ISSN: 2775-5118 VOL.3 NO.10 (2024) I.F. 9.1

THE SOCIAL NECESSITY OF PREVENTING CYBER FRAUD CRIMES

Sh.S.Mirzajonov,
independent researcher.

Abstract: This article provides a scientific analysis of the social necessity of preventing cyber fraud crimes and their growing threat to public security. The author explores the legal and social essence of cyber fraud, identifies its modern forms, dynamics, and underlying causes. Special attention is paid to the role of legal culture and digital literacy in combating cybercrime, as well as to the importance of strengthening cooperation between state institutions and civil society. Summarizing the theoretical views of scholars, the author emphasizes the existing challenges in the national system of cybercrime prevention and proposes practical measures for their elimination. In particular, the article recommends adopting a state program on cyber fraud prevention, introducing digital literacy courses in educational institutions, and expanding international cooperation with global cybersecurity organizations.

Keywords*:* Cyber fraud, prevention, social necessity, information security, legal culture, digital literacy, National Guard, law enforcement agencies, cybersecurity, legal awareness, international cooperation.

In recent years, along with the rapid development of information technologies, the expansion of Internet services, and the formation of the digital economy, cyber fraud crimes have been rapidly increasing all over the world. Cyber fraud is a category of crimes committed with the purpose of deceiving an individual or organization, unlawfully obtaining the data of an interested person, or gaining material benefit through illegal means [1].

This type of crime threatens not only economic security but also the legal, moral, and informational stability of the state and society. Therefore, the social necessity of preventive measures in combating cyber fraud is steadily increasing.

The main feature of cyber fraud crimes is that they are committed in a very short time, and it is difficult to detect the traces of such crimes. At present, they manifest themselves in the following forms: stealing personal data through phishing and spoofing, illegal interference in online payment systems, obtaining bank card information, and exerting psychological influence and manipulation through social networks [2].

ISSN: 2775-5118 VOL.3 NO.10 (2024) I.F. 9.1

According to the UN "Cybercrime Trends Report" of 2023, cyber fraud accounts for one in every four cybercrimes worldwide and, by 2024, may cause economic losses of 10.5 trillion US dollars to the global economy [3].

In Uzbekistan, law enforcement reports have noted that in recent years, this type of crime has increased by 2.5 times [4]. The issue of preventing cyber fraud crimes has been widely studied by both foreign and local scholars. According to A.I.Gurov, "one of the most dangerous forms of modern crime is fraud committed through manipulation of the information environment" [5].

His position underscores that cyber fraud is not merely a technical offense but a complex socio-psychological phenomenon that exploits human trust, information dependency, and the weaknesses of digital communication systems. Gurov's emphasis on the decisive role of legal education and preventive measures in combating such crimes highlights the necessity of proactive strategies rather than reactive law enforcement responses.

He also emphasized the priority importance of legal education and preventive measures in the fight against cybercrime. P. Barry and R. Clarke, in their research, explain that the main causes of cyber fraud are "human factors and the lack of digital literacy" [6].

Their approach expands the criminological framework by linking technological vulnerability to the broader context of social behavior and information culture. In other words, cybercrime prevention cannot be confined solely to improving technical infrastructure—it must involve the formation of responsible online behavior and public awareness.

Among Uzbek scholars, Sh.E. Ergashev believes that "the basis for effective combating of cyber fraud is the systematic organization of prevention at the levels of the state, education, and public institutions" [7].

His argument integrates the sociological and institutional dimensions of prevention, emphasizing intersectoral cooperation as a prerequisite for building cyber resilience in society.

From the author's analytical standpoint, these theoretical positions complement each other and collectively define the multidimensional essence of cyber fraud prevention. Gurov's criminological interpretation, Barry and Clarke's behavioral approach, and Ergashev's institutional concept together suggest that combating cyber fraud requires a comprehensive national model that simultaneously strengthens legislation, promotes digital literacy, and enhances public participation in ensuring cybersecurity.

According to the author, summarizing these theoretical approaches, the main direction in combating cyber fraud crimes should be aimed at raising the legal consciousness and information culture of society.

ISSN: 2775-5118 VOL.3 NO.10 (2024) I.F. 9.1

From the author's point of view, the social necessity of preventing cyber fraud can be explained by the following factors:

First, the need to ensure human rights and the security of personal data. Cybercrimes directly threaten the personal inviolability of individuals.

Second, ensuring the stability of the national economy. Cyberattacks against the banking and financial systems cause serious harm to economic security.

Third, creating an environment of digital trust in society. Ensuring information security increases the public's confidence in state and banking systems.

Fourth, strengthening information hygiene among youth, which can help reduce the tendency toward committing crimes.

The author also emphasizes the necessity of institutionalizing cooperation between the National Guard, the Ministry of Internal Affairs, and the Ministry of Information Technologies in strengthening the preventive system. In this direction, it is considered expedient to make use of international experience — particularly the Singaporean and Estonian models [8].

There are a number of problems in Uzbekistan in the field of preventing cyber fraud crimes:

- low public awareness regarding cybersecurity;
- the lack of special courses on digital literacy in educational institutions;
- a shortage of qualified personnel in the investigation of cybercrimes;
- insufficient integration of interdepartmental information exchange systems;
- the absence of clearly defined preventive activities in legislation.

These shortcomings negatively affect the effectiveness of crime prevention efforts. According to our opinion, in order to eliminate these problems, the following proposals should be implemented:

1. To adopt a separate state program on the prevention of cyber fraud, in which measures aimed at improving the population's digital literacy and raising legal awareness should be specified.

2. To clarify the relevant articles of the Administrative Liability Code and the Criminal Code, and to legally define the concept of "cyber fraud."

3. To conduct preventive media campaigns among youth — to regularly organize legal and educational events under the slogan "Cybersecurity — My Responsibility."

4. To strengthen international cooperation, in particular by holding practical training sessions jointly with the UN, OSCE, INTERPOL, and European Union cyber law platforms.

ISSN: 2775-5118 VOL.3 NO.10 (2024) I.F. 9.1

5. To expand the activities of the National Cybersecurity Center and to establish a laboratory under it for monitoring crimes.

Preventing cyber fraud crimes is not only the duty of law enforcement bodies but also an integral part of the process of forming the legal culture of the whole society. Preventive measures are an important guarantee of ensuring social security, protecting citizens' personal data, and maintaining the stability of the digital economy. Therefore, cooperation between the state, the public, and educational institutions in this field has strategic importance.

References

1. UNODC. Global Report on Cybercrime. New York: United Nations Publications, 2023.
2. Clarke, R. Cybercrime and Society. London: Sage Publications, 2020.
3. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva, 2024.
4. Ministry of Internal Affairs of the Republic of Uzbekistan. Statistical Data on the State of Crime (2024). Tashkent, 2024.
5. Gurov, A.I. Criminology: Textbook for Universities. Moscow: Yurayt, 2022.
6. Barry, P., & Clarke, R. Human Factors in Cybercrime. Oxford: Oxford University Press, 2021.
7. Ergashev, Sh.E. Cyber Fraud and Problems of Its Prevention. Tashkent: Academy of Legal Sciences, 2023.
8. Cyber Security Agency of Singapore. National Cybersecurity Strategy 2022. Singapore, 2022.