European Journal of Interdisciplinary Research and Development
Volume- 46 December- 2025
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

PREVENTING CYBER FRAUD AMONG YOUNG PEOPLE AND BUILDING A CULTURE OF DIGITAL SECURITY IN UZBEKISTAN

Turg‘unova Shodiya Shuhratjon qizi
Senior Consultant, Department of Justice of Namangan Region
shodiya0506@icloud.com

Abstract

Background: The rapid digitalisation of payments and public services has been accompanied by an explosive growth of cybercrime. In Uzbekistan, cybercrime accounted for almost half of all registered crimes in 2025, and the overwhelming majority of cases involve fraud and theft through bank cards and electronic payment systems. Young people are among the most active users of digital services and, for this reason, both frequent victims and potential participants in fraud schemes.

Aim: The article analyses the legal and organisational measures for preventing cyber fraud among young people in Uzbekistan and substantiates the concept of a culture of digital security as the basis of prevention.

Methods: The study combines doctrinal analysis of national legislation and recent policy measures, comparative analysis against international instruments (the UN Convention against Cybercrime, the OECD Recommendation on Children in the Digital Environment), descriptive analysis of official law enforcement data, and a review of criminological research on online fraud victimisation.

Results: The number of cybercrimes increased about elevenfold over five years, exceeding 62,000; losses in 2025 alone reached 1.9 trillion soums, and 96 per cent of cases involved electronic payment systems. The state has responded with stricter responsibility of banks and payment organisations, mechanisms for detecting suspicious transfers, specialised cybercrime units and awareness campaigns, and in 2026 the number of fraud complaints declined for the first time in several years. Gaps remain in the low detection rate, the involvement of young people as “money mules”, the absence of systematic digital safety education and limited support for victims.

Conclusion: The article proposes a national programme on digital security culture for young people, mandatory digital safety modules in education, legal measures against the recruitment of young people as money mules, rapid card-blocking and refund procedures, and support services for victims.

Keywords: Cyber fraud; cybercrime; young people; digital security; digital literacy; money mules; social engineering; Uzbekistan.

Introduction

Digital technologies have transformed everyday life: payments, education, employment and access to public services increasingly take place online. This transformation has also created new opportunities for crime. Fraud has migrated online, where offenders can reach thousands

of potential victims at minimal cost, conceal their identity and operate across borders. In the United States alone, the FBI's Internet Crime Complaint Center recorded reported losses of about 16.6 billion US dollars in 2024.[1] At the global level, the UN General Assembly adopted the United Nations Convention against Cybercrime in December 2024, the first universal treaty in this field.[2]

Uzbekistan illustrates both the benefits and the risks of rapid digitalisation. The number of internet users reached 31 million in 2024, and the country has expanded electronic payments and public services at high speed.[3] At the same time, cybercrime has become the leading category of crime. According to the Ministry of Internal Affairs, cybercrimes accounted for 42 per cent of all crimes in the first half of 2025 and 49.6 per cent for the year as a whole.[4,5]

Young people occupy a special position in this problem. They are the most active users of mobile banking, social networks and online marketplaces, which makes them frequent targets of fraud. At the same time, young people with limited income may be recruited, sometimes unknowingly, to provide their bank cards or SIM cards to criminals, becoming participants in fraud schemes. Criminological research shows that online fraud relies on social engineering, which exploits trust, urgency and emotion rather than technical vulnerabilities.[6,7] Prevention therefore requires not only technical and legal measures but also a culture of digital security.

The aim of this article is to analyse the legal and organisational measures for preventing cyber fraud among young people in Uzbekistan and to substantiate the concept of a culture of digital security as the basis of prevention. The research question is whether current measures address the specific vulnerabilities of young people as both victims and potential participants in cyber fraud.

Methods

Doctrinal analysis: The study examined the Criminal Code (Article 168 on fraud and related provisions), the Law "On Cybersecurity" of 15 April 2022, and policy measures adopted in 2025–2026 on the responsibility of banks and payment organisations and on the prevention of cybercrime.

Comparative analysis: National measures were compared with the UN Convention against Cybercrime[8] and the OECD Recommendation on Children in the Digital Environment.[9]

Descriptive analysis of official data: Data of the Ministry of Internal Affairs presented at press events, parliamentary hearings and in media reports for 2024–2026 were analysed.

[1] Federal Bureau of Investigation, Internet Crime Complaint Center. Internet Crime Report 2024. Washington, DC: FBI, 2025.
[2] United Nations General Assembly. United Nations Convention against Cybercrime. Resolution 79/243, 24 December 2024.
[3] Digital transformation of Uzbekistan promotes regional integration in Central Asia // Embassy of the Republic of Uzbekistan in Austria. URL: https://usbekistan.at/?p=2958.
[4] Spot.uz. Material on cybercrime statistics. 9 July 2025. URL: https://www.spot.uz/oz/2025/07/09/cybercrime/.
[5] Spot.uz. Report on the Senate session on cybersecurity. 16 June 2026. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.
[6] Button M., Cross C. Cyber Frauds, Scams and their Victims. London: Routledge, 2017.
[7] Whitty M.T. The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam // British Journal of Criminology. 2013. Vol. 53, No. 4. P. 665–684.
[8] United Nations General Assembly. United Nations Convention against Cybercrime. Resolution 79/243, 24 December 2024.
[9] OECD. Recommendation of the Council on Children in the Digital Environment. OECD/LEGAL/0389. 2021.

Literature review: Criminological research on online fraud, social engineering and victimisation was reviewed.[10,11]

Limitations: Official data are not disaggregated by the age of victims and offenders in published sources; conclusions about young people are therefore based on general data, research findings and policy documents.

Results

The scale of cyber fraud: The growth of cybercrime in Uzbekistan has been extremely rapid. In 2024 the number of cybercrimes increased 9.1 times compared with 2023.[12] Over five years the number of cybercrimes increased about elevenfold and exceeded 62,000, with total damage of 3.73 trillion soums; in 2025 alone, citizens lost 1.9 trillion soums as a result of cybercrime.[13] According to the head of the Cybercrime Department of the Ministry of Internal Affairs, speaking in the Senate in June 2026, the number of types of cybercrime grew from 18 to 64 between 2021 and 2025, and 96 per cent of cases involved cyber theft and cyber fraud through electronic payment systems.[14] Earlier data showed that about 98 per cent of cybercrimes were connected with bank cards.[15]

Detection remains a serious problem. In January 2026 the President criticised the low effectiveness of the fight against cybercrime, noting that in the capital the number of cybercrimes exceeded 16,000 in the previous year, citizens lost almost 2 trillion soums, and the detection rate did not reach 8 per cent.[16]

Policy response: The state response has developed in several directions. First, the responsibility of financial institutions was strengthened: where fraud occurs due to the negligence of banks or payment services, the damage is to be compensated at their expense, and the owners of bank cards and SIM cards used in crimes may also be held responsible.[17] The Ministry of Internal Affairs introduced the practice of publishing a list of banks and payment organisations with the highest number of cybercrimes.[18] Second, a mechanism for detecting suspicious transfers at the Central Bank was developed, with data transmitted to the Ministry of Internal Affairs through an electronic data exchange system.[19] Third, specialised units were established, including a Cybersecurity Centre and a Cybercrime Department of the Ministry of Internal Affairs.[20,21]

[10] Button M., Cross C. Cyber Frauds, Scams and their Victims. London: Routledge, 2017.
[11] Whitty M.T. The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam // British Journal of Criminology. 2013. Vol. 53, No. 4. P. 665–684.
[12] Spot.uz. Report on the press tour of the Cybercrime Centre of the Ministry of Internal Affairs. 29 May 2025. URL: https://www.spot.uz/oz/2025/05/29/cybercrime/.
[13] Spot.uz. Material on cybercrime results of 2025. 27 January 2026. URL: https://www.spot.uz/oz/2026/01/27/cybercrime/.
[14] Spot.uz. Report on the Senate session on cybersecurity. 16 June 2026. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.
[15] Ministry of Internal Affairs of the Republic of Uzbekistan. Press tour for the media dedicated to the activities of the Cybersecurity Centre of the Operational Search Department. 29 May 2025. URL: https://gov.uz/oz/iiv/news/view/57775.
[16] Spot.uz. Material on cybercrime results of 2025. 27 January 2026. URL: https://www.spot.uz/oz/2026/01/27/cybercrime/.
[17] Spot.uz. Report on the press tour of the Cybercrime Centre of the Ministry of Internal Affairs. 29 May 2025. URL: https://www.spot.uz/oz/2025/05/29/cybercrime/.
[18] Ministry of Internal Affairs of the Republic of Uzbekistan. Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish. 7 May 2025. URL: https://gov.uz/oz/iiv/news/view/52319.
[19] Ministry of Internal Affairs of the Republic of Uzbekistan. Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish. 7 May 2025. URL: https://gov.uz/oz/iiv/news/view/52319.
[20] Spot.uz. Report on the Senate session on cybersecurity. 16 June 2026. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.
[21] Ministry of Internal Affairs of the Republic of Uzbekistan. Press tour for the media dedicated to the activities of the Cybersecurity Centre of the Operational Search Department. 29 May 2025. URL: https://gov.uz/oz/iiv/news/view/57775.

Fourth, awareness campaigns were launched. In November 2025 the Ministry of Internal Affairs announced a "Month of raising cyber culture" aimed at informing citizens about safe behaviour online.[22] A nationwide information campaign was conducted jointly by the "Adolat" Social Democratic Party, the Ministry of Justice, the Ministry of Internal Affairs and the Association of Mahallas.[23] According to data presented by the Ministry of Internal Affairs in the Senate in June 2026, the number of fraud complaints declined for the first time in several years, by 6 per cent or about 2,500 complaints.[24]

Young people as victims and participants: Two patterns are particularly relevant for young people. As victims, young people are targeted through fake online shops, fraudulent job and scholarship offers, investment and "quick earnings" schemes, fake prize draws and requests to share one-time passwords. As participants, young people may be persuaded to sell or "rent" their bank cards or SIM cards, or to receive and transfer money for a reward. Such persons, often called "money mules", allow organisers to conceal the movement of stolen funds. Strengthened responsibility for card and SIM card owners used in crimes makes this pattern legally dangerous for young people who may not understand the consequences.[25]

The public debate has also highlighted the social consequences of fraud. Commenting on the death of a woman in Namangan who had been deceived by fraudsters, Saida Mirziyoyeva, then a member of the Republican Commission on Gender Equality, argued that the state should help victims of fraud and called on deputies to strengthen social protection for those who are helpless and deceived.[26]

Table 1. Main indicators and measures against cyber fraud in Uzbekistan

Indicator or measure	**Data or content**
Share of cybercrime in all crimes	42% (first half of 2025); 49.6% (2025)
Growth of cybercrime	9.1 times (2024 vs 2023); about 11 times over five years, over 62,000 crimes
Losses	1.9 trillion soums (2025); 3.73 trillion soums over five years
Main method	96–98% via bank cards and electronic payment systems
Measures	Responsibility of banks and payment organisations; suspicious-transfer detection; specialised units; awareness campaigns
First result	Fraud complaints down 6% (reported in June 2026)

[22] O'zbekistonliklar so'nggi besh yilda kiberfiribgarliklarga 159 million dollar yo'qotgan // Zamin.uz. November 2025. URL: https://zamin.uz/uz/ozbekiston/166748-ozbekistonliklar-songgi-besh-yilda-kiberfiribgarliklarga-159-million-dollar-yoqotgan.html.

[23] Ministry of Internal Affairs of the Republic of Uzbekistan. Kiberjinoyatchilik — dolzarb muammo. URL: https://gov.uz/oz/iiv/news/view/137374.

[24] Spot.uz. Report on the Senate session on cybersecurity. 16 June 2026. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.

[25] Spot.uz. Report on the press tour of the Cybercrime Centre of the Ministry of Internal Affairs. 29 May 2025. URL: https://www.spot.uz/oz/2025/05/29/cybercrime/.

[26] "The State should help victims of fraud" – Saida Mirziyoyeva comments on the suicide case in Namangan // Kun.uz. URL: https://kun.uz/en/87070659.

Sources: Ministry of Internal Affairs data reported in official and media sources.[27,28,29,30]

Discussion

Why technical and punitive measures are not enough: The low detection rate shows the limits of a purely law-enforcement response. Online fraud is often committed from abroad, through chains of cards and accounts, and funds are withdrawn within minutes. Even with improved detection, many victims will not recover their money. Prevention is therefore more effective than investigation. Research on online fraud shows that offenders use persuasion techniques, such as creating a sense of urgency, authority or exclusive opportunity, that work against people regardless of their technical knowledge.[31,32] Effective prevention requires people to recognise these techniques and to adopt safe habits.

The concept of a culture of digital security: A culture of digital security can be understood as a set of knowledge, attitudes and habits that enable a person to use digital services safely: protecting personal data and one-time passwords, verifying information before acting, recognising manipulation, knowing where to report fraud and refusing to participate in suspicious schemes. For young people, this culture should be formed systematically through education rather than through occasional campaigns. The OECD Recommendation on Children in the Digital Environment calls on states to promote digital literacy as an essential part of education and to ensure safety-by-design in digital services.[33]

Gaps: (1) Education: Digital safety is not yet a systematic component of school, lyceum and university curricula. The success of mass digital skills programmes, such as the “One Million Uzbek Coders” project, which trained more than 1.2 million young people,[34] shows that large-scale educational initiatives are feasible.

(2) Money mules: Young people need clear information that transferring their cards or SIM cards to others is unlawful, and there should be preventive measures, such as warnings and education, before punishment.

(3) Rapid response: Victims need a single fast channel to block cards and suspicious transfers within minutes. The data exchange between the Central Bank and the Ministry of Internal Affairs is an important basis, but it should be complemented by a 24-hour hotline and standard refund procedures.

(4) Victim support: Fraud can cause severe psychological harm and debt. Victims, especially young people and vulnerable women, need psychological and legal support, including access to state-funded legal aid in claims against banks.

[27] Spot.uz. Material on cybercrime statistics. 9 July 2025. URL: https://www.spot.uz/oz/2025/07/09/cybercrime/.
[28] Spot.uz. Report on the Senate session on cybersecurity. 16 June 2026. URL: https://www.spot.uz/oz/2026/06/16/cybersecurity/.
[29] Spot.uz. Report on the press tour of the Cybercrime Centre of the Ministry of Internal Affairs. 29 May 2025. URL: https://www.spot.uz/oz/2025/05/29/cybercrime/.
[30] Spot.uz. Material on cybercrime results of 2025. 27 January 2026. URL: https://www.spot.uz/oz/2026/01/27/cybercrime/.
[31] Button M., Cross C. Cyber Frauds, Scams and their Victims. London: Routledge, 2017.
[32] Whitty M.T. The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam // British Journal of Criminology. 2013. Vol. 53, No. 4. P. 665–684.
[33] OECD. Recommendation of the Council on Children in the Digital Environment. OECD/LEGAL/0389. 2021.
[34] Digital transformation of Uzbekistan promotes regional integration in Central Asia // Embassy of the Republic of Uzbekistan in Austria. URL: https://usbekistan.at/?p=2958.

Interpretation: The first decline in fraud complaints in 2026 suggests that the combined measures are beginning to work. Sustained success will depend on shifting the focus from reaction to prevention, and from general campaigns to systematic education of young people.

Conclusion and recommendations

Cyber fraud has become the leading crime threat in Uzbekistan, and young people are particularly exposed to it as both victims and potential participants. The state has responded by strengthening the responsibility of financial institutions, developing detection mechanisms, establishing specialised units and conducting awareness campaigns, and the first positive results have appeared. However, the low detection rate shows that prevention through a culture of digital security must become the main line of defence. The following measures are proposed:

1. Adopt a national programme on digital security culture for young people for 2027–2030, coordinated by the Ministry of Internal Affairs, the Ministry of Justice, the education authorities and the Youth Affairs Agency.
2. Introduce mandatory digital safety modules in schools, lyceums, vocational colleges and universities, covering social engineering, protection of personal data and payment security.
3. Conduct targeted prevention against the recruitment of young people as money mules, including clear warnings in banking applications and preventive conversations before criminal liability.
4. Establish a single 24-hour hotline for blocking cards and suspicious transfers and standard procedures for refunds when banks are at fault.
5. Provide psychological and legal support for victims of fraud, including state-funded legal aid in disputes with banks and payment organisations.
6. Publish annual data on cyber fraud disaggregated by the age and sex of victims and offenders, to allow targeted prevention.

References

Legal acts and international instruments

1. Criminal Code of the Republic of Uzbekistan (Art. 168).
2. Law of the Republic of Uzbekistan “On Cybersecurity” of 15 April 2022.
3. United Nations General Assembly. United Nations Convention against Cybercrime. Resolution 79/243, 24 December 2024.
4. OECD. Recommendation of the Council on Children in the Digital Environment. OECD/LEGAL/0389. 2021.

Reports and official sources

5. Federal Bureau of Investigation, Internet Crime Complaint Center. Internet Crime Report 2024.
6. Ministry of Internal Affairs of the Republic of Uzbekistan. Official news on cybercrime prevention, 2025–2026. URL: https://gov.uz/oz/iiv

Scholarly literature

7. Button M., Cross C. Cyber Frauds, Scams and their Victims. London: Routledge, 2017.

8. Whitty M.T. The scammers persuasive techniques model // British Journal of Criminology. 2013. Vol. 53, No. 4. P. 665–684.

Media sources

9. Spot.uz. Materials on cybercrime: 29 May 2025; 9 July 2025; 27 January 2026; 16 June 2026.

10. Zamin.uz. O‘zbekistonliklar so‘nggi besh yilda kiberfiribgarliklarga 159 million dollar yo‘qotgan. November 2025.

11. Kun.uz. “The State should help victims of fraud” – Saida Mirziyoyeva comments on the suicide case in Namangan.

12. Embassy of the Republic of Uzbekistan in Austria. Digital transformation of Uzbekistan promotes regional integration in Central Asia.