Issues in Information Systems
Volume 23, Issue 3, pp. 242-252, 2022

DOI: https://doi.org/10.48009/3_iis_2022_120

Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency

Vasilka Chergarova, *Florida International University, vchergar@fiu.edu*
Vinicius Arcanjo, *Florida International University, vindasil@fiu.edu*
Mel Tomeo, *Miami Dade College, mtomeo@mdc.edu*
Jeronimo Bezerra, *Florida International University, jbezerra@fiu.edu*
Luis Marin Vera, *Florida International University, lmarinve@fiu.edu*
Anthony Uloa, *Florida International University, anulloa@fiu.edu*

Abstract

The interest in cryptocurrency investing is constantly growing. Cryptocurrency may be the currency of the future, but it is also the heaven for con artists to scam investors from their money. Crypto transactions are irreversible. If the underlying blockchain technology has privacy or mixer capabilities it can be virtually untraceable, which creates a new avenue for criminals to scam victims with ease. Social media impersonation is one of the top scams currently performed by criminals. This study presents an example of a social media impersonation scam and the characteristics of the scam. The qualitative data is gathered from communication between the scammer and the potential victim. This study also indicates that cryptocurrency awareness should be included in cyber security training curriculums.

Keywords: Impersonating, Scammer, Crypto Scammer, Social Media Impersonation, Cryptocurrency, Crypto Transactions, Victims of Social Media, Cryptocurrency Fraud, Identity Theft, Fake Profiles

Introduction

Cryptocurrencies use an emerging financial technology based on secure distributed ledgers, also called blockchain (Nakamoto, 2008). Currently, there are a variety of cryptocurrencies on the market. For example, the Decentralized finance (DeFi) system removes the control banks and institutions have on money, financial products, and financial services (Sharma & Chavarria, 2022). DeFi enables users to stake their currency into networks on different exchange platforms and earn profit from the exchange. The user's currency can be locked into smart contracts on the network for which the user receives a periodic interest. Another characteristic of cryptocurrency is that a person can send it as a payment to another person using Peer-to-peer (P2P) financial transactions. The two parties agree to exchange cryptocurrency for goods or services without a third party involved. All it takes to send and receive bitcoin is a wallet address (a string of 26-35 alphanumeric characters). Personal information such as name, address, or any other personally identifiable information is not required. The transaction is irreversible and, in some cases, anonymous, which creates a breeding ground for criminal activities. According to CipherTrace's report in 2018 crypto scam activity resulted in $1.7 billion in investors' losses, $4.5 billion in 2019, and $1.9 billion in 2020 (Barragan, 2021). Another study concluded that about 80% of all Initial coin offering (ICO)s are scams (Dowlat & Hodapp, 2018). There are cryptocurrencies that are legitimate, but there are several that are complete scams. Crypto investors have a hard time being able to distinguish which cryptocurrency is legit and which one is a scam. Scammers are using the anonymous nature of crypto exchange processes and con

investors around the world. Horror stories of people losing their savings, houses, and even their retirement in crypto scam schemas have surfaced in the past several years. Cryptocurrency anonymity also creates a new money laundering problem for banking, law enforcement, and the legal system (Jacquez, 2016). Some networks have a single purpose of scamming people. Criminals are exploiting false advertisements on social media platforms such as Facebook, Twitter, YouTube, and other various schemas to lead investors to fake networks, fake websites, and fake wallets where their funds get stolen.

Literature Review

There are several types of cryptocurrency scams. In several cases, the criminals are combining them for better success. The following literature will provide examples of different types of crypto scams.

Spam Coins occurs when a user buys a spam coin that has no value. In some cases, it could be a malicious contract, meaning the user buys/trades/moves the spam coin from a website which can result in opening a door to allow criminals access to users' wallets.

Scam smart contract happens when the developers deploy an unaudited contract that has pre-approvals from the user's address to transfer funds to another wallet at any time. Rug pull can occur at any time because unsuspicious users can still sell the token. The developers can configure a function in the smart contracts that contain for example a 99% buy/sell fee which will steal all funds when users buy/sell the coin (Zaikin & Vanunu, 2022).

Multi-level marketing (MLM) crypto is a scam with typical characteristics of direct sales in a pyramid scheme. For example, Dr. Ruja Ignatova, a self-described "cryptoqueen", raised billions of dollars from investors between 2014 and 2017 when she disappeared. The Ponzi scheme promoted a fake cryptocurrency known as "OneCoin" and used a pyramided multi-level marketing to target its victims (Kamps, Trozze, & Kleinberg, 2022).

A bridging assets scam occurs when a user connects their wallet to a web app and initiates a transaction. A bridge is a combination of smart contracts that facilitate interoperability and transactions between different blockchains (Dillet, 2022). Hackers exploited a bridge between the Ethereum and Solana blockchains on a popular cryptocurrency platform Wormhole and redirected around $320 million of cryptocurrency to a shady wallet (Dillet, 2022).

Rug pull scam is when the liquidity is pulled out of the market and as a result, users can't sell the coin. Usually, the coin is bought at a very early stage. For example, in the Squid Game token scam, the creators listed only specific addresses that can sell the token. The token had a 45,000% growth, but investors were unable to sell. Another example of a rug pull scam is the DeFi100 coin exit scam, where the criminals stole $32 million of investors' funds. According to the CipherTrace report for the second half of 2020, DeFi rug pull and exit scams made up 99% of all crypto fraud schemes (Barragan, 2021). One of the biggest crypto rug pull scams occurred was the collapse of the centralized finance (CeFi) Turkish cryptocurrency exchange Thodex, which resulted in a $2 billion dollar theft in 2021 (Scharfman, 2022).

Malicious cryptocurrency website scams occur when a copy of a real website is duplicated for the purposes of capturing users' passwords and private information. These fake websites have a very similar URL and design appeal. In some cases, the user is redirected to a fake tech support website by a direct call from the scammers where the personal information is stolen under the pretext of a technical issue.

Subscriber Identity Module (SIM) swap scam, also called a port-out scam, happens when a user's personal information has been collected from multiple sources and it is used for an illegal acquisition of the user's wireless phone number and data. By using social engineering, the scammer pretends that the phone is lost or stolen and uses the leaked information to convince the phone company to set up a new phone. Once the phone has been restored to a new device, the scammers have access to all of the user's information, such as the victim's bank account, crypto wallet, two-factor authentication software, and verification text messages (Andrews, 2018). In some cases, SIM numbers are changed directly by telecom company employees bribed by criminals (Franceschi-Bicchierai, 2019).

Fake customers support scams occur using social media to steal a user's seed phrase and empty his/her crypto wallet. A seed phrase is a client-generated sequence of English words (Dowlat & Hodapp, 2018), which serves as a recovery phrase generated by the cryptocurrency wallet that gives access to the cryptocurrency associated with that wallet. A crypto wallet is a password manager for cryptocurrency and the master password is the seed phrase. In this type of scam, a user is redirected to a website where the seed phrase would be stolen, or a user is asked to send funds directly as a test to a shady account. Often a remote access to the user's personal computer or live stream tech support is requested for direct help.

Free crypto scams occur when a social media account is hacked or replicated to resemble the real person and a message is posted that if a certain amount is sent to the advertised crypto account the user will double or triple the initial investment. The victims are redirected to a scam website through an advertisement on a hacked/impersonated social media account. An example of such a scam, is when a copy of a Twitter account of a well-known individual (e.g., Elon Musk, Barack Obama) offeres free cryptocurrency (Phillips & Wilder, 2020). One study showed over 15,000 Twitter accounts promoting cryptocurrency scams (Wright & Anise, 2018).

Dating crypto scams occur on online dating sites where imposters persuade people into false crypto investments in the name of love (Miranda, 2021). In most cases, the scams have characteristics of a vector attack, and the victim never receives their money back.

Methodology

This paper aims to provide an understanding of an individual characteristics on social media who is an imposter that is persuading people into investing in a cryptocurrency scam. The data was analyzed and gathered from a mobile device. The data was collected during the month of November and December in 2021 from text messages on a mobile device. The data was exported and submitted to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) and the Federal Trade Commission (FTC Report Number 142485043) fraud detection web page. No funds were invested during this research in any of the below-mentioned websites and crypto wallets. The sole purpose of the engagement was to research the characteristics and the nature of the scam. The methodology includes identifying the scam, creating a model of the scam, and analyzing the data for common trends.

Identifying the scam

The imposters pretended to be a YouTube influencer by creating a fake profile with the same image as the real person. In general, the fake profile advertises advising through an untraceable phone number or number from foreign country. The scammer has created a fake YouTube account by using an influencer picture to impersonate his followers and to interact with them. The scammer used 1(802)772 0076 phone number pretending to be a YouTube crypto influencer and then gave instructions to the victim to set up an account, a crypto wallet, and how to deposit money. Next, new instructions were given to the victim to have them

transfer money to a one-stop-shop website (https://racepointfx.net/). The website contained multiple directions for investments (e.g., renewable energy, cryptocurrency investment, property management, forex trading, marijuana stocks, and retirement planning). According to this website, Racepointfx Trade has its office in partnership at Charleston, South Carolina, United States. The website is still functional at the time of the writing of this paper (IP address 66.29.146.12). The ICANN registered contact information contained the phone number +354 4212434 and the mailing address was Kalkofnsvegur 2, Reykjavik, Capital Region, 101, Island. Further research on the phone number revealed multiple online scam complaints. About 104 users reported online that this phone number is scam related.

Name of the company	Website domain
Deesse Exchange	deesseexchange.com
Blocked	warlightbravestone.com
Blocked	Monkeyvacation.com
Financeinvesting SanakoService Ltd	Finvestings.com
Pretending to be the UK post	oversightus.com
Blocked	oversightxyz.com
no info	theelitemale.com
Blocked	countpalatine.com
no info	walmartify.com
no info	spellmanrhodes.com
no info	simpfxp.com
Global Shipping Express- Free pet delivery	globalsshippingexpress.com
Reported scam page	geniuskiddie.com
Fake bank on the Philippines	n/a
RSM Logistics	rsmlogistics.org
Blocked	casperspins.com
Fake webull.com	wap.webullxap.com
Fake fdplatinum.com	fdpllatinum.com
Nigerian investing	abeginvest.com
Bitcoin Investment site	skylineglobalInvestment.com
Blocked	avasquare.com
Bitcoin trading and mining scam	appextraders.net
Crypto trading	bitpolon.com
Blocked	tickmilsfx.com
Blocked Drain Wallet	mywalletsdapps.com

Figure 1. Reported victims (n=104) (https://spamcalls.net/en/number/3544212434#61645081e20d77)

During the study, several calls were also recorded. The scammers had a foreign accent and occasionally hung the phone up unexpectedly. After extrapolating enough data, the research team confronted the scammers which made them flip their tactic. The victim was informed that the website for the final transfer was a scam, and they are helping the victim to get the funds out. During all correspondence, the victim was demanded to provide a screenshot of the actions taken.

Creating a model of the scam

Based on the collected data, a scammer's persuasive techniques workflow model was created (Figure2).

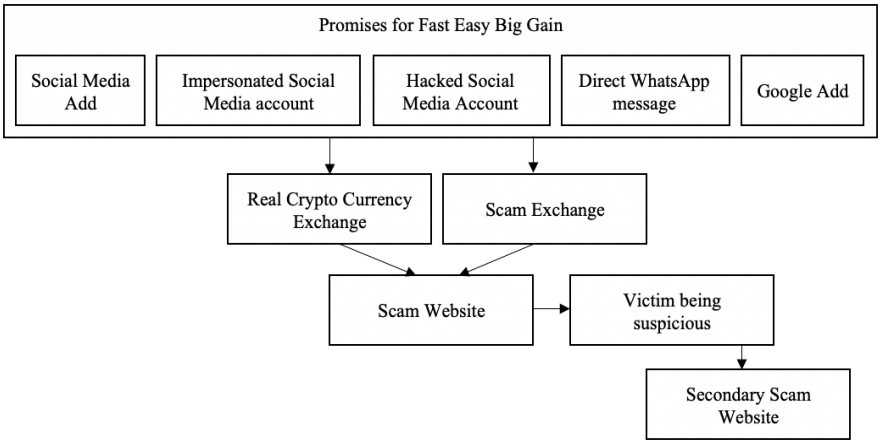

Figure 2 Scammers' persuasive techniques workflow model

First, the scammers used several channels to attract victims: social media ads (e.g., Facebook, YouTube, Twitter, LinkedIn), Google advertisements, impersonated social media accounts, hacked social media accounts, and direct messages on messengers (e.g., WhatsApp, Facebook messenger, Telegram, Signal). Next, the victim is redirected to buy bitcoin on a real or a "shady" cryptocurrency exchange. After the bitcoin is bought, the victim is guided to transfer it to a scam website or purchase another currency. The victim is promised a significant fast return on investment. If the victim becomes suspicious, then they are redirected to a secondary scam website or currency under the pretext that they are being helped.

Data Analysis

After the data was exported into a text format (Appendix A), several trends triggering the common red flag were identified. At the beginning of the correspondence, the scammers were very friendly and sociable but then started to move faster, creating a sense of urgency and fear of missing out on an investment opportunity. The scammer slowly tried to create pressure on the victim and started demanding screenshots as proof of a completed money transaction to the suspicious website. Several characteristics of the scammer were found, such as bad spelling, a sense of urgency, compliments and flirting, guilt, constant request for screenshots, pressure, and the double-dip strategy. More details related to the criminal characteristics are provided below.

Bad spelling

Bad spelling and the use of uncommon words in the data were in accordance with previous studies or scam cases. A common characteristic that is related to scams is the use of odd language, wording of the text that doesn't sound right, bad spelling, and grammar (Datar, Cole, & Rogers, 2014; Scharfman, 2022).

The sense of urgency

The goal of the scammers was to create a feeling of fear of missing out on an investment opportunity. Previous studies showed that scammers used triggers that were employed to make potential victims focus on huge prizes or benefits and imagined a positive future emotional state (Lea, Fischer, & Evans, 2009).

Compliments and Flirting

Compliments and flirting are generally more common in a romance scam, however, the data showed traces of compliments. The criminals groomed the victim prior to any financial request and tried to keep the victim believing that the criminal was interested in pursuing a relationship and not money. In such cases, the fraud ends only when the victim learns and accepts that they have been scammed and have stopped giving more funds (Whitty, 2013).

Guilt

When confronted with the truth, the scammers tried to make the victim feel guilty. The victim was accused of being ungrateful for the "help" provided by the scammer.

Constant request for screenshots

The scammers constantly requested screenshots under the pretext that it was helping them with the process. In general, scammers were particularly interested in any inside information of the victim's crypto security information. Their style of operation was similar to many common con artists. Once the hackers obtained

this information, they would have been able to steal the cryptocurrency stored in the victim's wallets (Priya, Ammal, & Khan, 2022).

Pressure

Pressure of transferring the funds was applied as often as possible. The end goal of the scammers was to extract as much funds as possible.

Double Dip Strategy

The data also revealed the use of the double-dip strategy. When the victim exposed the scam, the criminals started turning the game and pretending that they were helping or protecting the victim from a bad investment and redirecting to another scam coin or another scam website. In some cases, the scammers also targeted previous victims with the pretext that they would recover the losses or present a new investment opportunity. The second scam call could come from a new company offering a new service or a product and, in some cases, scammers could pretend to call from law enforcement or other types of authorities.

Discussion and Limitations

The scams and the Ponzi schemes are not new inventions. They have been executed around the world for over hundreds of years. The cryptocurrency scams are following the same road, but scammers are exploiting the anonymity of new cryptocurrency exchange technology. The scam is usually initiated with buying a list of customers' private information on the dark web or using call centers to scam. In this study, the scam was initiated by impersonating a social media account. The characteristics extrapolated from the data include bad spelling, the sense of urgency, compliment, guilt pressure, constant request for device access/screenshot, pressure, and the double dip strategy.

The social media platform where the scam for this study originated took no action whatsoever. Currently, marking an advertisement post as spam on Facebook will not remove it from the platform. Marking the impersonator's profile on YouTube will not remove a scammer profile either. After the famous scam case with Elon Musk's Twitter account, Twitter did become more vigilant of scams on its platform, however, this did not stop scammers from finding new avenues for advertising their phony services. The scammers are constantly sending new text messages using platforms such as WhatsApp, Facebook messenger, LinkedIn messenger, Telegram, and Signal. In some cases, individuals have received a direct phone call. Regulators could not track fast enough the source of the scam, because it can be originated from anywhere in the world. In the new crypto economy, crime control is mostly absent and full of scam (Mackenzie, 2022).

This study has its limitations. Although most of the common schemas are presented in the literature review, this study encompasses a single use case. Further research is needed to discover more common trends and their mitigation strategies. Another limitation in this study, was that the researchers used simple tools to trace the website hosting location. More sophisticated network forensic tools could be used to detect the origin and the physical location of the servers hosting the fraudulent websites.

Conclusion and Future Recommendations

It's an undeniable truth that the crypto world has become a breeding ground for scams because of how con artists have been allured by the prospect of anonymity once their crimes are complete. Social media platforms with Inadequate security are an easy target for an audacious security breach that puts consumer

funds at risk. Scammers can set up their own platform and their own websites with promising big returns and disappear with the capital once the account has reached enough investments. A naïve crypto enthusiast can lose their money in "shady" exchanges that offer enormous interest rates and an impossible withdrawal schema (Blenkinsop, 2019). According to the FTC data, since October 2020, about 7,000 people have reported losses to cryptocurrency investments scams, resulting in more than $80 million. One study showed that people ages 20-49 were five times more likely to report losing money on these scams. Cryptocurrency is more understood by the younger generation. While Cryptocurrency is understood better by the younger generation, more money has been lost on investment scams than on any other type of fraud by individuals between the age 20-30 years old. About $35 million or more than half of their reported investment scam losses were in cryptocurrency (Miranda, 2021).

A recommendation would be to include a scam prevention training for students. Recommendation for the following steps to be included in such a training are as follow: 1) Research the crypto exchange, website, and company before investing along with online information for the company and cryptocurrency name, plus "review," "scam," or "complaint", 2) Stay away from guarantees and big promises. Scammers often promise quick money, big payouts, guaranteed returns, and promised Annual percentage rate (APR) gain, 3) Stay away from offers of free money paid in cash or cryptocurrency, 4) Stay away from celebrity endorsement and never share your seed phrase with anyone, 5) Don't trust people who say they know a better and a faster way to multiply the investment, and 6) Requests for payment in cryptocurrency or gift cards are scams (Miranda, 2021). In case an individual falls victim to a cryptocurrency scam, they should follow the FTC advise and report the fraud and other suspicious activity involving cryptocurrency to the following agencies: FTC, Commodity Futures Trading Commission (CFTC), U.S. Securities and Exchange Commission (SEC), Internet Crime Complaint Center (IC3), and the cryptocurrency exchange company that was used.

References

Andrews, N. (2018). Can I Get Your Digits: Illegal Acquisition of Wireless Phone Numbers for SIM-Swap Attacks and Wireless Provider Liability. *Northwestern Journal of Technology and Intellectual Property, 16*, 79.

Barragan, J. (2021). Cryptocurrency Crime and Anti-Money Laundering Report, February 2021. *CipherTrace Cryptocurrency Intelligence*.

Blenkinsop, C. (2019). Crypto Scams: The Effect on Consumers and Legitimate Businesses. *Cointelegraph*.

Datar, T. D., Cole, K. A., & Rogers, M. K. (2014). Awareness of scam e-mails: an exploratory research study.

Dillet, R. (2022). Blockchain bridge Wormhole confirms that exploiter stole $320 million worth of crypto assets. *TechCrunch*.

Dowlat, S., & Hodapp, M. (2018). Cryptoasset market coverage initiation: network creation. *Satis Group (Satis Group)*.

Franceschi-Bicchierai, L. (2019). AT&T Contractors and a Verizon Employee Charged with Helping SIM Swapping Criminal Ring. *Vice*.

Jacquez, T. (2016). *Cryptocurrency the new money laundering problem for banking, law enforcement, and the legal system.* Utica College

Kamps, J., Trozze, A., & Kleinberg, B. (2022). Cryptocurrencies: Boons and curses for fraud prevention. In *A Fresh Look at Fraud* (pp. 192-219): Routledge.

Lea, S., Fischer, P., & Evans, K. (2009). The economic psychology of scams. *International Association for Research in Economic Psychology and the Society for the Advancement of Behavioral Economics, Nova Scotia, Canada*.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*.

Miranda, C. (2021). Spotting cryptocurrency investment scams. *Federal Trade Commission Consumer Advice*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Phillips, R., & Wilder, H. (2020). *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites.* Paper presented at the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

Priya, C. R., Ammal, K. A., & Khan, M. J. A. (2022). Cryptocurrency-An Expository Review. *Recent Developments in Business and Management*, 6.

Scharfman, J. (2022). Cryptocurrency Compliance and Operations Case Studies. In *Cryptocurrency Compliance and Operations* (pp. 155-170): Springer.

Sharma, R., & Chavarria, A. (2022). Decentralized Finance (DeFi) Definition. *Investopedia*.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665-684.

Wright, J., & Anise, O. (2018). Don't@ me: Hunting twitter bots at scale. *Blackhat USA*.

Zaikin, D. B. R., & Vanunu, O. (2022). Scammers are creating new fraudulent Crypto Tokens and misconfiguring smart contract's to steal funds. *Check Point Research*.

Appendix A. Exported data

Data from scammers is in black and data from research team is in gray

Oh..Hey! Glad to have you here..

Hey

Sorry miss the call

How is life

Pretty Great! Thanks for asking BTW..

What do I owe your esteemed DM..?

What is DM?

Direct Message..? Lol

I like the way you think

U look good with beard

So nice! Thanks tho

So tell me, are you into crypto as well..or its just my beard..? Lol(no offense tho)

Both □

Like the beard try to learn about crypto
Very good job explaining AI too
And honesty
Honesty is very much appreciated among all the pockerfaces online
And the beard ofcourse □

□□

what exactly do you think is the right strategy for your better experience investing crypto..?

Very simple: Invest early when low, invest as much as you can lose and won't hurt you, sell before go down
I m a beginner amateur

Absolutely! As we proceed through getting you started..you'll need your personal crypto wallet(to store your digital assets)

Recommendations? I m trying to verify on binance and it is such a pain in the neck
Coinbase doesn't give access to all

Okay..visit www.gemini.com to get your personal wallet, get back to me so we can proceed

Got it
Should I register as US or as EU?

US..for sure! Pretty much your location.

Got it

Send across screenshots to help you while we navigate through the process..
Proceed to Funding it..

I'm in
Do you trust this app?

Absolutely!

□□

Toss $5k into your wallet...pretty smart to start with small accounts to be safe!
I get so busy with my new inventions and tons of messages coming in..but I try to keep up! though sometimes later□.. got like and hour before I get back to other things..cease the moment!

When do you relax and have a break?
Don't burn out
Ooo and thank you too

Okay..with $1k at least, I can navigate you through starting something profitable in crypto.. run up your funds so we can proceed.

It doesn't want to add it

You mean Gemini..?
Doesn't want to add your fund..?

Yup
I ll try tomorrow again

Just use www.crypto.com instead! I use it too

Get www.crypto.com

Run up your funds and tomorrow when you wake up, we proceed,alright?

□□

Pretty easy start up procedures.. you'll like crypto investment better by the time you start making so much money from it... Are you registered?

Yes

Is it funded yet..?

No it doesn't work

What's your hindrance?
Let me see a screenshot of what you see on crypto.com..?
The server is pretty messed up..

I see
Where is the server?

Got like multiple calls coming in at the same time..□
Tf Im in NY! □..where else can I be?

Texas?

What your hindrance funding your wallet..? Try not to get distracted by my billionaire hot body..

Lol
I'll try

We'll catch up on our chit-chat later..okay? I'll call you when it's okay for me..

Ok

Let's get you started first..
You've got pretty nice voice BTW□..

□□

How's it going?

I'll try again tomorrow
It doesn't work

Contact support tomorrow and try to get it funded..hit me up immediately after it's done..so we can proceed with what's next.

I will
What will be next?

Have a sweet night dream,Huni□□□.. It's a step by step procedure,pretty much learn and understand better as you proceed through.

Thank you for helping me
Hi
I was able to add 1500
*A***, what is the next step?*

Okay! Which of the tokens did you buy?

Crypto.com..right?
http://Racepointfx.net
Get registered and get back to me..so we can proceed!

Gemini
But why register to second website
Which coin should I buy

http://Racepointfx.net
Is the contracting company platform that trades up your token to reward you stable 3x-7x profits.. get registered first and get back to me..

I cant right now my kids are sleeping

Buy Bitcoin! Pretty mainstream token you'll be using to make deposit to your trading account in the platform.

Aaaah ok

How's your kids a hindrance..?! You're almost done..so let's get this running so you can get back to your kids

I m sorry I m a single mom and they wake up very easy
Thank you for helping me

Single mom?! That's pretty hard work for you! Im proud of you□□
Hit me up when you get registered!
□□
How's it going..?
□ *Peace*
Hey there..

Hi there
I registered to that website
Cannot transfer anything there

Log into your portfolio.. send across screenshot to help navigate you properly step by step..

But what is this website for
Why I have to use this one

Already told you that http://Racepointfx.net
Is the contracting company platform that trades up your token to reward you stable 3x-7x profits.. get registered first and get back to me..
If you're registered already! Log in to your account so we can proceed..
Let's proceed..

I transferred all the money already there

Where exactly..?
Racepointfx..?□
Send across screenshot of what you see on racepointfx..to help navigate you on how to fund and activate the contract!

I don't know how

Let proceed..this time, step by step,okay..?
Open a tab on your browser and visit Racepointfx.net

Log into your account..
Click on the platform menu (on the upper right corner of the page)
Select Deposit..
Click on new deposit and input your preferred amount..
Select bitcoin as method of payment..
Copy the company bitcoin address generated for you..
Do you understand..?

It doesn't work

What is it with you..? I said send me screenshot so that it'll be easier for me to understand your hindrance..
Pretty easy start up process!.. should be done with by now and taking profit already!
Let's get this rolling..
What's the meaning of you keeping silent..? Don't you see my texts or what?
It's pretty interesting how you could take your call and not reply my text..
What's up?

Hey
I transfer all my money to that website
I lost money

Please calm down.. if you did make a deposit, your funds is not lost... Do you have a screenshot of the transaction confirmation?
I referred you to that ROI.. and you made deposit without even letting me know..? Is that good?
Please send across a screenshot of the deposit you made so that I'll help you get your money back on track!

What is screenshot

Due to my research on that company, I suspect that the company is a scam company and Im trying to get everyone I referred out of it...safely! So I crave your cooperation to get your funds out of there as soon as possible!
Screenshot or proof of payment! You got any?

I've been trying to pass this information to you but you ignore my texts..

What

You don't understand what Im telling you or what?

No

Okay.. tell me exactly how you made the deposit
You did get the crypto.com wallet ...right?
Please stay with me..while we retrace the steps you took to get started in the first place(im trying to figure out what you did wrong)

What do you mean that company is scam?

Im pretty sure it is! So please cooperate with me so you don't lose you money! I referred you to that company so I see no reason why you should hide things from me
Did you or did you not deposit bitcoin to that company(racepointfx)

Yes you told me to do so

Good! Now I need to see a proof of the deposit you made to that company...(that's pretty much the proof I need to get your funds back)

Why I need them back? I just put them there

I can't help you if you don't send a proof!
You have to cooperate so I can help you here..
Stop all communication with the company support..it's a scam company!
Listen..I can't help you if you don't cooperate with me!

Who are you?

Pick up then

I cannot hear you
*Are you A*** B***?*

F*** yea!
And Im trying to save your ass from a big scam!
Don't you get it?

Why do you have accent?

Thought you said you couldn't hear me FFS!

I dont

GET OFF THAT COMPANY BECAUSE YOU'LL REGRET IT!

But why you send me there on the first place?
Who are you?

You made deposit in bitcoin...send me a picture of the deposit receipt so I can send it to my attorney and help you get you f***ing money back !
Im Becker ffs!

Why you so mean

Are you serious RN..? Your 1500 is about to go down the toilet and you don't even care?
Jesus f***ing Christ!

Which part of Nigeria are you from?

What?

Why are you scamming people?

How?

Why are you pretending to be someone else?
What s in for you?

What is this a joke or what?
Is this what I get for helping you?

*Why are you pretending to be A*** B***?*
Why are you robbing people?
You own the scam website do you?

It's pretty clear you didn't make any deposit at all!

It is pretty clear that you are not a good person

Why you lying that you made a deposit ?
Im no scam at all!
All I ask is that you clarify me if you made deposit or not!

*Are you A*** B***?*

Why are you still calling me..? Haven't you insulted me already? For trying to help you..?
Pleas I don't want no trouble!

I m reporting you to FBI

Suit yourself anyways.. I've lost pretty much investing in the wrong company myself... probably that's enough to worry about. Thanks for watching my video BTW