European Journal of Innovation in Nonformal Education (EJINE)
Volume 4 | Issue 7 | Jul - 2024 ISSN: 2795-8612

Improving Measures to Combat Fraud using Information Technology

Marimboev M. R.
2nd year cadet of the Faculty of Investigative Activities
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Yugay L.Yu.
Doctor of Law, acting professor of the department
Administrative activities of the Department of Internal Affairs of the Academy of the Ministry of Internal Affairs of the Republic

A B S T R A C T
This article highlights a number of problems in cyber fraud investigations. The relevance of the threat of cyber fraud and its scale in the world is revealed. Based on the study of foreign experience and the opinions of scientists, conclusions and proposals for improving this area are formulated.

A R T I C L E I N F O
Article history:
Received 11 May 2024
Received in revised form
10 Jun 2024
Accepted 31 Jul 2024

Keywords: Internet, cybercrime, phishing, vishing, information technology.

Hosting by Innovatus Publishing Co. All rights reserved. © 2024

In the modern world, more and more attention is paid to the development and implementation of information technology in human life, people's lifestyles are moving into a digital format - live communication begins to fade into the background compared to communication on social networks and instant messengers, cash transactions are being replaced by non-cash transactions, online stores are replacing retail outlets. Along with the development of information technology and the implementation of innovative projects based on the use of advanced information technologies that can improve the quality of life of people, the level of crime in the field of information technology, for example, fraud, in particular, is growing. According to research from the University of Maryland, it was found that every 39 seconds hacker attack and of these over the past 20 years, 80% of registered cybercrimes are related to cyber fraud, that is, associated with phishing attacks.[1]

However, today there are a number of problems in investigating and solving crimes in this area. Basically, the main problem when investigating crimes in the field of information technology, including cyber fraud, is the lack of a sufficient number of qualified personnel who understand the field of information technology, sufficient evidence to prove their guilt. Investigators when investigating crimes classify such crimes as provided for in paragraph " d" part 3 of article 168 of the Criminal Code of the Republic of Uzbekistan, that is, fraud using an information system, including information technology. That is, not all investigators have enough knowledge and tools when interrogating criminals. If the investigator does not know the terms used in the information sphere such as (IP, APL, Cloud, MVP, Brandmauer, etc.), he will practically not be able to interrogate the criminal. The above terms are known not only to hackers, but also to a simple attacker who steals money from plastic

[1]Rasulev A.K. Prospects for the development of policy in the field of combating cybercrime in Uzbekistan // Society and Innovation. – 2023. – No. 3. – Volume 4. – P. 126-127.

cards, knowing only the card number and its password; he also requires enormous knowledge in the field of cybernetics. Usually, when talking among themselves, these people use their own terms in the field of information technology, which are not known to everyone. When a detainee accused of cyber fraud is brought in, due to a lack of knowledge in the field of information technology, investigators need the help of specialists. But the problem is that the investigator, without understanding the terms and systems, cannot interrogate the criminal. How can tactics and methods be used during interrogation and other investigative actions in order to prove the guilt or involvement of a person?

Over the last eleven months of 2023, about 5,500 crimes in cyberspace were recorded in Uzbekistan, of which 70% were fraud and theft of funds from bank cards. [2].

Speaking about the relevance of cyber fraud, we can say that the legislation of the Republic of Uzbekistan does not provide for a separate article for cyber fraud. It is a qualifying sign of fraud and is enshrined in paragraph "d" of Part 3, Article 168 of the Criminal Code of the Republic of Uzbekistan.

In addition to the above, it can be noted that in the Republic of Uzbekistan there is no Resolution of the Plenum of the Supreme Court regarding the investigation of cybercrimes, and therefore it causes a double interpretation of the law. It will be necessary to adopt resolutions explaining each type of cybercrime, including fraud using information technology and the Internet, as well as the specifics of their qualification and investigation.

In addition, another reason for committing fraud using information technology is people's insufficient knowledge about information technology, about cyber fraudsters and insufficient ability to use plastic bank cards. At the same time, we can say that cyber fraudsters are good actors and even experienced psychologists who know how to get into character and defraud people of money.

In this regard, to solve these problems, *firstly,* it would be advisable to introduce a training system in the state, improve the qualifications of all investigators in information technology, train them in the technical aspects of investigating cybercrimes with holding exams and issuing them the appropriate certificates of the state standard.

Secondly, if we consider the legislation of the Republic of Uzbekistan, then it should be noted in this area that many scientists note the absence of certain norms in the Criminal Code of the Republic of Uzbekistan. As some experts note, " *the study of the opinions of specialists, foreign legislation and law enforcement practice entails the need to make appropriate changes and additions to the criminal law legislation of the Republic of Uzbekistan: - the inclusion of a new section "Crimes in the field of information technology and security, telecommunications and communications", which will include separate chapters* ; [3]and other experts determine that " *definitions such as cyber theft, cyber fraud must be included in the Plenum of the Supreme Court of the Republic of Uzbekistan "On judicial practice in cases of fraud" for the purpose of a uniform interpretation, qualification and further investigation of this category of criminal cases.* " [4]Joining their opinions, we consider it appropriate to introduce criminal liability for committing cyber fraud as a separate article 168 [1] of the Criminal Code of the Republic of Uzbekistan. Because cyber fraud includes separate subtypes, methods, and subsequently the amount of damage caused may vary. Ways to commit cyber fraud are vishing (using a phone call), phishing (via sending a link), fraudulently obtaining personal data, etc. A clear example of this is the fact that in many states cyber fraud is included in a separate article of the Criminal Code. For example: "theft through the use of computer equipment (Article 212 of the Criminal Code of the Republic of Belarus)" or Article 159.6 of the Criminal Code of the Russian Federation, which provides for criminal liability for fraud in the field of computer information, that is, the theft of someone else's property or the acquisition of rights to someone else's property by entering, deleting, blocking, modifying computer information or other interference in the functioning of means of storing, processing or transmitting computer information or information and telecommunication

[2]Speech by the President of the Republic of Uzbekistan Sh. Mirziyoyev on the topic of development of the IT industry in Uzbekistan December 20, 2023 URL : https://t.me/Press_Secretary_Uz/3651 (access date: 04/20/2024).

[3] Yugay L.Yu Improving criminal law policy in the field of combating cybercrime in the Republic of Uzbekistan – Defender of the Fatherland.;//No. 16/2023.; C 308-309

[4]Sabyrbaeva.A Electronic evidence as a new type of evidence in the investigation of modern forms of fraud – Reviewoflawsciences .; //No. S 2020.; C 218-219;

networks, as well as Resolution of the Plenum of the Supreme Court of the Russian Federation dated December 15, 2022 N 37 "On some issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet. In this case, the main object is property relations, regardless of its form, and an additional object is legal relations ensuring information security. When making changes to the Criminal Code and highlighting cyber fraud as a separate article, it is necessary to adopt a new Resolution of the Plenum of the Supreme Court of the Republic "On judicial practice in cases of cyber fraud " or " cyber crimes ", which will allow investigators to correctly qualify and investigate cyber fraud.

Thirdly, before revealing and investigating a crime committed, we must pay special attention to their prevention. At the same time, people's knowledge in the field of information technology should first be increased, after which people themselves can protect themselves from such criminal attacks. Basic knowledge in the field of IT is taught in schools, lyceums and higher educational institutions, and graduates possess only this. But this is not enough to prevent crimes of this type; people must know how to commit them, what deceptions attackers use when contacting people. Crimes in the field of information technology also include cyber attack, cyber theft, computer sabotage, modification of computer information, **violation of legislation in the field of circulation of crypto assets,** including cyber fraud, etc.

For this reason, if we need to raise the level of people in this area, then we must start this first of all, from school. It would also be purposeful to introduce in schools a new subject, the basics of cybersecurity, which would teach all students to be careful when handling the Internet and encourage them to be vigilant. If you look at the criminological aspect of this type of crime, you can see that the bulk of victims of cyber fraud are elderly people who do not have information literacy in this area and minor teenagers who use the Internet. These people are not well versed in the ways of committing fraud using information technology. Therefore, it will be necessary to inform people about the types and methods of committing them, increase the number of banners on the streets calling on people to be vigilant, and show various videos on all TV channels providing information about cyber fraudsters. But not all people can pay attention to these preventive measures, as a result of which they may become victims of crime. Because of this, in order to interest all people, it will be purposeful to create very interesting films or TV series about cybercriminals, cyber fraudsters, and with this method we can inform the population about the methods and types of cyber fraud.

Conclusion:

Based on all the opinions proposed above, the implementation of the proposed legal remedies, countermeasures and propaganda work makes it possible to increase the efficiency of law enforcement activities and the detection of cyber fraud by curbing its spread, exposing criminals and introducing new norms in criminal legislation. We can say that cyber fraud is a type of crime that can be countered through the use of organizational, legal, social, technical and methodological measures.

References:

1. Fadina Yu. P. Criminal legal characteristics of fraud on the Internet // Bulletin of the Yugra State University. 2017. No. 1 (44). pp. 117-121.
2. Kuli-Zade T. A. Problems of qualification of fraud in the field of computer information. 2019. - [Electronic resource] - Mode access : https://urfac.ru/?p=2165 .
3. Speech by the President of the Republic of Uzbekistan Sh. Mirziyoyev on the topic of development of the IT industry in Uzbekistan December 20, 2023 URL : https://t.me/Press_Secretary_Uz/3651 (access date: 04/20/2024).
4. Rasulev A.K. Prospects for the development of policy in the field of combating cybercrime in Uzbekistan // Society and Innovation. – 2023. – No. 3. – Volume 4. – P. 126-127.
5. Yugay L.Yu. Improving criminal law policy in the field of combating cybercrime in the Republic of Uzbekistan // Defender of the Fatherland. – 2023. – No. 16. pp. 308-309.
6. Sabyrbaeva A.B. Electronic evidence as a new type of evidence in the investigation of modern forms of fraud. // Review of law sciences. – 2020. – Special issue. – pp. 218-219.

7. Williams EJ, and Joinson AN Developing a measure of information seeking about phishing // Journal of Cybersecurity. 2020. Vol. 6.No. 1. R. 13.
8. Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu. Investigating phishing victimization with the Heuristice Systematic Model: A theoretical framework and an exploration. Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA. URL: http://dx.doi.org/10.1016/j.cose.2012.12.003
9. Resolution of the Plenum of the Supreme Court of the Russian Federation dated December 15, 2022 N 37 "On some issues of judicial practice in criminal cases involving crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet https://www. vsrf.ru/documents/own/?category=resolutions_plenum_supreme_court_russian (Date of access: 04/20/2024).
10. Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan, dated June 23, 2023 No. 17 "On judicial practice in cases of fraud" https://lex.uz/uz/docs/6523584 . (Date of access: 04/30/2024).