Vol.4 N.1 (2026)
science-conference.com

CRIMINOLOGICAL CHARACTERISTICS OF CYBER FRAUD AND THE LEGAL MECHANISMS FOR ITS PREVENTION

Avazbek Sayfiddinov
Tashkent State University of Law

ABSTRACT

This article analyzes the criminological characteristics of cyber fraud in the context of the rapid development of digital technologies, the methods by which it is committed, the specific characteristics of offenders and victims, as well as the legal and organizational mechanisms for preventing such crimes. The criminal-law foundations of cyber fraud in the Republic of Uzbekistan, in particular Article 168 of the Criminal Code and the provisions of the Law "On Cybersecurity," are examined from a comparative legal perspective. In addition, the European Union's strong customer authentication mechanism, the United Kingdom's mechanism for reimbursing victims of fraud, and international cooperation standards under the Budapest Convention are compared with the practice of Uzbekistan. The study substantiates that an approach based solely on punishment is insufficient for combating cyber fraud and emphasizes the need to strengthen mechanisms for rapid information exchange among banks, telecommunications operators, law enforcement agencies, payment organizations, and digital platforms, as well as mechanisms for the immediate blocking and recovery of victims' funds.

KEYWORDS

cyber fraud, cybercrime, criminological characteristics, phishing, social engineering, bank cards, digital evidence, cybersecurity, prevention, electronic payments, international cooperation.

INTRODUCTION

The expansion of the digital economy is accelerating financial transactions and creating new opportunities for citizens and entrepreneurs. Yet digitalization also has a darker side: traditional forms of crime have migrated into cyberspace and are now being committed through new methods and instruments. Cyber fraud, in particular, is spreading widely through the exploitation of citizens' bank cards, electronic payment systems, social media accounts, and personal data. In Uzbekistan, the scale of this problem has become especially serious. According to the Ministry of Internal Affairs, in 2019, 863 crimes of 18 types committed using information technologies were recorded, whereas in 2024, 58,800 cybercrimes of 62 types were recorded. In 2024, the share of cybercrime in overall crime reached 44.4 percent, with 98 percent of these offenses consisting of cyber theft and cyber fraud linked to bank cards (Ministry of Internal Affairs of the Republic of Uzbekistan, 2024). According to data presented in March 2026, 82 percent of fraud offenses committed last year were carried out in cyberspace (President of the Republic of Uzbekistan, 2026).

These figures demonstrate that cyber fraud must be studied not as ordinary "online fraud" but as an independent criminological and legal problem. Its danger is not defined solely by the material damage caused. The transnational nature of the offense, the anonymity of the perpetrator, the rapid alteration of digital traces, the potential for psychological manipulation of the victim, and the transfer of criminally obtained funds across multiple accounts within seconds distinguish it significantly from traditional fraud. From a criminological standpoint, cyber fraud can be characterized as an intentional crime committed through information and communication tools in cyberspace, aimed at acquiring a person's property or property rights through deception or abuse of trust.

Article 168 of the Criminal Code of the Republic of Uzbekistan defines fraud as the acquisition of another's property or property rights through deception or abuse of trust. Part three of this article specifically identifies the commission of fraud using an information system, including information technologies, as an aggravating qualifying circumstance (Criminal Code of the Republic of

Uzbekistan, Art. 168). The existing criminal-law model thus treats cyber fraud not as an independent, freestanding offense but as a qualified form of fraud committed with the use of information technologies. The advantage of this approach is that it preserves the core legal essence of fraud. However, given the distinctive nature of the digital environment, focusing solely on the elements of the offense and the applicable punishment is not sufficient. Preventing cyber fraud also requires identifying its criminological mechanism. The most common methods of cyber fraud include phishing links, impersonation of a bank employee or a law enforcement officer, obtaining SMS codes or one-time passwords, distributing malicious software, fake online stores, fraudulent investment and loan offers, fake social media accounts, and deception on online trading platforms.

Statistical data from Uzbekistan's practice confirm this conclusion. In 2024, 60 percent of cybercrimes were committed by gaining control over a bank card or mobile device through malicious links and software, while 16 percent were committed by obtaining SMS codes and account-management information through deception (Cybersecurity Center under the Ministry of Internal Affairs of the Republic of Uzbekistan, 2024). This shows that cyber fraud relies more on the human factor than on technical means. Accordingly, alongside the offender's technical knowledge, the ability to psychologically manipulate the victim occupies an important place in the criminological profile of cyber fraud. Offenders frequently exploit the victim's fear, urgency in decision-making, financial interest, or trust in an official figure. In other words, at the center of modern cyber fraud lies not "technology" itself but the mechanism of "controlling human behavior through technology."

A one-sided approach to the victim profile is likewise mistaken. Cyber fraud does not harm only individuals with low digital literacy. Because fraudsters increasingly employ professional social-engineering techniques, even technically literate users may fall victim to manipulation. For this reason, reducing preventive measures to the notion that "citizens should simply be careful" is neither scientifically nor practically sufficient.

Uzbekistan's system for combating cybercrime is built upon several legal foundations. First, Article 168 of the Criminal Code establishes the direct basis for criminal liability for cyber fraud (Criminal Code of the Republic of Uzbekistan, Art. 168). The second important legal source is the Law "On Cybersecurity," No. O'RQ-764, of 15 April 2022 (Law of the Republic of Uzbekistan No. O'RQ-764, 2022). This Law treats the prevention of cybercrime not merely as law-enforcement activity carried out after an offense has occurred, but as a comprehensive activity encompassing cyber defense, the detection of cybersecurity incidents, the elimination of their consequences, and the maintenance of information system stability. By legally defining concepts such as cybercrime, cyberattack, cyber defense, and cybersecurity incident, the Law has created a unified terminological framework for this field (Law of the Republic of Uzbekistan No. O'RQ-764, 2022).

At the same time, an important weakness of the existing system is that the legal mechanisms for preventing cyber fraud are, in most cases, directed toward identifying and punishing the offender after the fact. Yet in cyber fraud, the time factor is of decisive importance. For instance, once funds have been unlawfully withdrawn from a citizen's bank card, blocking the suspicious transaction within the first few minutes yields far greater preventive effect than identifying the offender over the course of several months. From this standpoint, it would be worthwhile for Uzbek legislation to further improve clear, unified algorithms for banks and payment organizations to detect suspicious transactions, temporarily suspend them, promptly review victims' complaints, and return funds.

International experience shows that in developed countries, the prevention of cyber fraud rests on three principal directions: prior detection, rapid intervention, and international cooperation.

Within the European Union, "strong customer authentication" has been

introduced under PSD2, requiring that certain electronic payments be confirmed through at least two different authentication elements (Directive (EU) 2015/2366 [PSD2], 2015, Art. 97). A joint 2025 report by the EBA and the ECB noted that this mechanism has been effective in reducing fraud based on the

theft of authentication credentials, but that fraudsters are increasingly shifting toward manipulating the user directly (European Banking Authority & European Central Bank, 2025). This experience yields an important conclusion for Uzbekistan: authentication through an SMS code alone is not a sufficient security guarantee. Biometric authentication, device identification, transaction-behavior analysis, and risk-based monitoring systems need to be expanded.

The United Kingdom's experience points to an even more significant dimension. Beginning on 7 October 2024, the country introduced a mandatory mechanism for reimbursing victims in certain cases of Authorised Push Payment (APP) fraud. This system incentivizes banks and payment service providers not only to assist customers after harm has occurred, but also to detect fraud in advance (Payment Systems Regulator, 2025).

In addition, the United Kingdom also provides for the possibility of briefly delaying the execution of a suspicious payment for further verification. In other words, the underlying philosophy of the system is not "the funds are gone — now we search for the offender," but rather "we identify the risk before the funds are lost" (Payment Services Regulations 2024, Explanatory Memorandum).

Introducing precisely this approach would be of great practical value for Uzbekistan. However, rather than fully transplanting the UK model, it should be adapted to the local banking system and payment infrastructure. In particular, a compensation mechanism could be developed that separately assesses the degree of care exercised by the bank, the payment organization, and the customer in a given case of fraud. The transnational nature of cybercrime requires a distinct mechanism of international cooperation. The Council of Europe's Budapest Convention provides not only for the criminalization of cybercrime but also procedural mechanisms for obtaining and preserving electronic evidence and for international cooperation (Council of Europe, 2001). Its Second Additional Protocol is aimed at further strengthening cross-border access to electronic evidence and cooperation with service providers (Council of

Europe, 2022). The significance of this experience for Uzbekistan lies in the fact that in cyber fraud, the offender, the victim, the bank account, the server, and the electronic evidence may all be located in different countries. Under such conditions, acting solely within the bounds of national jurisdiction significantly limits the ability to promptly expose the crime.

CONCLUSION

Cyber fraud is one of the negative consequences of the process of digital transformation, its danger determined by the relative ease with which the offense can be committed, the breadth of the potential victim pool, its transnational character, and the rapid loss of digital evidence. The fact that 58,800 cybercrimes were recorded in Uzbekistan in 2024, 98 percent of which were related to bank cards, demonstrates that this problem is systemic in nature (Ministry of Internal Affairs of the Republic of Uzbekistan, 2024).

Although Article 168 of the Criminal Code of the Republic of Uzbekistan covers fraud committed with the use of information technologies as a qualifying circumstance, preventing modern cyber fraud cannot be resolved through the strengthening of criminal liability alone. On the contrary, effective prevention must be shifted to the stage preceding the commission of the offense. Based on the findings of this study, the following proposals are put forward: first, to create a unified, rapid platform for exchanging cyber-fraud indicators among banks, payment organizations, telecommunications operators, and law enforcement agencies; second, to introduce a legal mechanism for the automatic detection and brief delay of suspicious transactions; third, to clearly define banks' liability and procedures for reimbursing funds to victims of cyber fraud; fourth, to develop mechanisms for the rapid preservation and international exchange of digital evidence; and fifth, to raise the population's cyber-legal literacy through practical, scenario-based methods. Thus, the most suitable model for Uzbekistan is an integrated system of cyber-fraud prevention that combines punitive, technical, and organizational mechanisms. International experience — in particular, the European Union's strong-authentication model, the United Kingdom's victim-compensation and payment-delay mechanisms, and the electronic-evidence and international-cooperation standards under the

Budapest Convention — can serve as an important methodological foundation for improving the national system.

REFERENCES

1. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. https://www.coe.int/en/web/cybercrime/convention-on-cybercrime

2. Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224).

3. Criminal Code of the Republic of Uzbekistan, Art. 168 (Fraud).

4. Cybersecurity Center under the Ministry of Internal Affairs of the Republic of Uzbekistan. (2024). Data on the structure of cybercrime.

5. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2), Art. 97.

6. European Banking Authority & European Central Bank. (2025, December 15). Joint EBA-ECB report on payment fraud.

7. Law of the Republic of Uzbekistan No. O'RQ-764. (2022, April 15). On Cybersecurity.

8. Ministry of Internal Affairs of the Republic of Uzbekistan. (2024). Statistics on the dynamics of cybercrime, 2019–2024. https://gov.uz/oz/iiv/news/view/52319

9. Payment Services Regulations 2024 (UK), Explanatory Memorandum.

10. Payment Systems Regulator (United Kingdom). (2025). Annual report and accounts 2024/25.

11. President of the Republic of Uzbekistan. (2026, March 12). Combating organized crime and cybercrime to be strengthened. https://president.uz/oz/lists/view/9009