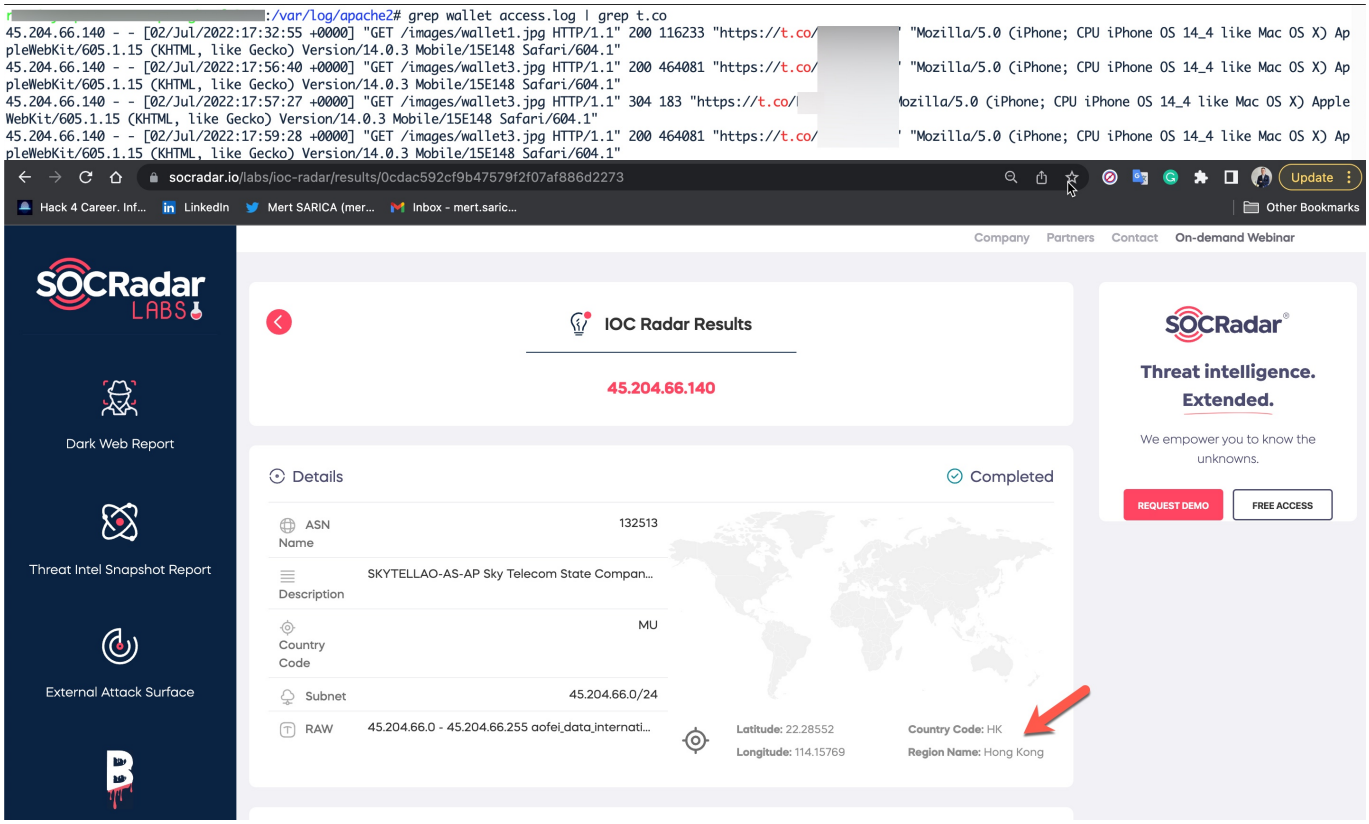
How much money do you plan to start investing?

Jun 28, 2022, 2:29 PM

As I began to wonder which country Anna was really communicating with me from, I started to think about what I could do to find out Anna’s IP address. I guessed that Anna, who had never suspected me despite the éCyber Security Researcher” background image on my Twitter profile, continued to carry on her plan to trap me for 15 days, had no concern about Operations Security (OPSEC). For this reason, I decided to share the web addresses of the screenshots I hosted on my website with Anna by using the Bitly URL shortening service in order to obtain her IP address.

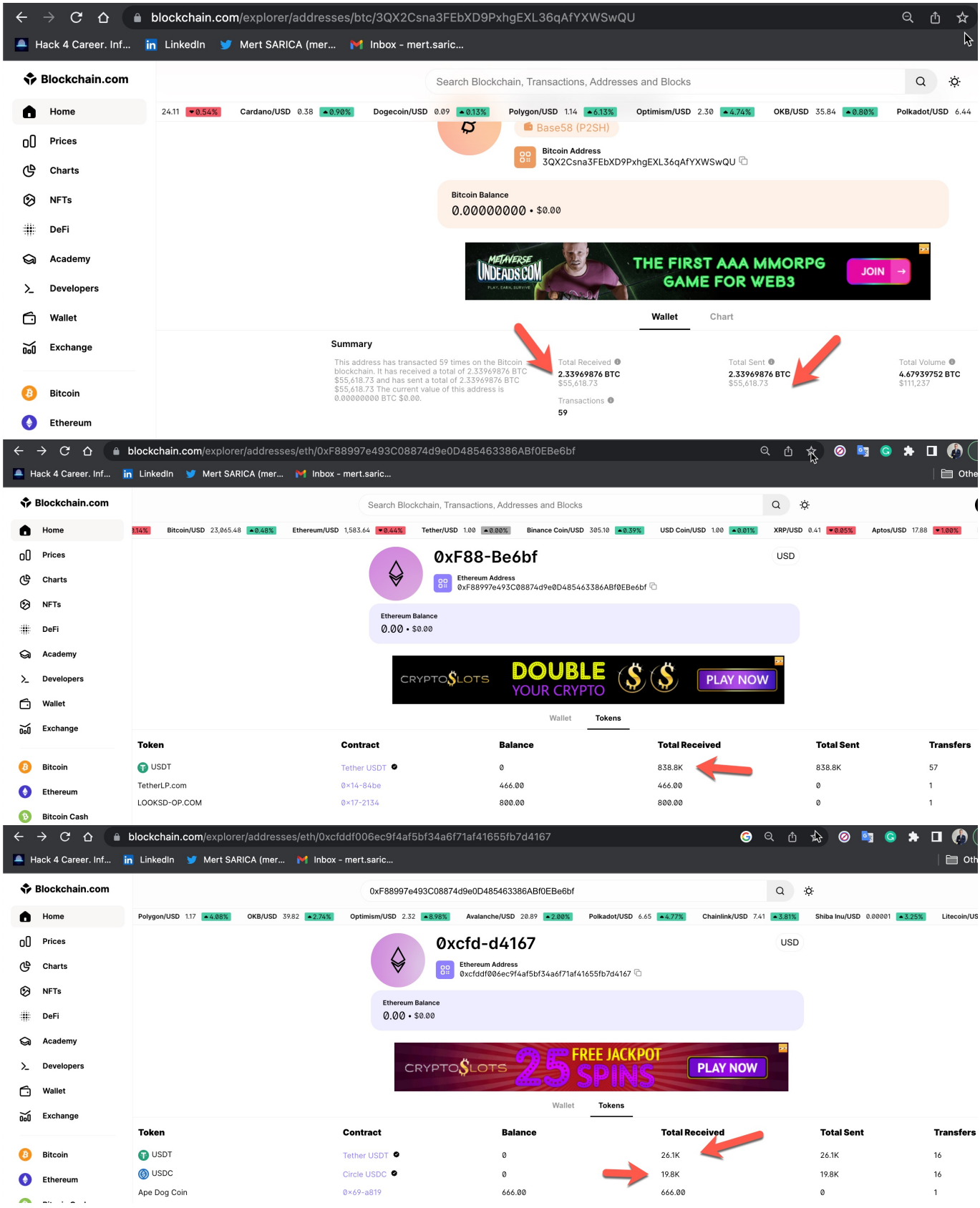
Because Anna did not hesitate to click on the three bit.ly addresses I shared, with the help of the SOCRadar’s IOC Radar I learned that she was communicating with me from the 45.204.66.140 IP address located in Hong Kong.


Anna
That is a bit complicated, let me share the screenshots with you.
Jul 2, 2022, 1:15 PM
okay
Let's start with the transfer.
Jul 2, 2022, 1:18 PM
You openbinanceGive me a screenshot of the homepage and I'll tell you what you should do.
Jul 2, 2022, 1:20 PM
is this the address of USDT wallet that I have to send from Binance ? bit.ly/
Jul 2, 2022, 1:29 PM
Yes
Jul 2, 2022, 1:34 PM
After copying, open Binance to find the transfer, then paste the wallet address you copied and transfer it.
After successful transfer, go back to the short-term exchange and upload the certificate of successful transfer.
You can start trading.
Jul 2, 2022, 1:37 PM
If you have any questions, please take screenshots and ask me.
Jul 2, 2022, 1:38 PM
After the transfer, I ll see the amount of the USDT on this area, is that correct ? bit.ly/
Jul 2, 2022, 1:43 PM
Yes
Jul 2, 2022, 1:44 PM
If you want to finish it in a few minutes
You can take a screenshot for me.
After all, it's your first time, and I'm afraid you'll make a mistake during the transfer.
Jul 2, 2022, 1:48 PM
At Binance, this is where I should buy USDT ? bit.ly/
Jul 2, 2022, 1:55 PM
:o)
Why is your screenshot like this?



As I continued to browse the MonexCrypto website, I decided to check if the Bitcoin and Ethereum cryptocurrency wallet addresses were unique to me or same for everyone who joined the platform. If these wallet addresses belong to scammers and they show their own addresses as wallet addresses to each person who joins the platform (victim), they can easily steal the cryptocurrency from their victims with ease. Based on the research I conducted on this matter, I discovered that;

1. On June 28, 2022, when I checked my Bitcoin wallet address (3QX2Csna3FEbXD9PxhgEXL36qAfYXWSwQU) on the Blockchain.com website, it was seen that this wallet was created on June 6, 2022 and until September 29, 2022, $55,618.73 worth of Bitcoin was transferred to this wallet and then withdrawn.
2. On the same date, when I checked my Ethereum wallet address (0xF88997e493C08874d9e0D485463386ABf0EBe6bf) at the same place, it was seen that this wallet was also created on June 26, 2022 and until November 23, 2022, ~$839.000 worth of Ethereum and USDT was transferred to this wallet.
3. Again, on the same date, this time checking my USDC wallet address (0xcfddf006ec9f4af5bf34a6f71af41655fb7d4167), it was seen that this wallet was created on June 17, 2022 and until August 16, 2022, ~$46.000 worth of Ethereum and USDT was transferred to this wallet.



Disclaimer: I would like to remind that I am not an IRS agent or a Blockchain expert capable of tracing end-to-end cryptocurrency transfers as described in the book Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency in case of any errors. :)

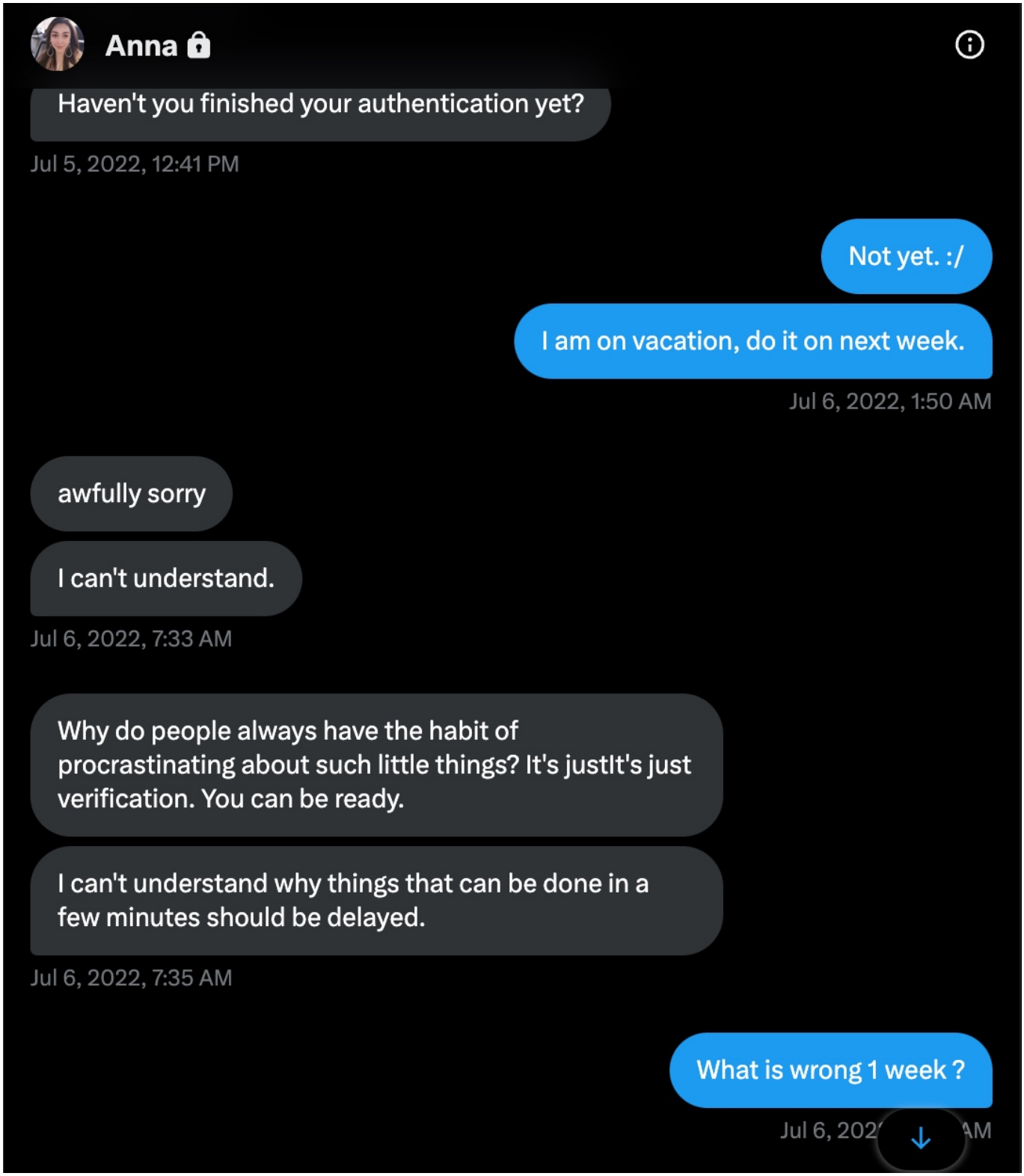
From the date I registered on the MonexCrypto website, June 26, 2022, to January 29, 2023, I roughly checked my wallet addresses 5 times by logging into the MonexCrypto website, and I noticed that they changed every time. Based on this information, the wallet addresses were not individually produced, but were the scammers' own wallet addresses, and they changed these addresses at certain intervals. When I listed and gathered the wallet addresses and the money transfers made to these wallets, I realized that the scammers had stolen approximately 3 million dollars worth of cryptocurrency, to the best of my estimation.

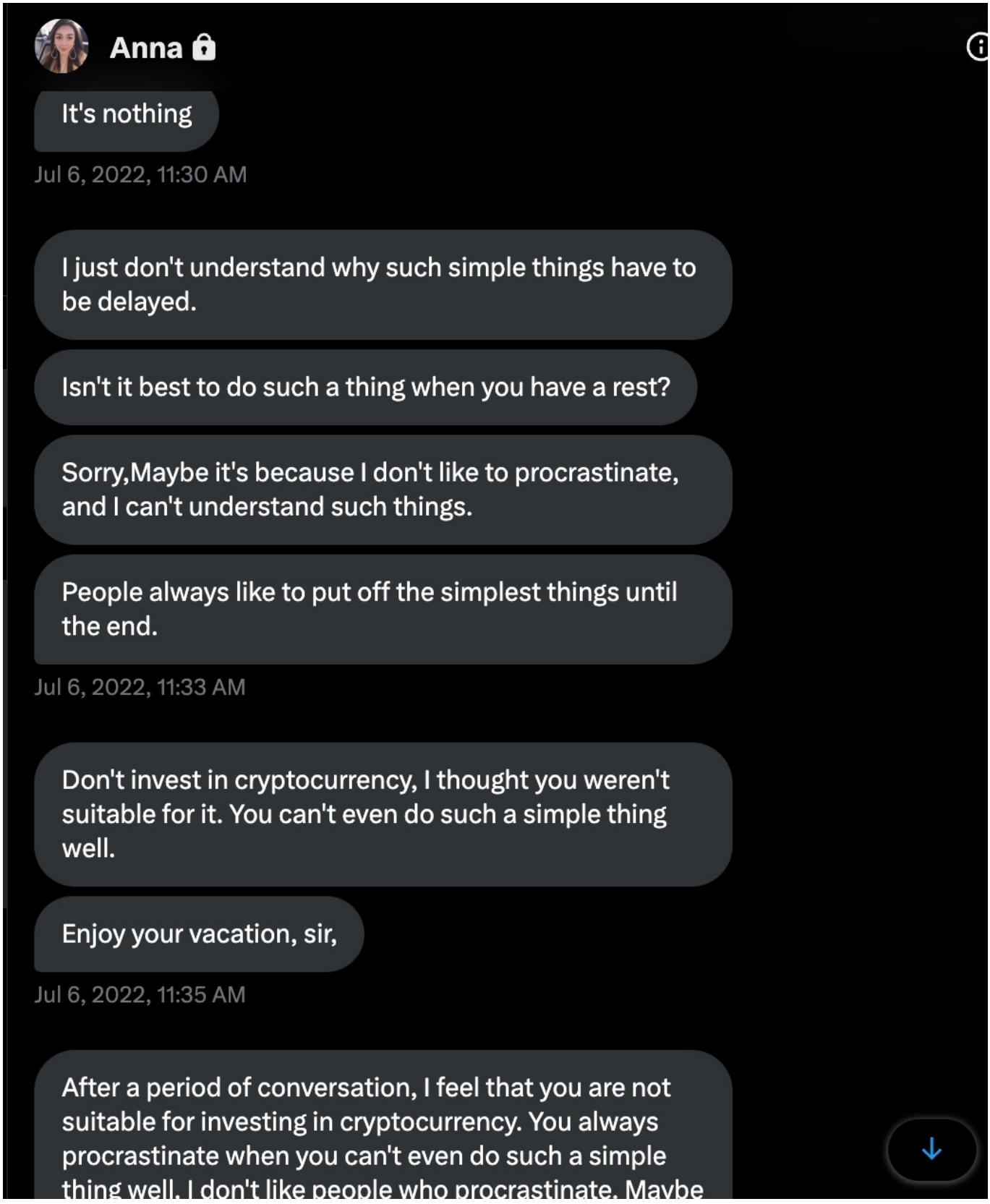
A	B	C
Blockchain Type	**Wallet Address**	**~Stolen Amount (USD)**
Bitcoin	3QX2Csna3FEbXD9PxhgEXL36qAfYXWSwQU	$55,618.73
Ethereum	0xF88997e493C08874d9e0D485463386ABf0EBe6bf	$818,800.00
Ethereum	0xCFDDF006EC9F4AF5BF34A6F71AF41655FB7D4167	$46,000.00
Ethereum	0x392667b0CDf9B04Ce5C48754Ea4185056A65DD31	$246,000.00
Ethereum	0x66FD1C86ae25BDd278bb90f1174f668392EBB540	$675,000.00
Ethereum	0xA9434DFb0fa3f29fc6324AA60DB377C863022f13	$204,000.00
Ethereum	0xC495928233A6E4433c151B7A552e34A3d7Af54D7	$564,000.00
Ethereum	0xaE7A6F74c09BDB3E1e17e51040C070A65ACf7859	$134,000.00
	Total Stolen Amount (USD)	$2,743,418.73

Of course, while I was trying to unmask Anna on July 18th, 2022, the FBI issued a warning against fraudulent attempts made through fake crypto exchanges/investment applications like MonexCrypto. According to this warning, approximately 42.7 million dollars worth of crypto had been stolen from 244 people worldwide. I had already learned how 3 million dollars were stolen. :)

In 2021, the FBI's Internet Crime Complaint Center received more than 4,300 submissions related to pig butchering scams, totaling more than $429 million in losses. And at the end of November, the US Department of Justice announced that it had seized seven domain names used in pig butchering scams in 2022. (Source: Wired)

Anna, who exhausted all means of persuasion to deceive me from June 14th to July 6th, 2022, she started sending messages full of complaints on July 6th. I put an end to our conversation with the bad guy smile by informing Anna of the FBI's warning on August 1st, 2022. :)


Anna
Haven't you finished your authentication yet?
Jul 5, 2022, 12:41 PM
Not yet. :/
I am on vacation, do it on next week.
Jul 6, 2022, 1:50 AM
awfully sorry
I can't understand.
Jul 6, 2022, 7:33 AM
Why do people always have the habit of procrastinating about such little things? It's justIt's just verification. You can be ready.
I can't understand why things that can be done in a few minutes should be delayed.
Jul 6, 2022, 7:35 AM
What is wrong 1 week ?
Jul 6, 202
AM


Anna
It's nothing
Jul 6, 2022, 11:30 AM
I just don't understand why such simple things have to be delayed.
Isn't it best to do such a thing when you have a rest?
Sorry,Maybe it's because I don't like to procrastinate, and I can't understand such things.
People always like to put off the simplest things until the end.
Jul 6, 2022, 11:33 AM
Don't invest in cryptocurrency, I thought you weren't suitable for it. You can't even do such a simple thing well.
Enjoy your vacation, sir,
Jul 6, 2022, 11:35 AM
After a period of conversation, I feel that you are not suitable for investing in cryptocurrency. You always procrastinate when you can't even do such a simple thing well. I don't like people who procrastinate. Maybe

Anna

You can wait until next week. It's your right, but I'm not going to teach you. You didn't cherish it when I gave you the opportunity to learn.

Jul 6, 2022, 11:42 AM

Sorry to hear that

Jul 6, 2022, 2:30 PM

You can study it yourself.

Or find someone else to teach you.

I don't like people who procrastinate, because it is a trivial matter.

Jul 6, 2022, 2:33 PM

I have no reason to wait for you. I have given you many chances.

Jul 6, 2022, 2:49 PM

How do you do ?

Jul 22, 2022, 10:28 AM

hello

What's the matter?

Aug 1, 2022, 11:58 AM

bleepingcomputer.com

FBI warns of fake cryptocurrency apps used to defraud investors

The FBI warned that cybercriminals are creating and u...

Have you read this article ?

Aug 1, 2022, 2:53 PM

What is this?

Aug 8, 2022, 9:10 PM

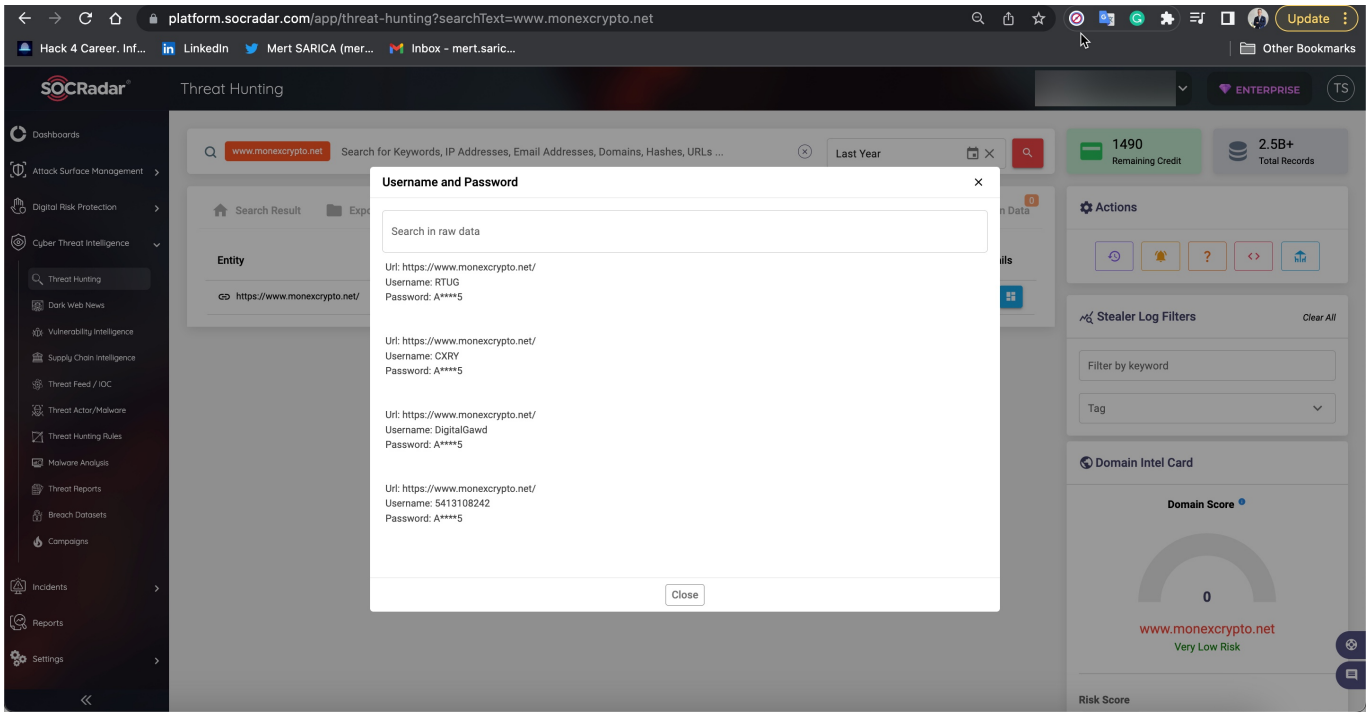
Read and tell me that is it familiar to you ? ;)

Aug 9, 2022, 12:16 AM

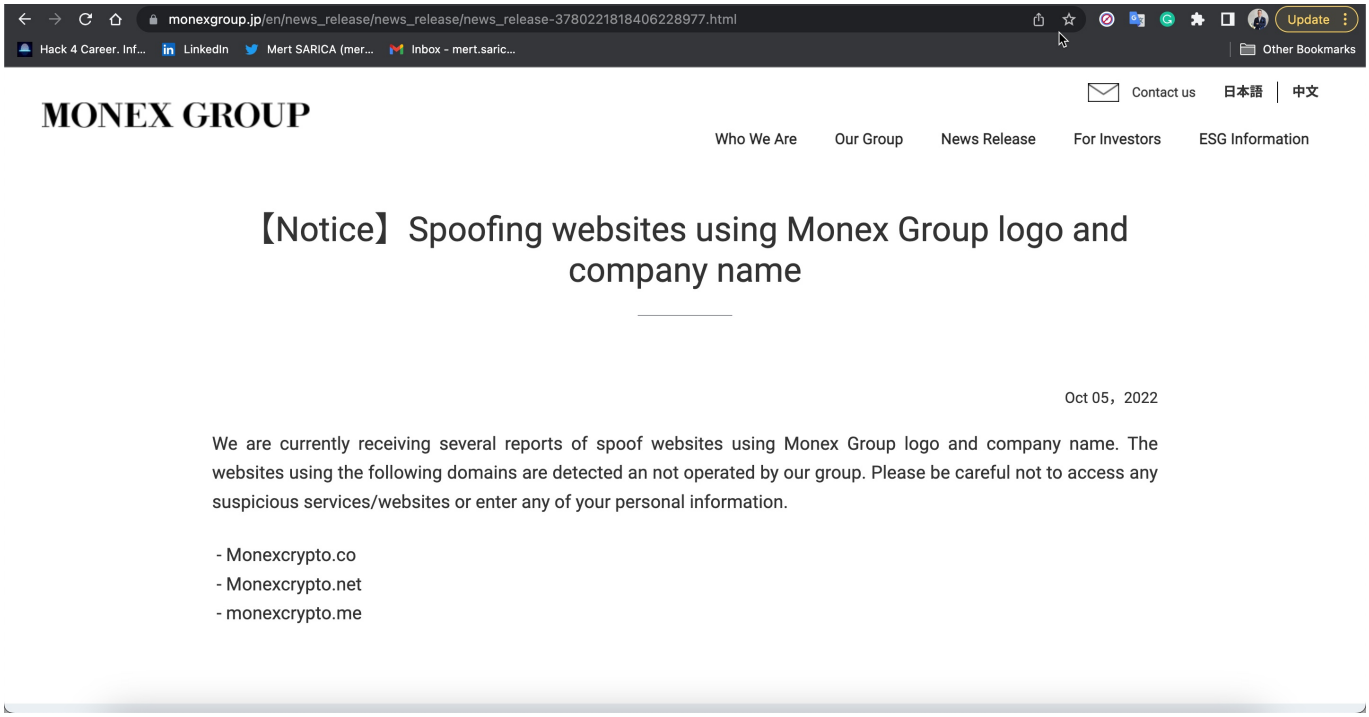
never heard

Aug 9, 2022, 12:41 PM

It seems that Anna continued to catch new victims in her web without slowing down in the following months and was successful, as some user passwords were also stolen when they entered the monexcrypto.net site on September 5th, 2022, according to information detected as stolen by a malicious software (Stealer) on the SOCRadar Cyber Threat Intelligence platform.



By October, the Monex Group issued a warning that two more websites, starting with the monexcrypto.net website, were using the group logos without permission.



As a result, we have learned in detail how Anna and her scammer friends carried out the Pig Butchering Scam, a well-designed fraudulent scheme, and how they made millions of dollars in loot, from the applications downloaded not only from 3rd party websites but also from the Apple App Store and Google Play Store.

Pig Butchering scam is named after the practice of fattening a pig for slaughter. In this case, scammers build a relationship with a victim online before convincing them to send money or invest in high yield crypto-currency accounts.

I strongly request you to share this article with your friends, loved ones to raise security awareness. Hope to see you in the following articles.