Phishing Attacks on Cryptocurrency Traders in Arab States of The Gulf

Sawsan Alshehri[1], Reem Alhotaylah[1], Marwa Alyami[1], Abdullah Alghamdi[1], Mesfer Alrizq[1]

Department, of Information Systems, College of Computer science and information systems, Najran, Saudi Arabia

Summary
With the great development of technology in all fields these days, including the financial field, people have gone into cryptocurrency trading, without prior knowledge or experience, which made them prey and coveted by hackers through phishing attacks. Therefore, we will study cases where people can be a victim of phishing because cryptocurrency occurs without an intermediary, such as banks and monetary institutions. It is a form of peer-to-peer transaction, physical wallets, and fake investing. This study aims to know the concept of a phishing attack on cryptocurrencies, and to measure the extent of peoples awareness of the security risks on these currencies. Previous literature will be reviewed, and a questionnaire will be published on traders who use cryptocurrency trading platforms, and then we collect data and analyze the answers provided, so that we can suggest educational solutions to these phishing problems.

Keywords:
Cryptocurrency, Ceybersecurity, Phishing Attack, Awareness, Privacy.

1. Introduction

With the wide spread of technology, people have become obsessed with keeping abreast with everything that is modern and fast especially the new ones that are interesting and may bring fun and interest to them at the same time. Recently, the concept of investing in cryptocurrencies has spread, and there has been a rise in the number of cryptocurrency users as an investment platform, so people rushed to get into it and look for ways to earn money faster. Cryptocurrency exchange on electronic investment platforms (such as Binance platforms) refers to effective exchange of an asset directly between people without the intervention of a central authority that guarantees their rights and checks their transactions. The basic motivation behind the establishment of cryptocurrencies was to create a direct peer-to-peer cash exchange.

This process done by using cryptography to secure transactions, without the need for the presence and participation of a trusted authority such as a central bank. Rather, it uses a decentralized system to record transactions and issue new units. Since today we are seeing a massive technological leap, and the popularity of cryptocurrency exchanges is high among the public, cryptocurrency platforms have made a way for hackers. They exploit ignorant people who is looking to make a quick profit and make them attractive targets for hackers who are greedy to steal these people's money. Taking advantage of the idea that the identity of users on cryptocurrency platforms can be fake and unreal, which increases the chance of them escaping and not getting held, and legally punished when fraud and exploitation of people. As the idea contributed to the implementation of a group of large and varied electronic attacks on exchanges, especially social engineering attacks such as phishing and trust trading fraud.

Based on the statistic in earlier scientific research, the percentage of fraud in cryptocurrency exchanges were 83%, phishing was the second largest category common fraud method in cryptocurrency communities, as it occurred by 26.65% [1]. Phishing is one of the most important and most dangerous electronic attacks related to social engineering to occur on digital currency platforms, and it is a cyber-attack that means an attempt by an unauthorized hacker to access the victim's private and sensitive information directly or indirectly. Phishing is an attack, happen when the victim is fraud and lured by the hackers, and the hacker gained the victim's trust. in the hope of obtaining his confidential data and property. The attacker includes fake personal information with ability to make it more believable, or through false fake advertisements, deceptive email that appears officially and legally, which prompts users to believe that it is a trusted party to deal with it through trading and exchanging currencies with it.

This is the outcome of our research; our first step is to look into cryptocurrency exchange phishing, discuss the security issues associated with it, how people become victims of it, and what are the proposed and potential solutions to do to actually avoid phishing attacks, and it's done by contributing to suggesting and developing more strong defensive mechanisms against these attacks. In this research, the previous literature will be reviewed on the latest crimes related to phishing attacks on cryptocurrencies, disseminating a questionnaire to several community groups for cryptocurrency traders, then analyzing the answers to find out the fraud issues and problems faced by traders of cryptocurrencies, thus provide suggest solutions for these security issues, for future studies related to these phishing

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.12

issues. Our study in this paper had a main aim, which is to study the threat and danger of phishing fraud on digital currencies, identify a proposed defense mechanism to avoid these attacks, and driven by the following research questions (RQs):

RQ1: Are phishing attacks the most common attack on cryptocurrencies?

RQ2: What phishing methods might occur?

RQ3: What is the impact of phishing attacks?

RQ4: Does the cryptocurrency users in the Arab States of the Gulf have enough knowledge about each cryptocurrency background, and their related projects?

RQ5: How aware is the traders of cryptocurrencies about the dangers of phishing attacks?

RQ6: What are the proposed solutions and defensive mechanisms available to avoid the risks of phishing attacks on cryptocurrency and to detect a suspicious attackers account?

2. Literature Review

In this section, we will review the literature that has been relied upon in this paper. The first section focuses on the general concept of cryptocurrency technique. The second section also summarizes the fraud, specifically phishing in the cryptocurrency community and platforms, and mentions the stories, issues, and problems that this phishing causes. The third section summarized the ways and solutions to avoid this phishing fraud that exists in cryptocurrency platforms and communities.

2.1. CRYPTOCURRENCY DEFINITION

Cryptocurrencies are digital assets that exist to create intangible money based on blockchain technology which invented in 2008[2], that provides and manages a data warehouse without a central and government system, and ensures the safety of the input, by encryption, to becomes difficult to change in these inputs [3]. Traders generate these currencies through a series of numbers and letters, and then transferred between devices through private and public keys[4],and when a trader wants to make a deal, the trader must have one key out of two pairs of digital keys. once traders execute the transaction, there is no modifications or retrieve [5]. There are two ways to store these cryptocurrencies; Either the hot wallet (online), or the cold wallet (offline) [5]. These features of Blockchain technology as an intangible asset, decentralization, no need to provide a real identity, and the absence of a judicial authority have created an ideal environment for cybercrime [6].

2.2. CRYPTOCURRENCY FRAUD AND PHISHING ISSUES

Cryptocurrencies are by their nature decentralized as they do not depend on official authorities, government, and banks, thus facilitating cybercrime such as fraud, theft, unauthorized use of computer resources (for mining), social engineering attacks (to steal credentials), besides provided criminals with opportunities to develop new crimes [7, 8, 9]. Perhaps the most important feature that blockchain trading platforms provide is the anonymity feature, where the trader, whether hacker or other person, does not appear as a reason to attract hackers to use it as a means to reach the victims, disguised as false pseudonyms to deceive the victim and gain their trust[3]. Social engineering is the main attack that has become increasingly common in the cryptocurrency community [10, 11], as attackers use psychological tricks that enable them to gain access to the financial values stored in users' wallets [11] . Cryptocurrency phishing is every phishing threat that seeks to reveal sensitive information, and gain cryptocurrency using mail, ads, social media sites, and text messages [12,13], phishing incidents also accounted for 98% of social incidents in 2018 [14], and according to a study that took place in 2019, on the famous Binance platform, a group of thieves took cryptocurrencies in the amount of 7,000 Bitcoin, which is equivalent to today's $41 million, by carrying out fraudulent attacks, including phishing [15].

Attackers seek to obtain the private keys or credential information of the user in phishing in cryptocurrency occurs in many ways, and its most common of them are Punycode method or Fake Airdrops, where Punycode sends an email to the user by falsifying the mail and domain of the official website, besides demands to enter the required data at the official site, as for Fake Airdrops, it is more accurate phishing as the attacker asks the user for his complete data (e-mail, wallet information), by imitation of the official exchange of money in the wallet, whether in e-mail or social networking sites [6]. Credential phishing is one of the biggest security issues on the internet, and attackers have found cryptocurrency phishing a very profitable attack [16], perhaps one of the reasons that prompted thieves to steal nearly 50 million US dollars of cryptocurrency in trading platforms is the difficulty of detecting the attacker who phished on Ethereum [17,18].

In 2017, victims reported that phishing on Ethereum, with almost $115 million stolen, one of them is the famous Bitcoin phishing campaign called "Coinhoarder" in Ukraine, during which attackers stole tens of millions of dollars, by evolving to make their phishing pages appear as an official page, with bad use of fake SSL certificates [16]. One of the problems that made users fall victim to phishing is ignorance, users did not have enough knowledge of cryptocurrencies and enough security awareness, as they interact with phishing sites that look like legitimate sites and send their coins to the attacker's wallet [19] . A famous issue in cryptocurrency is Cryptojacking attacks, in which computer resources (processor, etc.) are accessed in many ways, one of which is phishing, which is the common way for attackers to initiate mining operations [20] ,also in the dark web there are services for presenting pages and

disguised phishing documents (invoices, etc.) and they are sold. [21] Finally, there was a recent release accompanying the Covid 19 crisis in 2020, due to the expansion of digital currencies in the Covid 19 crisis and the increase in the number of newbie users, which prompted companies to start accepting them as payment, therefore, making cryptocurrency phishing one of the most common and growing forms of fraud in This crisis[2]. Previous literature included various forms of phishing, directly or indirectly, as phishing was a means of other attacks and crimes on/using cryptocurrencies. Recognizing the types of attacks leads us to identify ways to prevent and recover from them.

2.3. METHODS AND RESULTS

The Internet environment is a constantly growing environment, and provides complex and difficult tools, so it is necessary to impose preventive and defensive measures worldwide to prevent and mitigate such cybercrimes on cryptocurrencies, and to reduce phishing attacks that caused different losses (as we saw in the second section). Mircea Constantin ȘCHEAU, et al, believes that cryptocurrencies hold promising and bad future surprises [22]. Researchers used machine learning to detect suspicious activities with high accuracy in transactions to detect phishing attack, after they analyzed the periodic behavior of transactions [3]. As for other researchers proposed solutions, the AdaBoost classifiers used to detect malicious entities. It turns out that the features were effective in finding malicious entities[23]. A suggestion to use RASP (a cyber security technique and a security tool) due to the lack of knowledge that users have about cryptocurrency, by detecting the attack according to vulnerabilities in code, by observing the behavior of the application in real-time rather than relying on predefined patterns or signatures [19].

The researchers categorized six types of threats to cryptocurrency, and suggested countermeasures for each threat. One of them was phishing, and countermeasures to it such as: opening the URL of the legitimate system directly, multiple authentications, using a cold wallet, and others [13]. Researchers analyzed public data via the internet and blockchain-based data and created a classification of frauds with pre-charged phishing frauds, and applied DBSCAN technology to this data, the classification found sixteen out of one thousand phishing websites for prepaid fee frauds [24]. While researchers analyzed the schemes most used in phishing attacks on the blockchain, recommended a defense against these schemes, and made alternatives to DNS used in phishing [14]. A phishing detection framework has been developed based on the use of engineering, and this is returned to the records of agreements and transactions. Also, this framework was worked on by doing 3 steps on Ethereum, specifically to find phishing attacks on it, Where the steps are taken starting from an extensive search in their transaction records. Then the criminals' Ethereum account will be found directly, instead of their fraudulent methods and messages [17]. While [25] researchers proposed detecting phishing in Ethereum blockchain transactions by means of algorithms that effectively detect phishing using etherscan.io client and crawling, and then aggregate all phishing transactions and addresses. Next, create a transaction graph and suggest a way to extract the progression feature based on the graph.

Besides that, a framework that automatically recognizes cryptocurrency frauds was also provided new insight into future exposure work on Ethereum [26, 27], and 1,000 phishing nodes have been processed to advance the development of phishing fraud detection to take care of blockchain security, by data structures and the representation structures of nodes in the technology of the features of nodes in the network [27]. There was also a classification of two phishing addresses in two approved sites, trans2vec is a classification aims to find and report addresses sequence, to find and identify possible future phishing attack [28] . Authors evaluated Ethereum security and anti-phishing tools, using 200 phishing URLs and 500 legitimate URLs by using ten phishing tools for evaluation; and they found out that just one tool of their tools could perform the identification all the time by over 90% of the phishing URLs [29].

Researchers provide a new apriori method for detecting user groups that are likely to be involved in P&D schemes. The Mt. Gox confirmed the leaked algorithm's validity using Bitcoin exchange's transaction history, many suspicious trading practices were discovered on the exchange [30]. Legally, cryptocurrency is data; as one of the provisions of the Information Crimes Act in South Africa was to criminalize those who possess data suspected of illegally obtaining them through phishing and others, with the perpetrators prosecuted [4] besides that, the Criminal Code of the Russian Federation punishes the presence of the possibility to perform phishing to access protected computer data, which leads to copying, destroying, or modifying the content of the cryptocurrency [5]. At the end, Arab researchers have analyzed the real challenges of currencies in Arab countries and found that the digital currency has not been recognized in the Arab community because of the terms of religion, approval from Governments and the cost of the Internet [31]. Researchers have limited the literature to the technical and legal aspects of combating phishing on cryptocurrency, where awareness among users has not received sufficient studies. We made a table in order to compare the previous literature studies from six aspects (cryptocurrency, phishing, attack techniques, suggested solutions, and contact with traders) as shown in Table 1, through which we discovered the limitations of previous studies on specific aspects and not others. In our study, we will seek to cover the six aspects of the table, in order to find and analyze the most important causes of fraud in order to educate people about its dangers and how to stay away from them.

Table1: References Assessment

Reference	Cryptocurrency	Phishing	Attack's Techniques	Solution Suggestion	Case Studies	Contact with Traders
[1]	√	√	√	√	√	√
[2]	√	√	√	√		
[3]	√	√	√		√	
[4]	√	√	√		√	√
[5]	√	√	√	√		
[6]	√	√	√			
[7]	√	√	√			√
[8]	√	√	√		√	
[9]	√	√	√	√		
[10]	√	√	√	√	√	√
[11]	√	√	√	√	√	
[12]	√	√	√	√	√	
[13]	√	√	√	√	√	
[14]	√	√	√		√	√
[15]	√	√	√	√	√	
[16]	√	√		√	√	
[17]	√	√	√	√		
[18]	√	√	√	√		√
[19]	√	√	√			
[20]	√	√	√	√	√	
[21]	√	√	√	√	√	
[22]	√	√		√		
[23]	√	√	√	√	√	
[24]	√	√		√		
[25]	√	√		√	√	
[26]	√	√	√	√	√	
[27]	√	√		√	√	
[28]	√	√	√	√		
[29]	√	√	√	√	√	
[30]	√	√		√	√	
[31]	√				√	

3. Methodology

This study was cross-sectional using a questionnaire, conducted in April 2022, the target audience are the traders of cryptocurrency on Arab States of the Gulf total number about (747,100) according to the statical, the pools and channels of cryptocurrency traders were searched in the social media platforms Twitter and Telegram, and the total number of these traders on pools and channels was 250,000. An electronic questionnaire was used to collect data and the number of traders approached was 970, and for the final number of our respondents was 614, with rate of 63.3%; because we excluded both the responses that were in the trial period of the questionnaire and non-gulf citizens responses, as the non-gulf citizens respondents were 241, and as the trial period responses were 115. The data was collected during two consecutive weeks, in each week it was collected from one platform, the first week was the Telegram platform, the second week was the Twitter platform. influencers in these communities have cooperated with us to publish the survey. We also obtained admin approval for each channel and grouped before publishing the survey. We have interacted with the participants in their gatherings during the publication, in case there was a need to clarify a specific question and asked them to answer with credibility.

We sent the survey to several WhatsApp group traders before it was officially published and asked for their feedback regarding the questions in terms of clarity and comprehensiveness. the feedback has been considered, improved the survey, and published it in its final version. The data collected in the trial period was excluded - as mentioned earlier - as 115 responses were excluded from the trial period. The survey contains 14 questions divided into 3 sections that were written as follows: The first section was 3 questions about personal information of the survey recipients including gender, age group, and country (since we target cryptocurrency communities in the Arab States of the Gulf). The second section was questions about knowledge about cryptocurrencies and how to use their systems and platforms, as it included a question that contained a measure of people's knowledge of dealing with these platforms and currencies. The third section contains questions about exposure to fraud in terms of forms of fraud. The questionnaire has been presented to the integration of the Arabic and English, as in cryptocurrencies there are English terms in cannot be translated into Arabic.

4. Statical Analysis

The characteristics of our respondents were described using frequency distribution, also we used Chi-square test in order to examine the distribution of methods of falling victim to cryptocurrency phishing attacks among traders according to demographics. As we use P-value if less than 0.05, then it's considered as the level to cut-off the statistical significance.

5. Results

At first, Figure1 will display the demographic characteristics and the personal information of our final respondents. such as age, gender, and country (since we target cryptocurrency communities in the Arab Gulf countries). In general, most of the respondents were males (85%), and the majority were in Saudi Arabia with the rate (83.5%).

This table shows the data rates for the questions of the first section that refer to the personal information of the respondents on the questionnaire. Follow Table2:

Table2: Demographic characteristics of study respondents (n= 614).

Variable	n (%)
Gender	
Male	522 (85%)
Female	92 (15%)
Age	
18 – 25	110 (17.9%)
26 – 40	396 (64.5%)
41 – 60	100 (16.3%)
More than 60	8 (1.3%)
Country	
Saudi Arabia	513 (83.5%)
UAE	27 (4.4%)
Oman	11 (1.8%)
Qatar	7 (1.1%)
Kuwait	44 (7.2%)
Bahrain	12 (2%)

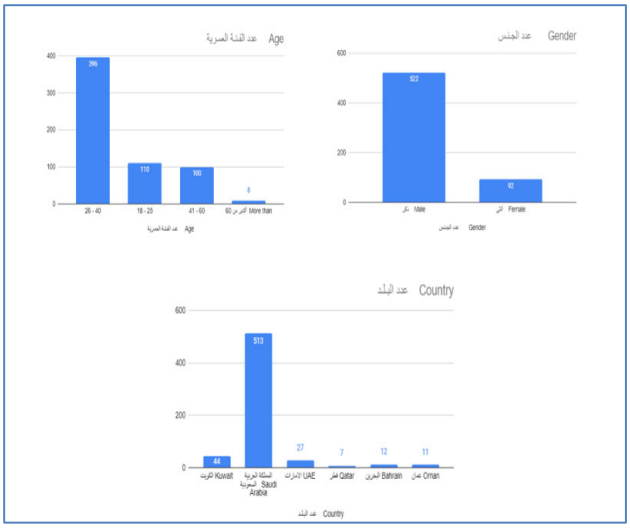

Figure1: Demographic characteristics and personal information of the end responders

Figure 2 is about revealing answers to questions about traders' experiences and ways of dealing with cryptocurrencies, and most of the respondents were expecting a high rate of cryptocurrency use in their country in the future (86.3%) as we expect this also due to the increase in these currencies in their circulation. Nearly half of the respondents believed that the English language was not an obstacle to dealing with cryptocurrencies (60.3%) that may be another barrier they face, rather than that these currencies hinder their trading in it because of the language.

About 50.8% use decentralized platforms for trading since it allows them to use more than one wallet. However, most of the respondents were using Binance as a cryptocurrency exchange, since it is one of the most popular cryptocurrency exchanges, so the trader is trading on one they can trust. Despite being a centralized platform, it has an average rate of 82.7%. With most respondents trusting global platforms when trading cryptocurrencies, the average of 81.1% is due to the popularity of global platforms, which are the oldest. We also found that most respondents use a hot wallet to store their cryptocurrency instead of a cold wallet, their rate was (83.2%) and this is one of the reasons why they are vulnerable to fraud because a hot wallet is considered less secure compared to a cold wallet with no internet connection. 39.25% of cryptocurrency traders were previously scammed while trading, because they trade ignorantly and impulsively, with the highest rates of email scams because it is one of the commonly used methods of phishing and seems more trusting to the user if they receive a message in their mail, social media or platform page fake trading.

The table also displays the percentage of data for each answer to the questions of the second section of the

questionnaire, which is related to the experience of traders and their methods of dealing with cryptocurrencies, follow up on Table 3:

Table 3: traders' experiences and methods to deal with cryptocurrency

Variable	n (%)
High Expectancy of Cryptocurrency Usage	
Yes	530 (86.3%)
No	18 (2.9%)
Maybe	66 (10.7%)
English Language as an Obstacle%	
Yes	231(37.6%)
No	370 (60.3%)
Maybe	66 (2.1%)
Platform System	
Centralized Platforms	302(49.2%)
Decentralized Platforms	312 (50.8%)
Used Arabic Trading Platform	
Coinmena	67 (10.9%)
Rain	182 (29.6%)
Bitoasis	94 (15.3%)
others	271 (44.2%)
Used Trading Platform	
Coinbase	13 (2.1%)
Binance	508 (82.7%)
Bitfinex	14 (2.3%)
Kucoin	49 (8%)
others	30 (4.9%)
Trusted Platforms	
Arabic platform	116 (18.9%)
Global platform	498 (81.1%)
Wallet type	
Hot	511 (83.2%)
Cold	103 (16.8%)
Phishing And Scam Methods (From 240 answers)	
Via e-mail or social networking sites	
Fake trading platform page	46 (19.2%)
Electronic way, such as malicious	43 (17.9%)
links	35 (14.6%)
Google adware	37 (15.4%)
Fake mobile apps	17 (7.1%)
Fake education websites	34 (14.2%)
Automated trading (boot)	21 (8.8%)
Other answers	7 (2.8%)

Figure 3 is about revealing answers to questions related to knowledge about cryptocurrencies and how their systems and platforms are used, as it included a question containing a measure of people's knowledge of dealing with these platforms and currencies. As for the respondents' opinions about cryptocurrencies (knowledge, difficulty, awareness, security and possibility of fraud), their percentage was (35.3%, 70.3%, 36.7%, 66.8%, 33%, respectively).

Where their knowledge of the cryptocurrency was less than half and it was 35%, which is a frustrating percentage and an indication that the trader rushes ignorantly and takes risks without enough knowledge until he becomes vulnerable to fraud. On the other hand, respondents indicated that they face difficulty in using and dealing with cryptocurrencies, as the difficulty was 70.3%. In terms of awareness, they were 36.7% security aware, which makes sense given the ignorant deliberations they are trading. As for the safety they see in trading, the percentage is 66.8%, which makes them feel safe while trading, ignoring their great role in increasing security through their awareness. As for the probability of being scammed, their percentage was 33%, which is a somewhat contradictory result compared to their great ignorance in trading, we do not consider it an accurate percentage, they may not have been exposed before to receiving a disguised phishing email impersonating a trusted platform, so they think that they are not vulnerable to defraud.

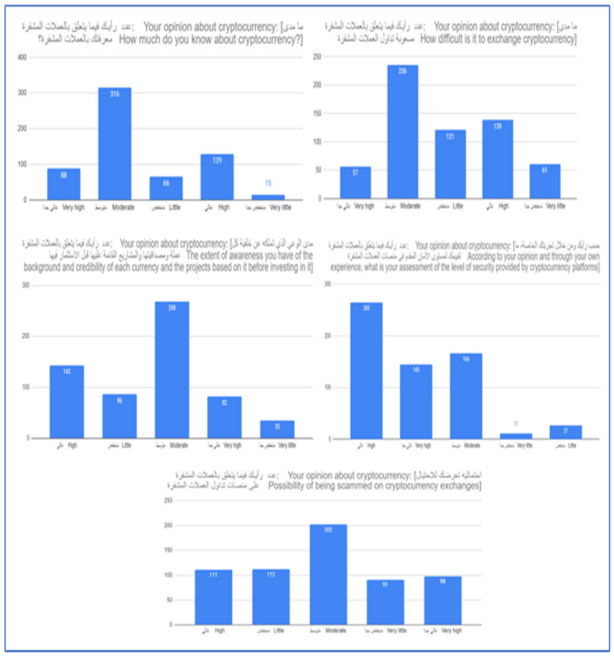

Figure 3: Knowledge about cryptocurrencies

The third section also reviews the measurement of people's knowledge of dealing with cryptocurrencies and the ratios were as shown in the following table.

When comparing the distribution of crypto-phishing tactics among traders according to demographics (gender, age, and country), it showed a significant association with awareness (shown in Table 1), with a higher rate of female scam victims. Males, perhaps because females are quick to trust without checking more than males. (56.7%, 36%, $p < 0.05$). For the age group most exposed to phishing attacks, the over 60 age group occupies the highest 87.5% as they lack knowledge of reliable methods for checking messages and phishing methods, and they are less knowledgeable and less in-depth about technical means than cryptocurrency traders.

The highest percentage of traders exposed to phishing attacks is among traders from Oman with an average of 63.6%. For example, only 28.6% of traders in Qatar experienced phishing attacks when dealing with cryptocurrencies, while 58.3%, 55.6%, 40.9%, and 37.2% of traders in Bahrain, UAE, Kuwait, and Saudi Arabia, respectively, disclosed phishing attacks when dealing with cryptocurrencies. Dealing with cryptocurrency. The general level of awareness of dealing with cryptocurrencies was not sufficient for 240 traders (39.25%) because they were victims of cryptocurrency phishing attacks, while 371 traders (60.75%) had a good level of awareness to avoid phishing attacks as shown in Table 5.

Table4: measuring people's knowledge of dealing with cryptocurrencies

	n (%)				
Question	Very high	High	Moderate	Little	Very little
How much do you know about cryptocurrency?	88 (14.3%)	129 (21%)	316 (51.5%)	66 (10.7%)	15 (2.4%)
How difficult is it to exchange cryptocurrency?	57 (9.3%)	139 (22.6%)	236 (38.4%)	121 (19.7%)	61 (9.9%)
The extent of awareness you have of the background and credibility of each currency and the projects based on it before	82 (13.4%)	143 (23.3%)	268 (43.6%)	86 (14%)	35 (5.7%)
According to your opinion and through your own experience, what is your assessment of the level of security provided by cryptocurrency platforms?	145 (23.6%)	265 (43.2%)	166 (27%)	27 (4.4%)	11 (1.8%)
Possibility of being scammed on cryptocurrency exchanges	98 (16%)	111 (18.1%)	202 (32.9%)	112 (18.2%)	91 (14.8%)

6. Discussion and Recommendations

This study was conducted in order to assess cryptocurrency traders' knowledge and awareness of research dealing with cryptocurrency and avoid falling victims for phishing attacks. We see that the culture of cryptocurrency trading is more popular among Gulf males than females, as they had a great interaction on the social media platforms that we published, perhaps because they have a greater interest in everything new in financial trading. Regarding the age group, young people between the age of 26-40 see maybe because they have a limited income and they are more willing to risk the craving for quick profit in any form, or maybe because they are the most interactive on social media platforms, so they represented the majority of the age group traded in our survey which we have done. As for the fact that the majority are from Saudi Arabia, we believe that the reason is likely because the platforms through which it was published were mostly Saudi, not Gulf.

Insufficient awareness was most noticed in all groups of age, especially elderly traders (more than 60), but there was approximately enough awareness between traders in the age group 26 - 60. These findings from the survey responses emphasize the increasing needs in raising the awareness and the training of the cryptocurrency traders before and during their journey with dealing with other traders in all platforms and websites. Also, we find out that more than half of female traders were scammed in many different ways, made us assuming many reason that made them a special target by phishing attacks, notably When comparing the distribution of methods of falling victim to cryptocurrency phishing attacks among traders according to demographics (including gender), it showed a significant association with awareness, with a higher rate of female scam victims, perhaps one of the most important reasons that made them victims of phishing attacks is the emotions

known to female more than the male traders, and the blind trust and their large presence on social media sites such as Twitter and Telegram may also be another reason for them to fall victim.

In our current study, we found that more than a third of traders have fallen victims to fraud and phishing attacks, specifically nearly 40% of them, which is not a small percentage that may increase in the future with the increase of cybercriminal means among phishing attackers in light of ignorance and lack of awareness among cryptocurrency traders. Specially that the general level of awareness of dealing with cryptocurrency was not sufficient for 389 traders (63.35%) with average or lower awareness level, while 225 traders (36.64%) had a high level of awareness (more than average) In conclusion, the results of our current study revealed insufficient awareness about dealing with cryptocurrency among traders in the Arab Gulf countries, as the majority of respondents were not aware about dealing with cryptocurrency in a good way to avoid phishing attacks. The results of our study emphasize the importance of proper trading ways in dealing and exchange of cryptocurrency, especially since once traders execute the transaction, there is no modifications or retrieve. Also, a good training is recommended before and during their journey with dealing with other traders in all platforms and websites, as it will improve treaders' abilities to identify untrusted traders and attackers, as well as understand the importance of checking before performing trading transactions and be aware of the different ways of phishing attacks.

Table 5: distribution of phishing methods on victims among cryptocurrency traders according to demographics

Variable	Cryptocurrency Traders as Victims of Phishing Score		P-Value
	Yes N (%)	No N (%)	
Gender			$X^2(1, N = 614) = 13.814, p = 0.0002$
Male	188 (36%)	334 (64%)	
Female	52 (56.7%)	40 (43.3%)	
Age			$X^2(3, N = 614) = 9.503, p = 0.0233$
18 – 25	48 (43.36%)		
26 – 40	148 (37.4%)	62 (56.64%) 248 (62.6%)	
41 – 60	37 (37%)	63 (63%)	
More than 60	7 (87.5%)	1 (12.5%)	
Country			$X^2(5, N = 614) = 8.303, p = 0.140$
Saudi Arabia	191 (37.2%)	322 (62.8%)	
UAE	15 (55.6%)	12 (44.4%)	
Oman	7 (63.6%)	4 (63.4%)	
Qatar	2 (28.6%)	5 (71.4%)	
Kuwait	18 (40.9%)	26 (59.1%)	
Bahrain	7 (58.3%)	5 (41.7%)	

7. Conclusion

At the conclusion of this research paper, many papers have studied Arab states of the gulf [32-35] while some other studies focus on blockchain usage [36-37]; however, we focus on the aspect of awareness of trading in cryptocurrencies in the Arab States of the Gulf, by study the threat and danger of phishing fraud on digital currencies with the help of thirty one scientific papers as literature review, and as a methodology for this paper we use questionnaire for the targeted audience (Traders of cryptocurrencies in the Arab States of the Gulf) , we showed that the above-mentioned from gathering data that we found that the majority of traders did not have sufficient awareness of currencies and trading in them as well. On the other hand, there was a heavy attack of phishing in this regard, our study emphasizes the importance of having sufficient awareness before and during trading in order to avoid falling as a victim various types of phishing, full background about cryptocurrencies, self-education and greater interest from the concerned authorities about the danger of fraud in cryptocurrency its recommended as it will improve through its investor awareness.

Our results may be developed into supportive technical solutions, such as machine learning solutions and methodologies to detect cryptocurrency phishing, and we encourage the Arab researcher to show sufficient interest in this fast-spreading topic recently, in order to reduce such attacks and spread adequate awareness of how to avoid them.

References

[1] Xia, P., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., Wang, H., & Xu, G. (2020). Characterizing Cryptocurrency Exchange Scams. http://arxiv.org/abs/2003.07314

[2] Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., Xu, G., Huang, G., & Liu, X. (2020). Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. http://arxiv.org/abs/2007.13639

[3] Lal, B., Agarwal, R., & Shukla, S. K. (2021). Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain. http://arxiv.org/abs/2108.11818

[4] Reddy, E. (2020). Analysing the investigation and prosecution of cryptocurrency crime as provided for by the South African cybercrimes bill. In Statute Law Review (Vol. 41, Issue 2, pp. 226–239). Oxford University Press. https://doi.org/10.1093/slr/hmz001

[5] Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. In Crime Science (Vol. 11, Issue 1). BioMed Central Ltd. https://doi.org/10.1186/s40163-021-00163-8

[6] Astrakhantseva, I., Astrakhantsev, R., & Los, A. (2021). Cryptocurrency fraud schemes analysis. SHS Web of Conferences, 106, 02001. https://doi.org/10.1051/shsconf/202110602001

[7] Reddy, E., & Minnaar, A. (2018). CRYPTOCURRENCY: A TOOL AND TARGET FOR CYBERCRIME Civil-military relations View project Rural crime View project. https://www.researchgate.net/publication/338572871

[8] Lapuh Bele, J. (2021). Cryptocurrencies as facilitators of cybercrime. SHS Web of Conferences, 111, 01005. https://doi.org/10.1051/shsconf/202111101005

[9] Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., Vigne, S. A., & Chi Minh City, H. (n.d.). The Destabilising Effects of Cryptocurrency Cybercriminality.

[10] Ivanov, M. A., Kliuchnikova, B. v., Chugunkov, I. v., & Plaksina, A. M. (2021). Phishing Attacks and Protection against Them. Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, 425–428. https://doi.org/10.1109/ElConRus51938.2021.9396693

[11] Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). Exploiting the human factor: Social engineering attacks on cryptocurrency users. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12206 LNCS, 650–668. https://doi.org/10.1007/978-3-030-50506-6_45

[12] Sayeed, S., & Marco-Gisbert, H. (n.d.). On the Effectiveness of Blockchain Against Cryptocurrency Attacks.

[13] Froehlich M, Hulm Ph.,& Alt F. (2021). Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners

[14] Andryukhin, A. A. (2019). Phishing Attacks and Preventions in Blockchain Based Projects. Proceedings – 20 International Conference on Engineering Technologies and Computer Science: Innovation and Application, EnT 2019, 15–19. https://doi.org/10.1109/EnT.201900008

[15] Anti-Phishing Working Group, & Institute of Electrical and Electronics Engineers. (n.d.). 2018 APWG Symposium on Electronic Crime Research (eCrime) : proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime) : San Diego, California, USA, May 15-17, 2018.

[16] Wen, H., Fang, J., Wu, J., & Zheng, Z. (2021). Transaction-based hidden strategies against general phishing detection framework on ethereum. Proceedings - IEEE International Symposium on Circuits and Systems, 2021-May. https://doi.org/10.1109/ISCAS51556.2021.9401091

[17] Badawi, E., & Jourdan, G. V. (2020). Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. In IEEE Access (Vol. 8, pp. 200021–200037). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3034816

[18] Gottipati, H. (2020). A PROPOSED CYBERSECURITY MODEL FOR CRYPTOCURRENCY EXCHANGES.

[19] Varlioglu, S., Elsayed, N., Elsayed, Z., & Ozer, M. (n.d.). The Dangerous Combo: Fileless Malware and Cryptojacking.

[20] Ahvanooey, M. T., Mazurczyk, W., Taleby Ahvanooey, M., Zhu, M. X., Kilger, M., & Choo, K.-K. R. (n.d.). Do Dark Web and Cryptocurrencies Empower Cybercriminals? Covert Channels and Malware Analysis View project Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Study View project Do Dark Web and Cryptocurrencies Empower Cybercriminals? http://ax555xx.onion

[21] Șcheau, M. C., & Zaharie, Ștefan. (2018). The Way of Cryptocurrency. In Economy Informatics (Vol. 18, Issue 1).

[22] Poursafaei, F., Hamad, G. B., & Zilic, Z. (2020). Detecting Malicious Ethereum Entities via Application of Machine Learning Classification.

[23] Phillips, R., & Wilder, H. (2020). Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. https://help.twitter.com/en/rules-and-policies/financial-scam

[24] Chen, W., Guo, X., Chen, Z., Zheng, Z., & Lu, Y. (2020). Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. https://bitcoin.org/bitcoin.pdf

[25] IEEE Circuits and Systems Society, & Institute of Electrical and Electronics Engineers. (n.d.). 2020 IEEE International Symposium on Circuits and Systems (ISCAS) : proceedings : ISCAS 2020 : Virtual Conference, October 10-21, 2020.

[26] Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. IEEE Access, 9, 148353–148373. https://doi.org/10.1109/ACCESS.2021.3123894

[27] Chen, L., Peng, J., Liu, Y., Li, J., Xie, F., & Zheng, Z. (2021). Phishing Scams Detection in Ethereum Transaction Network. ACM Transactions on Internet Technology, 21(1). https://doi.org/10.1145/3398071

[28] Wu, J., Yuan, Q., Lin, D., You, W., Chen, W., Chen, C., & Zheng, Z. (2022). Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(2), 1156–1166. https://doi.org/10.1109/TSMC.2020.3016821

[29] Dika, A., & Nowostawski, M. (2018). Security Vulnerabilities in Ethereum Smart Contracts. 2018 IEEE International Conference on Internet of Things (IThings) and

IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 955–962. https://doi.org/10.1109/Cybermatics_2018.2018.00182

[30] Chen, W., Xu, Y., Zheng, Z., Zhou, Y., Yang, J. E., & Bian, J. (2019). Detecting "Pump & dump schemes" on cryptocurrency market using an improved apriori algorithm. Proceedings - 13th IEEE International Conference on Service-Oriented System Engineering, SOSE 2019, 10th International Workshop on Joint Cloud Computing, JCC 2019 and 2019 IEEE International Workshop on Cloud Computing in Robotic Systems, CCRS 2019, 293–298. https://doi.org/10.1109/SOSE.2019.00050

[31] Laadam, J. A., Profile, S., Li, J.-J., Shetewy, N., Aitlaadam, J., Li, *, & Jiang, J. (2019). Challenges of the Bitcoin in the Arabic Countries. https://doi.org/10.7176/JESD

[32] A. Alghamdi, "A Hybrid Method for Customer Segmentation in Saudi Arabia Restaurants Using Clustering, Neural Networks and Optimization Learning Techniques," Arabian Journal of Science Engineering, Jul. 2022, doi: 10.1007/s13369-022-07091-y.

[33] A. Alghamdi, "A Hybrid Method for Big Data Analysis Using Fuzzy Clustering, Feature Selection and Adaptive Neuro-Fuzzy Inferences System Techniques: Case of Mecca and Medina Hotels in Saudi Arabia," Arabian Journal of Science Engineering, Jun. 2022, doi: 10.1007/S13369-022-06978-0.

[34] Alghamdi, A., "Computer Science Graduation Project During Covid-19 Pandemic: Challenges and Solutions." IJCSNS - International Journal of Computer Science and Network Security, 22, 1, 718–724, 2022, doi: 10.22937/IJCSNS.2022.22.1.94

[35] A. Alghamdi, "Analyzing the Barriers and Possibilities with p-values towards Starting a New Postgraduate Computer and Engineering Programs at Najran University: A Cross-Sectional Study," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 11, no. 12, 59/31 2020, doi: 10.14569/IJACSA.2020.0111215.

[36] Y. Liu, G. Shan, Y. Liu, A. Alghamdi, I. Alam, and S. Biswas, "Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective," IEEE Access, vol. 10, pp. 28509–28519, 2022, doi: 10.1109/ACCESS.2022.3156591

[37] Reza, Md. S., Biswas, S., Alghamdi, A., Alrizq, M., Bairagi, A. K., & Masud, M., "ACC: Blockchain Based Trusted Management of Academic Credentials." 2021 IEEE International Symposium on Smart Electronic Systems (ISES) (Formerly INiS), 438–443, 2021, https://doi.org/10.1109/iSES52644.2021.00104

Sawsan Alshehri received the B.E. and M.E. degrees, from King Khaled University, Saudi Arabia. She is pursuing her professional master's degree at Najran University, Saudi Arabia, and she is working as a young researcher. Her research interest includes cryptocurrency, cybersecurity, and privacy.

Reem Alhotaylah received the B.E., from Najran University, Saudi Arabia. She is pursuing her professional master's degree at Najran University, Saudi Arabia, and she is working as a young researcher. Her research interest includes cryptocurrency, cybersecurity, and privacy.

Marwa Alyami received the B.E., from Najran University, Saudi Arabia. She is pursuing her professional master's degree at Najran University, Saudi Arabia, and she is working as a young researcher. Her research interest includes cryptocurrency, cybersecurity, and privacy.

Abdullah Alghamdi has a Ph.D. in Computer and Information Systems Engineering from Tennessee State University, Nashville, TN. Dr. Alghamdi obtained his M.Sc in Networking and Systems Administration from Rochester Institute of Technology, Rochester, NY and B.Sc in Information Systems from the Al-Imam University, Saudi Arabia. Dr. Alghamdi is currently working as an assistant professor at Information Systems Department at Najran University, Najran, Saudi Arabia. He is also trustee and executive secretary of scientific board. He has many publications in international journals and conferences. He is experienced in teaching, administration and research. He has been reviewer and guest editor of many journals, including MDPI electronics and energies. Also Dr. Alghamdi attended several conferences. His current research topics are security, privacy, IoT, interdisciplinary applications, and data analytics.

Mesfer Alrizq is an Assistant Professor at the Department of Information Systems in Najran University, Najran, Saudi Arabia. He received his Ph.D. in Computer Science from Western Michigan University, Kalamazoo, MI. Dr. Alrizq obtained his M.Sc in Information Technology from Rochester Institute of Technology, Rochester, NY and B.Sc in Information Systems from King Khalid University, Abha, Saudi Arabia. He has good number of publications in international journals and conferences. He is experienced in teaching, administration and research. His research interests span across broad areas of distributed artificial intelligence, multi-agent modeling, human behavior modeling, security, sentiment analysis, and information technology. He was awarded an Outstanding Graduate Research Award by the Department of Computer Science at Western Michigan University in 2019.