# Phishing Attacks and Preventions in Blockchain Based Projects

A.A. Andryukhin
KCD
Moscow, Russia
Alexandr@kcdigital.ru

***Abstract*— With the development of Internet technologies, the number of threats and attacks directed at networks and systems is increasing. Attackers invent new ways of attack or improve old ones. One of the most common serious threats is "Phishing", in which cybercriminals attempt to steal user credentials using fake emails or websites or both. Blockchain projects increasingly becomes the target of attacks by intruders due to high investments and gaps in national legislation. After a series of attacks on blockchain projects around the world, the issue of cybersecurity of blockchain became particularly relevant. The article classifies the main types and schemes of phishing attacks on the blockchain, suggests methods of protection against them, examines the development of blockchain protection against phishing attacks.**

***Keywords*— *blockchain, phishing, cryptocurrency, security, malware, social engineering***

## I. Introduction

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication [23]. It represent 98% of social incidents and 93% of breaches in Q2 2018 [20]. The goal can be anything from trying to get people to send you money, hand over sensitive information, or even just download malware unwittingly, and the authors of these attacks will use lies, trickery, forgery, and outright manipulation in order to see them succeed. The danger of phishing attacks is not the presence of vulnerabilities in the system, but in human gullibility and inattention. Often phishing uses Social Engineering: a kind of attack that relies on human fallibility rather than a hardware or software flaw in order to work [2]. Many blockchain projects that have strong security policies turned out to be helpless before the attacks using phishing, and members of the blockchain communities and investors lost their money. According to Cisco [12] and Kaspersky Lab [1] research the greatest number of successful attacks on blockchain projects were made with the help of phishing and scam without hacking the blockchain infrastructure itself. Kaspersky Lab experts tracked 1000 purses Ethereum, where users were deceived to list ETH 21 000, which is equivalent to about $10 million based on current rates [1]. This figure does not include the funds that the criminals stole directly from the victims' purses. The bulk of the problems lies in the vulnerability of cryptosystems using blocking technology. In the case of Ethereum, problems were observed not in the platform itself but in cryptosystems: they faced vulnerabilities in their own smart contracts, deface, compromise of admin accounts (Slack, Telegram), phishing sites copying the content of sites of companies issuing to ICO [22]. The article will review and classify the most known cases of fraud in blockchain projects, describe ways to implement attacks, propose existing methods of protection against them, and directions in which it is necessary to develop phishing protection.

## II. Types of Phishing Attacks

Conventionally, all phishing attacks can be divided into two types: social engineering schemes and technical schemes. Social engineering schemes are based on deception and subsequent independent wrong actions of the victim [17,24], while technical schemes use vulnerabilities and imperfections of software and infrastructure.

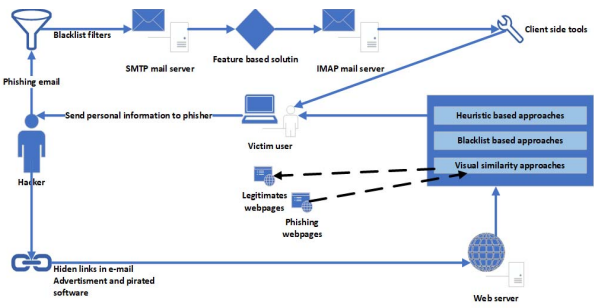


Fig.1 Example of the phishing scheme

### A. Social Engineering Schemes

The peculiarity of such schemes is the direct participation of network users in them. The attack is carried out by delivering to

978-1-7281-1915-1/19/$31.00 ©2019 IEEE
DOI 10.1109/EnT.2019.00008

the users false information and is activated after the user performs certain actions (opening the letter, moving on the link or downloading the malicious attachment) According to the Verizon research, 4% of users click on phishing links [20]. In order for an attacker to enter the system, one such click is sufficient.

TABLE I. Social engineering schemes

| Scheme | Project | Description |
|---|---|---|
| Clones | Blockchain.info, MyEtherWallet, Binance, IOTA | Scammers use of homograph attack to create a clone, advertising campaign and distribution. $50 million were stolen on the fake Blockchain.info site. A phishing website to generate private IOTA wallet seed passphrases, collected wallet keys, with estimates of up to $4 million worth of MIOTA tokens stolen. |
| Social networking | Telegram, Blockchain.info | Scammers create fake accounts in social networks posing as well-known projects |
| Bloating | ChainCoin, HighCoin | Artificially created demand, aggressive advertising in the media and social networks led to an unprecedented growth and the subsequent sharp drop in the rate of the Crypto-currency |
| Fake ICO | PlexCoin, E-coin | Projects did not own either the technologies that were claimed, nor the teams that could create the product. $15 million of PlexCoin ICO were frozen by SEC. |
| Pyramids, Ponzi | Bitcoin, Bitconnect | The organizer of an alleged Ponzi scheme advertised a Bitcoin "investment opportunity" in an online Bitcoin forum. Investors were allegedly promised up to 7% interest per week and that the invested funds would be used for Bitcoin arbitrage activities in order to generate the returns. Instead, invested Bitcoins were allegedly used to pay existing investors and exchanged into U.s. dollars to pay the organizer's personal expenses [21]. Bitconnect promised 1% per day growth of invested funds. |
| Aimed phishing | Enigma, Bee, Seele | The hackers got access to the email of Enigma CEO Gaius Ziskind. As a result, all the investors were sent messages with the offer to participate in reselling the tokens and the account details for transferring funds and $500 000 has been stolen. $1 million (Bee) and $1.8 million (Seele) were stolen using hacking of companies official e-mail lists. |
| Fake cryptocurrency wallets | NEO, Tether, MetaMask | Four fake wallets were found on Play Store |

***Clone phishing***. To carry out this type of attack, attackers create a copy of the site, a site with a similar name, or a fake page on the official website, and send out a link containing a link to a fake resource to potential victims from the addresses of trusted organizations. [1]. Phishers always take the benefit of human factors that generally ignore the critical warning messages [19]

Often, to create fake pages and sites, scammers use Punycode encoding [4,5]. This encoding allows to register domains with foreign characters. It works by converting a single domain label to an alternate format using only ASCII characters. Most often in the spelling of the site name scammers use Cyrillic [12]. The American standard code for information exchange (ASCII) "a" (U + 0061) and Cryillic "a" (U + 0430) are completely different characters, but they are displayed in exactly the same way. This means that the human eye can not tell the difference. As a result, it becomes impossible to identify the site as fraudulent, without thoroughly checking the URL of the site. This is called ***homograph attack*** [6].

To achieve the greatest resemblance and lull the vigilance of victims, fake websites and pages are equipped with ***SSL certificates*** using free 90-day certificates of Let's Encrypt and Comodo certification centers, having fake pages on hacked sites that have the necessary certificates, using web hosting with SSL-certificate, as well as forged certificates [3].

***Social networking phishing.*** Phishing attacks on social networks have become very widespread. Cases of hacking accounts of well-known personalities and publishing posts on their behalf containing phishing links, creating pages of clone-known personalities, communities, etc., have become more frequent. [18]. Scammers use the fact that Facebook allows you to create a page with any name, and conduct activities from fake clone pages that have very similar names to real community pages.

***Aimed Phishing***. The object of phishing are large investors, owners of purses, the first persons of companies, cryptocurrency owners. Attackers clearly represent what exactly, how many, from whom and how they want to hack. The spread has received a new kind of such hacking. Attackers calculate the activity of the victim in other spheres of activity and steal the necessary data imitating the interest in those spheres, coming into contact with the victim.

***Bloating***. Scammers artificially raise prices for easy-to-manage crypto-currencies with low liquidity and small market capitalization. The unprecedented price increase is widely reported through numerous media channels (YouTube, Twitter, Telegram), heavily advertised, promising a high return to external investors. After considerable investments by users, scammers stop supporting the course of the crypto currency and its price is returned to its original positions.

***The Pyramids, Ponzi.*** Not having any block-infrastructure and communication with the exchanges, these projects promise a high profitability of investments in crypto-currencies and blockchain projects, as well as a percentage of the investments of newly attracted users. Scammers close projects unexpectedly for everyone after collecting the necessary amount [21]. Most often, these schemes are used in the organization of imaginary cloud mining and fake crypto-exchange exchanges.

***Fake ICO.*** ICO (Initial Coin Offering) is the dream of any hacker. Lightning fast, often quite simple attack on crypto-currency services and block-start-ups brings millions of dollars of profit with minimal risk for criminals [22]. Early ICO

investors are the most vulnerable to cybercriminals. In 2017, ICO invested $ 1.6 billion, of which $ 150 million were in the hands of scammers [9].

Due to the fact that in the legislation of most countries there are serious gaps in the circulation of crypto-currencies and there is no judicial practice, scammers use the excitement around the detachment to withdraw to ICO projects that do not have a real product and the team to create it, attracting investors with tempting promises the success of the project and the high return on investment. To do this, scammers create a project page, which is only a video or presentation of the project, WhitePaper (at best) and a cryptocurrency wallet for investment. The campaign is widely covered in the media, at conferences. Scammers appeal directly to investors, organizing personal meetings.

Also, scammers use the scheme of hacking the base of addresses of early investors of real projects with the subsequent invitation to early ICO on favorable terms, the purse for transferring funds belongs to scammers.

***Fake cryptocurrency wallets.*** Scammers place fake wallets in popular app stores. Fake wallets are divided in to two categories. The first one is a category where malicious app after launch requests from the user his private key and wallet password. The second one doesn't create new wallet by generating public address and private key. These malicious apps only display attacker's public address without user's access to private key. Private key is owned by the scammer. Once the fake app is launched, user thinks that app already generated his public address where user can deposit his cryptocurrency. If user send his funds to this wallet, he is not able to withdraw them because, he doesn't own private key.

### *B. Technical Schemes*

This type of attack is more labor-intensive but less visible, so the percentage of goal achievement is much higher than in social engineering schemes.

***DNS based phishing***. In this attack, the attacker initially creates a rogue access point and lures the client to connect to the access point where he runs a fake DNS server. This server redirects particular sites to the attacker's phishing server [7,8].

***Session hijacking (cookies hijacking).*** The attack is based on using a valid computer session, sometimes also called a session key, to gain unauthorized access to information or services on a computer system. In particular, it is used to denote the theft of a *cookie* used to authenticate a user on a remote server. A popular method is using source-routed IP packets. This allows an attacker at point B on the network to participate in a conversation between A and C by encouraging the IP packets to pass through B's machine. An attacker can use a "blind" capture with the original routing disabled, sending commands but not seeing the responses to set a password allowing access from somewhere else on the net. An attacker can also be "inline" between A and C using a sniffing program to watch the conversation. This is known as a "man-in-the-middle attack".

***Malware.*** When using phishing based on malware, malware is used to store credentials on the victim computer and send it to the owner, that is, to the phisher. For example, threat can be delivered via malspam messages with an attached doc file that contains a Powershell script which downloads malware. Then it finds stored wallets and credentials and uploads them to the C2 [12]. The number of malicious programs used by attackers is constantly increasing, and the tools themselves are constantly being modified. Among the most frequently used malicious programs are the trojans AZORult and Pony Formgrabber, as well as the bot Qbot. At the same time, cybercriminals continue to use tools that were previously targeted for attacks on banks, and now successfully use them to crack crypto-wallets, wallets and access to personal data of users [22].

***Key / Screen Loggers.*** They are used to steal data when the user inputs information from his device. With the advent of virtual keyboards and touchscreens, screen shots are used, sending them to intruders [15]

TABLE II. Technical schemes

| Scheme | Project | Description |
|---|---|---|
| DNS based | Blockchain.info, MyEtherWallet | Substitution of DNS data, users were targeted at malicious sites |
| Session hijacking | Hardware wallet manufacturer Ledger | Attackers replace the code responsible for creating the recipient's address with its own address, as a result of which all future deposits will be sent to the attacker |
| Malware | North Corean Cryptoexchanges | Hackers from Lazarus Group chatted, posing as "key people" in the crypto currency industry, and during the conversation they published a small piece of code that was actually malware. If the user downloaded this code, the hacker had the opportunity to enter his system and steal the crypto-currencies. |
| Key loggers | Blockchain.info, Electrum wallet | Thousands of Bitcoins were stolen using keyloggers |

## III. ANALISYS

Phishing becomes more common measure for the commission of electronic crimes. According to statistics, the share of phishing emails in the worldwide mail traffic is more than 50%, 15% of unique users and 85% of companies least once encountered a phishing attack [3]. About 80% of the attacks were theft of funds. Most phishing campaigns are short-term, and the number of users who reported timely about the attack is negligible [20]

Every time researchers come up with any idea to detect and prevent phishing, phishers to change their attack strategy, using vulnerabilities found in the current solution. Phishing scams can

be performed either by malware or by social engineering which refers to the use of either fake web pages or emails. Currently, there are no tools to provide 100% protection against phishing attacks, since most of these attacks use the human factor. Due to the fact that the blockchain is a new rapidly developing technology that requires investments, the number of phishing attacks on blockchain projects will increase every year [3,12,14].

The most common mistakes people and companies affected by phishing attacks were:

- insufficient protection of infrastructure;
- go to links from letters to false sites;
- launching malicious scripts from scam messages;
- trust in fraudulent advertising campaigns, promising quick and easy income;
- insufficient level of protection in social networks;
- excessive trust in sites containing SSL certificates;
- insufficient familiarization with the project when investing in ICO;
- failure to use modern methods of protection against phishing attacks (antiviruses, special extensions and add-ons).

## IV. Prevention of Phishing

Protection with blacklisting fraud sites (development of Yandex, Google and other analogues) has long been the only method used in the anti-phishing protection. Modern anti-phishing protection is based on the use of a number of techniques and methods most commonly used with the machine learning and artificial intelligence.

To identify phishing sites, a large number of algorithms are constantly being developed and improved. Most of the existing anti-phishing algorithms are based on the search and comparison of sites with the original: comparing writing and displaying in the address bar of the site name, comparing the content of the site. Such algorithms allow implementing special extensions for browsers that notify users about the unreliability of the site and the likely phishing attack and spam filters in mail boxes. To protect against phishing, the protection of users' passwords is actively used, which uses the storage of passwords not their passwords, but their hashes.

Despite the fact that many companies spend huge amounts of money to study phishing and develop special tools and algorithms for its detection and blocking, there are no tools of providing 100% protection from such attacks. Due to the fact that phishing attacks are mostly carried out with the victim's participation, antiphishing protection methods include a combination of technical and social engineering tools.

TABLE III. Methods of Prevention

| Scheme | Type | Solution | |
|---|---|---|---|
| Social engineering phishing | Fake ICO | Checking projects documentation and site traffic; avoiding risky financial investments | Using bookmarks instead links; the use of browsers with anti-phishing extension, the installation of anti-phishing software, the prohibition of clicking through links and downloading questionable attachments; authentication of the SSL certificate before using the services; inform about phishing, launch off-line copies of cryptowallets, use of two-factor authentication, complex passwords (minimum 14 symbols), refusal of public Wi-Fi, use of secure gateway. |
| | Bloating | | |
| | Pyramids, Ponzi | | |
| | Clones | Protection of mail servers, databases of employees, customers, investors; tracking activity on corporate pages and community pages | |
| | Aimed phishing | | |
| | Social networking | | |
| | Fake cryptowallets | | |
| Technical phishing | DNS based | Develop a DNS alternative, for example, ENS (the Ethereum name service) | |
| | Hijacking | Verify receive and send address | |
| | Malware | Do not open and install attachments | |
| | Key loggers | Monitor processes on task manager of device, check signatures, use on-screen keyboards, password wallets. | |

## Conclusions

Phishing attacks have existed for decades and are used by intruders to steal personal data, finance, important information. Phishing is so universal that it finds application and is successfully implemented even on such new technologies as blockchain, causing distrust to it and hampering their development. Despite the fact that companies are developing anti-phishing protection measures, attackers find vulnerabilities in them and conduct phishing attacks. In the article special attention is paid to social-engineering schemes. Protection from such schemes in most cases is possible only if the security measures and analysis of the information supplied by the user are observed.

From the foregoing, it follows that to repel phishing attacks, one should try to exclude unreasoned actions of users and apply maximum identification and strict filtering of phishing resources, making it impossible to register sites, crypticheIps and other infrastructure elements for phishing purposes. In the near future, it is necessary to create protocols for public documentation of the identity and reliability of purse holders. Such protocols will provide users with protection from phishing attacks at the most fundamental level, eliminating the multiple "point of failure" that are currently threatening individuals who carry out transactions on targets. It is also promising to use artificial intelligence and machine learning to identify and block

phishing resources. The development of alternatives to the DNS and Security Gateway will minimize the attacks of a technical nature. Fraud in the field of blockchain project is facilitated by the unclear position of most states in the field of crypto-currency and ICO. Although the idea of crypto-currency and excludes state intervention, there is a need to determine the positions of states and the adoption of appropriate legislation.

## REFERENCES


[1] Alex Drozhzhin, “Phishing for cryptocurrencies: How bitcoins are stolen”, January 22, 2018, available at “https://www.kaspersky.com/blog/crypto-phishing/20765/”

[2] Suryavanshi, Nirmala, and Anurag Jain. "A Review of Various Techniques for Detection and Prevention for Phishing Attack." International Journal of Advanced Computer Technology (IJACT) ISSN (2013): 2319-7900.

[3] Gudkova D., Vergelis M., Scherbakova T., Demidova M. “Spam and Phishing in 2017”, February 15, 2018, available at: “https://securelist.ru/spam-and-phishing-in-2017/88630/”.

[4] Xudong Zheng “Phishing with Unicode Domains”, April 14, 2017, available at: “https://www.xudongz.com/blog/2017/idn-phishing/”.

[5] Costello, A. Punycode: A bootstring encoding of unicode for internationalized domain names in applications (IDNA). No. RFC 3492. 2003.

[6] Hannay, Peter, and Christopher Bolan. "Assessment of Internationalised Domain Name Homograph Attack Mitigation." Australian Information Security Management Conference. 2009.

[7] Bin, Sun, Wen Qiaoyan, and Liang Xiaoying. "A DNS based anti-phishing approach." 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. IEEE, 2010.

[8] Exploit Db Blog “DNS-Based Phishing Attack in Public Hotspots”, August 14, 2014, available at: “https://www.exploit-db.com/docs/english/20875-dns-based-phishing-attack-in-public-hotspots.pdf”

[9] Lulu Yilun Chen, Yuji Nakamura “Cryptocurrency Cyber Crime Has Cost Victims Millions This Year”, August 24, 2017, available at: “https://www.bloomberg.com/news/articles/2017-08-24/cyber-criminals-extracting-a-heavy-toll-from-ethereum-advocates”

[10] Thomas, Kurt, et al. "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017.

[11] CISCO, “2018 Annual Cybersecurity Report”, available at: “https://www.cisco.com/c/en/us/products/security/security-reports.html”

[12] Artisan Holub, “Protecting ICO’s and cryptocurrency users”, September 27, 2017, available at “https://umbrella.cisco.com/blog/2017/09/27/protecting-icos-cryptocurrency-users/”

[13] Ollmann, Gunter. "The Phishing Guide–Understanding & Preventing Phishing Attacks." NGS Software Insight Security Research,2004.

[14] Chiew, Kang Leng, Kelvin Sheng Chek Yong, and Choon Lin Tan. "A survey of phishing attacks: their types, vectors and technical approaches." Expert Systems with Applications, 2018.

[15] Rajivan, Prashanth, and Cleotilde Gonzalez. "Creative Persuasion: A study on adversarial behaviors and strategies in phishing attacks." Frontiers in psychology 9, 2018.

[16] Prakash, Pawan, et al. "Phishnet: predictive blacklisting to detect phishing attacks." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[17] Jagatic, Tom N., et al. "Social phishing." Communications of the ACM 50.10 (2007): 94-100.

[18] Pearson, Ed, et al. "" To click or not to click is the question": Fraudulent URL identification accuracy in a community sample." Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on. IEEE, 2017.

[19] Gupta, B. B., Nalin AG Arachchilage, and Kostas E. Psannis. "Defending against phishing attacks: taxonomy of methods, current issues and future directions." Telecommunication Systems 67.2 (2018): 247-267

[20] Verizon Enterprise “2018 Data Breach Investigations Report”, 11th edition 2018, available at : “https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf”

[21] U.S Securities and Exchange Comission “Ponzi Schemes Using Virtual Currencies”, available at “https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf”

[22] Group-IB “2018 Cryptocurrency Exchanges. User Accounts Leaks Analysis”, available at ‘https://www.group-ib.com/resources/threat-research/cryptocurrency-exchanges.html/”

[23] Ramzan, Zulfikar. "Phishing attacks and countermeasures." Handbook of information and communication security. Springer, Berlin, Heidelberg, 2010. 433-448.

[24] Andryukhin, A. A. "Methods of protecting decentralized autonomous organizations from crashes and attacks." Труды Института системного программирования РАН, 30.3 2018.

[25] Lucas Stefanko “Fake cryptocurrency wallets found on Play Store”, November 13, 2018 available at “https://lukasstefanko.com/2018/11/fake-cryptocurrency-wallets-found-on-play-store.html”