Improving digital fraud prevention in Uzbekistan: evidence from 2019-2026 official statistics and the adaptive MKP-5 model

Dostonbek Muhiddin-ugli Muysinov
M.S.Vosiqova Academic Lyceum under Tashkent State University of Law

Abstract: *This article examines how the system for preventing technology-enabled crime in Uzbekistan can be improved in the context of a sharp rise in threats related to cyber fraud and the theft of citizens' funds through electronic payment instruments. According to official data, 863 technology-enabled crimes were recorded in 2019; by 2024 this figure had reached 58,800, and in 2025 cybercrimes totalled 76,852, accounting for 49.6% of all 155,002 registered crimes. The central problem of the study is the gap between the quantitative reach of prevention activities and citizens' actual safe behaviour. Although more than 23 million people were reportedly reached by cyber-prevention awareness campaigns in the first half of 2026, international meta-analytic evidence shows that cybersecurity training affects knowledge and attitudes considerably more strongly than actual behaviour. Drawing on descriptive statistics, formal legal analysis, systems analysis and comparative analysis, the author proposes MKP-5, a five-stage adaptive model of targeted cyber prevention. The model integrates diagnosis, risk segmentation, scenario-based prevention, rapid warning and outcome measurement into a single feedback cycle. The article argues that the effectiveness of cyber prevention should be assessed not only by the number of people reached, but also by indicators of threat recognition, safe decision-making, speed of reporting, repeat victimisation and financial loss. MKP-5 is presented as a conceptual and applied model that requires pilot validation, not as an intervention whose causal effectiveness has already been demonstrated.*

Keywords: *cybercrime; cyber fraud; social engineering; deepfake; cyber prevention; digital literacy; safe behaviour; mahalla; youth; MKP-5*

1. Introduction

As digital transformation expands the possibilities of public administration, education, banking, commerce and everyday communication, the methods and settings of crime, as well as the mechanisms linking offenders and victims, are also changing. In traditional property crime, the offender, the victim and the object of the crime are usually connected within a particular physical space. In cyber fraud, by contrast, the offender may be located in another region or country and may influence the victim through a messenger, social network, mobile communication, banking application, fake website or malicious software.

The Law of the Republic of Uzbekistan "On the Prevention of Offences" defines prevention not merely as a response to offences already committed, but as a system of legal, social, organisational and other measures aimed at identifying and eliminating their causes and the conditions that enable them [1]. With respect to contemporary forms of cybercrime, this requirement implies the need to adapt prevention to the actual risk structure and to constantly evolving social engineering techniques.

The scale of the problem in Uzbekistan is clearly visible in official statistics. According to the Ministry of Internal Affairs (MIA), 863 crimes of 18 types were committed using information technology in 2019, whereas 58,800 crimes of 62 types were recorded in 2024.

This is an open-access article distributed under the terms of CC BY License

The share of cybercrime in total crime rose from 6.2% in 2023 to 44.4% in 2024 [6]. According to MIA data for 2025, 76,852 of the 155,002 registered crimes, or 49.6%, were cybercrimes [7].

An official statement issued by the President on 12 March 2026 noted that the number of complaints related to cybercrime had increased 48-fold over the previous six years, that 82% of fraud offences and 76% of thefts in 2025 had been committed in cyberspace, and that the resulting material damage exceeded UZS 2 trillion [8]. It should be emphasised that the number of complaints cannot be equated with the number of registered crimes, as these are different statistical categories.

The main research problem is formulated as follows: under conditions in which the forms and methods of cybercrime are changing rapidly, how can the assessment of prevention effectiveness be shifted from population-reach indicators to a system that measures actual safe behaviour and reductions in harm? This question links the statistical analysis, the international research evidence and the proposed MKP-5 model into a single logical framework.

The aim of the study is to develop a research-based applied model for the targeted prevention of cyber fraud by synthesising open official statistics for Uzbekistan for 2019–2026, the existing legal mechanisms, the anti-fraud practice of the Central Bank and international research evidence. The object of the study is the socio-legal relations associated with the early prevention of property crimes committed using information technology; its subject is the statistical structure of cybercrime, social engineering, citizens' safe digital behaviour and institutional prevention mechanisms.

2. Literature Review and Legal Framework

Uzbekistan's legal framework regulates cybersecurity and the prevention of cybercrime along several interrelated lines. Law No. ZRU-764 "On Cybersecurity" establishes the general legal basis for protecting the interests of individuals, society and the state in cyberspace [2]. Presidential Resolution No. PP-153 of 30 April 2025 designated the MIA as the authorised body for establishing a unified practice of combating cybercrime and coordinating the activities of responsible entities, and placed specific responsibility for ensuring customers' financial security on banks, payment system operators and payment organisations [3].

Presidential Decree No. UP-38 of 10 March 2026 approved the Cybersecurity Strategy for 2026–2030 and included among its strategic objectives the protection of the interests of individuals, society and the state in cyberspace, the improvement of the cybercrime prevention system and the development of a cybersecurity culture among citizens [4]. Presidential Resolution No. PP-314 of 4 September 2026 further strengthened mechanisms of neighbourhood (mahalla)-level prevention, including close and open dialogue with residents, the early identification and elimination of the causes of offences at the local level, and an enhanced role for prevention inspectors [5].

National research literature is also beginning to systematise the statistical and institutional features of cyber fraud in Uzbekistan. Synthesising open data for 2019–2024, M.M. Umarov demonstrated the sharp growth of cybercrime, the high share of bank-card-related fraud and the central role of social engineering, and proposed countermeasures in the form of a four-tier model combining legal, technical, organisational and educational

This is an open-access article distributed under the terms of CC BY License

levels [17]. The present study does not merely replicate this national empirical base: it adds new official data for 2025–2026 and operationalises the preventive-educational level through the MKP-5 adaptive cycle, which measures behavioural outcomes.

International literature emphasises that countering social engineering cannot be limited to technical tools. The systematic review by Syafitri et al. shows that preventing social engineering attacks requires policies, training, awareness, protocols and user-centred protection mechanisms to be considered together [15]. The scoping review of phishing training by Marshall, Sturman and Auton, covering 42 studies, identifies active participation, repeated practice and detailed feedback as important design elements, while evidence on long-term behavioural retention remains limited [12].

In a meta-analysis of 69 studies, Prümmer, van Steen and van den Berg found an overall positive effect of cybersecurity training; however, its effect on knowledge and attitudes was considerably stronger than its effect on actual behaviour [11]. This finding provides scientific support for the "reach–behaviour gap" thesis of the present article: delivering prevention materials or raising knowledge does not in itself mean that safe behaviour has been formed.

The development of generative artificial intelligence (AI) is raising the risk of social engineering to a qualitatively new level. Schmitt and Flechais show that generative AI can amplify attacks by producing realistic content, enabling deep personalisation of targets and automating attack infrastructure [13]. INTERPOL's Asia and South Pacific Cyberthreat Assessment Report 2025/2026 likewise identifies the AI-assisted creation of convincing phishing messages, fake identities and realistic deepfake content as one of the new drivers of cybercrime [14].

3. Methodology and Data Quality

This study is not an empirical experiment but an analytical-conceptual study that combines open official statistics, legal documents and high-level research evidence. The main methods are descriptive statistical analysis, formal legal analysis, comparative analysis, a systems approach and evidence synthesis.

For the national statistical base, the MIA of the Republic of Uzbekistan, the official website of the President and the official report of the Central Bank of the Republic of Uzbekistan were selected as priority sources. Legal documents were verified through LexUZ, the National Database of Legislation. In selecting international evidence, priority was given to systematic reviews and meta-analyses rather than individual small-scale experiments.

Four constraints were applied in interpreting the data. First, complaints, recorded crimes, solved crimes and prevented financial transactions were treated as distinct indicators. Second, no interpolation was performed for the years between 2019, 2024 and 2025 for which data were unavailable. Third, results for the first quarter and the first half of 2026 were not extrapolated to full-year figures. Fourth, statistical associations or parallel dynamics were not interpreted as causal effects.

The author's MKP-5 model was developed as a synthesis of the available statistical and research evidence. Accordingly, the article does not claim that its practical effectiveness has already been proven; the model is a research-based applied proposal that requires separate pilot testing and subsequent empirical evaluation.

This is an open-access article distributed under the terms of CC BY License

4. Results: The Statistical Transformation of Cybercrime in Uzbekistan

4.1. Absolute figures and share in total crime

Table 1.

Key official indicators of cybercrime in Uzbekistan

Period	Indicator	Value
2019	Crimes committed using IT	863
2019	Types of crime recorded	18
2023	Share in total crime	6.2%
2024	Crimes recorded as committed using IT	58,800
2024	Types of crime recorded	62
2024	Share in total crime	44.4%
2025	Total registered crimes	155,002
2025	Cybercrimes	76,852
2025	Share of cybercrime	49.6%
2026, Q1	Crimes committed using ICT	more than 18,000
2026, Q1	Share related to theft of funds via electronic payment systems	97%

Source: *MIA official statements of 7 May 2025 and 11 April 2026, and MIA performance data for 12 months of 2025 [6, 7, 9].*

The simple ratio between the figures for 2019 (863) and 2024 (58,800) is 68.1, which corresponds to the roughly 68-fold increase reported by the MIA [6]. The difference between the 2024 figure (58,800) and the 2025 figure (76,852) is 18,052, a relative increase of approximately 30.7%. These calculations were performed by the author on the basis of the official absolute annual figures.

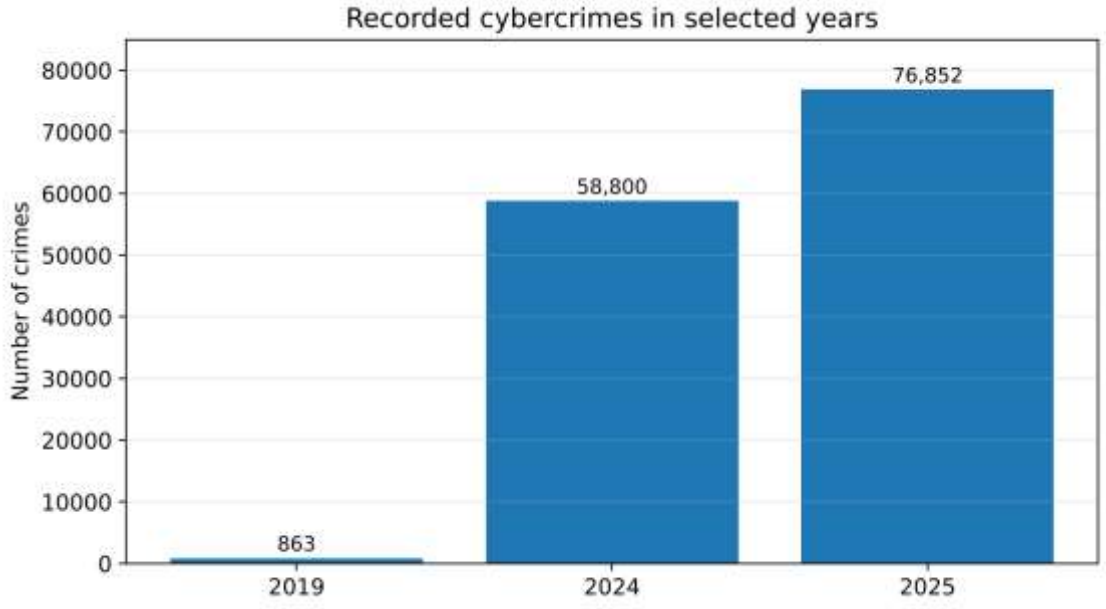

Figure 1. Number of cybercrimes recorded in selected years

Source: *compiled by the author from official MIA data [6, 7]. Values for intermediate years have not been interpolated.*

Figure 1 should be interpreted not as a continuous time series, but as a comparison of selected officially published annual data points. Nevertheless, the difference in scale

This is an open-access article distributed under the terms of CC BY License

between 2019 and 2024 and the further increase between 2024 and 2025 show that cybercrime is a systemic rather than a peripheral problem for offence prevention.

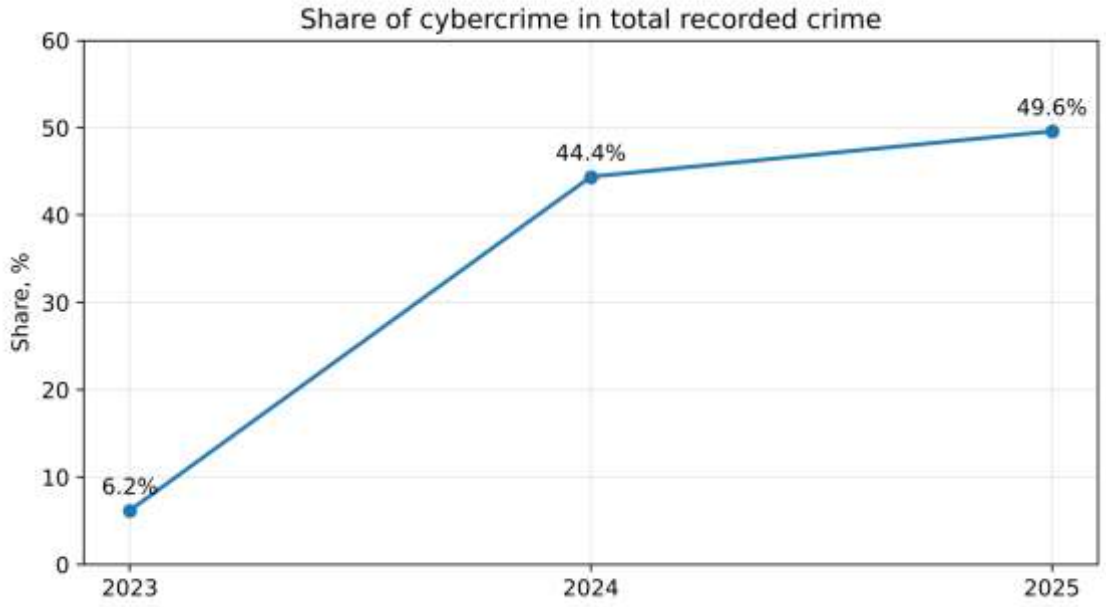

Figure 2. Share of cybercrime in total recorded crime, 2023–2025

Source: *compiled by the author from official MIA data [6, 7].*

The share of cybercrime in total crime rose from 6.2% in 2023 to 44.4% in 2024 and to 49.6% in 2025. This represents an increase of 38.2 percentage points between 2023 and 2024 and a further 5.2 percentage points between 2024 and 2025. Although possible differences in statistical classification and registration methodology across periods cannot be ruled out, the official data clearly indicate the need to align prevention resources with digital risks.

4.2. Methods of offending: what should determine preventive content?

Table 2.

Main methods of committing cybercrime

Method	Share	Preventive content
Malicious link/software	60%	Checking links, domains, APK files and app permissions
Obtaining SMS codes by deception	16%	Social engineering and "bank employee" scenarios
Online shopping fraud	11%	Checking fake advertisements and payment pages
Other fraud schemes	9%	Investment, prize and "quick income" schemes
Illegal online loans	4%	Protection of personal data and identity

Source: *official MIA data [6]. The "Preventive content" column is the author's analytical recommendation.*

This is an open-access article distributed under the terms of CC BY License

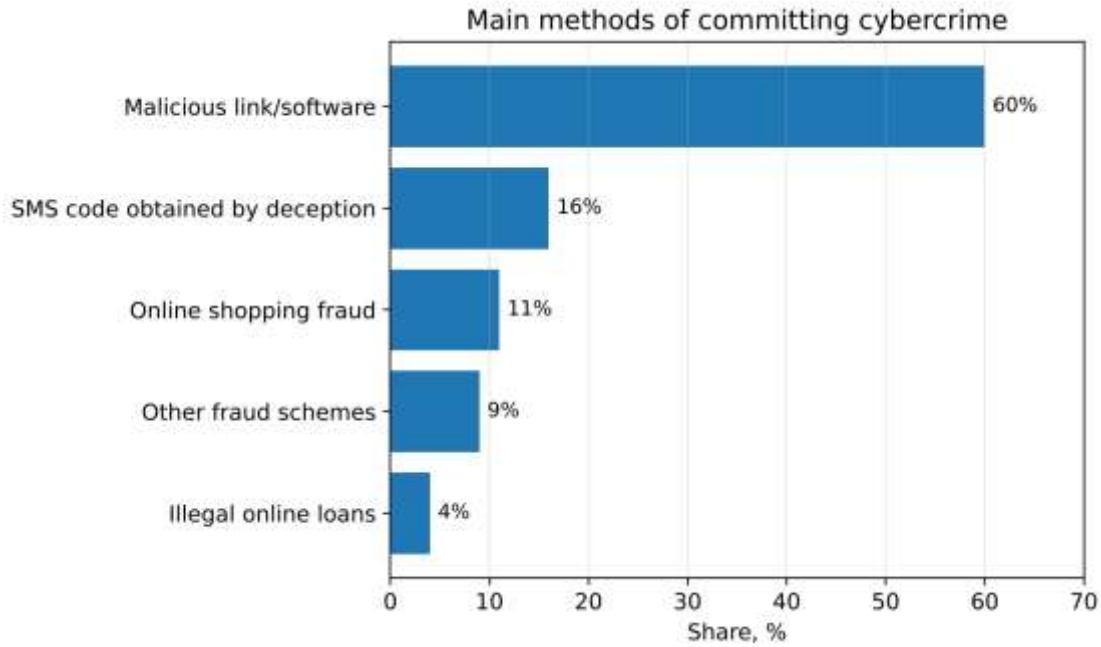

Figure 3. Main methods of committing cybercrime, %

Source: *official MIA data [6].*

This distribution provides a basis for the principle of "risk-proportionate prevention": rather than distributing educational and awareness resources evenly and in isolation from the actual structure of crime, priority should be given to the mechanisms that generate the greatest harm and occur most frequently. However, the 60-16-11-9-4% structure should not be treated as a permanent norm. As fraud methods change, the content of prevention must also be updated on the basis of periodic statistical diagnosis.

4.3. 2026: the central role of financial security

According to the MIA's official report for the first quarter of 2026, more than 18,000 crimes were committed using information and communication technologies (ICT) within three months, and 97% of them involved the theft of citizens' funds through electronic payment systems [9]. This figure is not extrapolated to the whole of 2026; its scientific value lies in showing how central digital financial security has become to the substance of cybercrime.

In the first half of 2026, a special system operated jointly by the MIA and the Central Bank blocked 18,838 crime-related bank cards; 9,282 cybercrimes were solved, 4,011 crimes were detected proactively, and more than UZS 120.496 billion in material damage was returned to more than 13,000 citizens [10]. These figures show that cyber prevention must include not only advice to citizens, but also rapid technological and financial blocking mechanisms.

5. Technological Anti-Fraud and the Human Factor: The Need for Multi-Layered Protection

The Central Bank's 2024 annual report notes that a re-confirmation mechanism of up to 48 hours was introduced to prevent online-loan fraud. From November to the end of the year, funds totalling UZS 304.1 billion were returned to credit institutions in 28,138 cases because the customer had not passed additional identification. In addition, as a result of rapid measures taken on citizens' complaints about bank-card fraud, UZS 9.5 billion was blocked during 2024 [16].

This is an open-access article distributed under the terms of CC BY License

The same report states that a centralised anti-fraud system was introduced at the Central Bank on a pilot basis, with 34 banks and 9 payment organisations integrated into it [16]. These data show that technical protection mechanisms have real practical value in preventing cybercrime.

Table 3.

Selected results of institutional and technological measures against cyber fraud

Period	Measure / result	Value
2024	Funds blocked in bank-card fraud cases	UZS 9.5 billion
2024, Nov–Dec	Online-loan transactions reversed because additional identification was not passed	28,138
2024, Nov–Dec	Funds involved in these transactions	UZS 304.1 billion
2024	Integration into the centralised anti-fraud system	34 banks + 9 payment organisations
2026, H1	Crime-related bank cards blocked	18,838
2026, H1	Material damage returned to citizens	more than UZS 120.496 billion

Source: *Central Bank of the Republic of Uzbekistan, Annual Report 2024; MIA official statement of 11 August 2026 [10, 16].*

However, the existence of technological anti-fraud does not eliminate the human factor. In most social engineering attacks, the offender exploits a person's trust, fear, haste, self-interest or habit of obeying an apparent authority rather than a technical vulnerability in the system. For this reason, the article adopts the formula "human + technology + institution", rather than "human or technology", as its core protection principle. This conclusion is consistent with the four-level approach proposed by M.M. Umarov, which calls for the integrated application of legal, technical, organisational and educational measures [17]. The present article deepens the preventive-educational component of that approach by adding mechanisms for risk diagnosis and outcome measurement.

6. The "Reach–Behaviour Gap": How Should Prevention Outcomes Be Measured?

In the first half of 2026, more than 23 million people in the country were reached by awareness campaigns aimed at preventing cybercrime and raising the population's cybersecurity culture. The same official statement criticised the measures taken as insufficient and stressed the need for a deeper analysis of citizens' complaints, the causes of cybercrime and the factors that enable it [10].

It would be incorrect to interpret these two points as contradictory. Reaching 23 million people is an output indicator reflecting the volume of activity; in itself, it does not answer whether citizens were able to recognise fraud in a real situation, whether they made a safe decision, or whether victimisation decreased. The article therefore uses the concept of the "reach-behaviour gap" to denote the methodological difference between receiving a preventive message and acting safely in practice.

Table 4.

Effects of cybersecurity training in the meta-analysis

Outcome	Cohen's d	95% confidence interval
Overall effect	0.75	0.58 to 0.92
Knowledge and attitudes	1.02	0.58 to 1.46

This is an open-access article distributed under the terms of CC BY License

Actual behaviour	0.36	−0.09 to 0.80

Source: *meta-analysis by Prümmer, van Steen and van den Berg, 69 studies [11].*

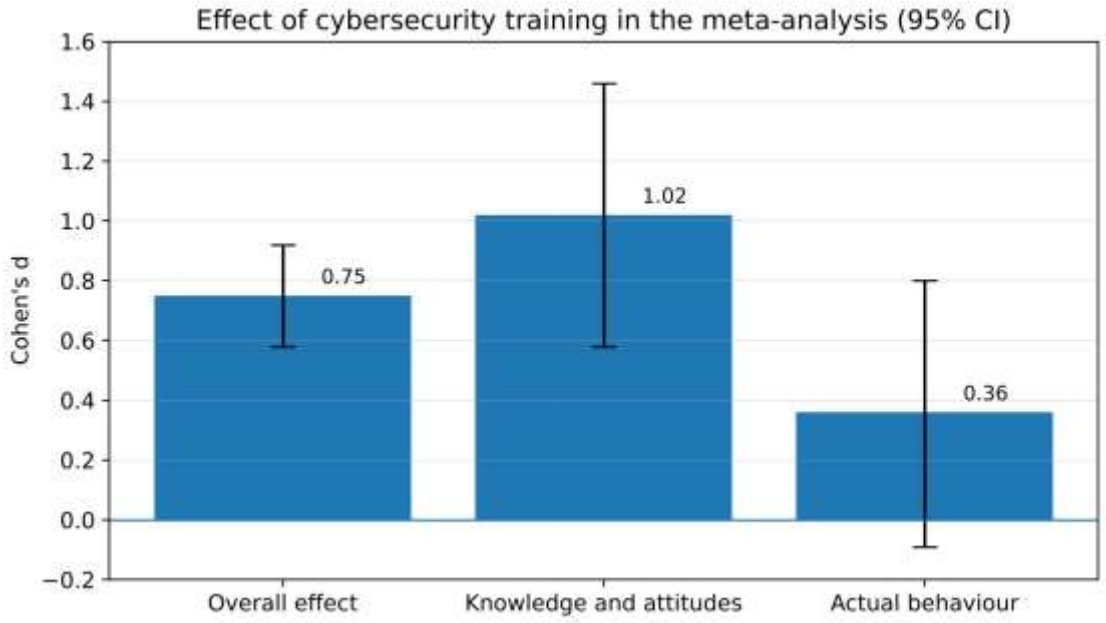

Figure 4. Effects of cybersecurity training in the meta-analysis with 95% confidence intervals

Source: *compiled by the author from data in Prümmer, van Steen and van den Berg [11].*

In the meta-analysis, the overall effect of training was positive (d = 0.75) and relatively strong for knowledge and attitudes (d = 1.02). For actual behaviour, d = 0.36 with a 95% confidence interval from −0.09 to 0.80, which includes zero [11]. This result cannot be interpreted as meaning that "training does not work". The correct conclusion is that additional methodological steps are needed between increasing knowledge and forming actual safe behaviour.

The scoping review of 42 studies by Marshall et al. likewise highlights the importance of active learning, repeated practice, detailed feedback and repeated training [12]. Consequently, the next stage of preventive work should move from one-off lectures to decision-making in safe, near-realistic situations.

7. Generative Artificial Intelligence and Deepfakes: A New Object of Prevention

Generative AI has three main capabilities that amplify the social engineering threat: producing realistic content, deeply personalising targets and automating attacks [13]. Because text, voice, image and video can now be generated, the cue "the message looks credible" is becoming an increasingly weak authentication criterion.

INTERPOL's Asia and South Pacific Cyberthreat Assessment Report 2025/2026 lists phishing and online fraud among the most widespread threats in the region and those causing the greatest financial losses, and identifies AI as a factor used by criminals to scale and automate attacks and to create realistic deepfake content [14]. These international indicators cannot be compared directly and quantitatively with Uzbekistan's statistics, but they are important for identifying the qualitative direction in which the threat is evolving.

Therefore, a new universal competence should be added to traditional rules such as "do not trust unknown numbers" or "do not share SMS codes": when money, confidential information or urgent action is requested, the authenticity of the person or organisation

This is an open-access article distributed under the terms of CC BY License

should be confirmed through a channel independent of the one used in the message. The author refers to this rule as the "independent verification principle".

8. MKP-5: A Five-Stage Adaptive Model of Targeted Cyber Prevention

Based on the analysis, the author proposes the MKP-5 model. The novelty of the model lies not in creating a separate preventive activity, but in integrating existing statistical, educational, mahalla-level and technological mechanisms into a measurable feedback cycle. Conceptually, the model is scientifically continuous with the educational-preventive line identified in M.M. Umarov's multi-level system of countermeasures against cyber fraud [17]; MKP-5 differs in that it transforms this line into a five-stage, measurable feedback cycle.

Table 5.

Architecture of the MKP-5 model

Stage	Key question	Action	Output
1. Diagnosis	Which schemes pose a real risk?	Analysis of crimes, complaints, losses and new schemes	Current risk profile
2. Segmentation	Who needs help with which risk?	Matching risk types to audience needs	Targeted content
3. Scenario training	What does a citizen do in the situation?	Safe simulation, decision and feedback	Practical skill
4. Rapid warning	When is a new scheme communicated?	Short standardised warning	Reduced information delay
5. Outcome measurement	What has prevention changed?	Knowledge, behaviour and harm indicators	Evidence for the next cycle

Source: *developed by the author.*

The model is not a closed chain: the measurement results of the fifth stage become input data for a new diagnosis. Its full formula is therefore: diagnosis → segmentation → scenario → rapid warning → outcome measurement → re-diagnosis.

8.1. Diagnosis and risk-proportionate prevention

Instead of fixing preventive content as an unchanging list at the beginning of the year, periodic statistical diagnosis is recommended. Depersonalised indicators such as the crime mechanism, the communication channel used, the material loss, repeat victimisation, broad age groups and the time elapsed before reporting make it possible to build a real risk profile. Personally identifiable information must not be disclosed, and personal data protection requirements must be strictly observed.

If, in a given period, malicious links and software are the dominant mechanism, the main share of preventive exercises should be directed at that risk. If deepfake voice fraud or a new financial scheme increases in the following period, the content is redistributed accordingly. In this way, prevention develops together with the statistics rather than lagging behind them.

This is an open-access article distributed under the terms of CC BY License

8.2. Scenario-based prevention and the "STOP–CHECK–VERIFY–REPORT" algorithm

In scenario training, the participant is not a passive listener but a decision-maker. For example, a message requesting an SMS code on behalf of a "bank employee", a fake payment link for an online purchase, an APK file, a "high-yield investment" offer or a deepfake audio message imitating a relative's voice is presented in the form of a safe simulation. Participants do not use real accounts, cards or passwords.

For everyday use, the author proposes a four-step algorithm: STOP - do not make an automatic decision under pressure of an urgent request; CHECK - identify warning signs in the sender, link, file, account and request; VERIFY - contact an independent official communication channel rather than the channel indicated in the message; REPORT - report to the competent authority if there are signs of fraud.

8.3. Rapid warning

Because cyber fraud schemes are updated rapidly, the practical value of a preventive message declines if it is delivered long after a new threat has been identified. Within MKP-5, it is proposed that a standardised initial warning be issued as quickly as possible for any reliably confirmed new scheme with a risk of wide dissemination. No fixed deadline is set as a mandatory standard, since none is prescribed by law; speed must be balanced against technical capacity, fact-checking and the risk of false alarms.

The minimum content of a warning is: what the scheme looks like; what the fraudster demands; the main warning sign; what the citizen should not do; and how to act safely and where to report. This format does not replace detailed technical guidance but serves as initial rapid protection.

8.4. Outcome measurement: from outputs to outcomes

Table 6.

Architecture for assessing the effectiveness of cyber prevention

Level	What is measured?	Examples
A. Activity (output)	How much work was done?	Reach; number of trainings and materials
B. Learning	What was learned?	Correct threat recognition; 30-day knowledge retention
C. Behaviour	What was done in the situation?	Rejecting a suspicious link; independent verification; reporting
D. Criminological harm	How did the real risk change?	Victimisation; repeat victimisation; material loss; time to report

Source: *developed by the author. A → B → C → D is not an automatic causal chain; the relationships require empirical testing.*

Reaching more than 23 million people through awareness campaigns is an important Level A result [10]. However, a full assessment of prevention also requires Level B and C indicators and, where possible, Level D indicators. This transition is the practical answer to the "reach–behaviour gap" identified in the article.

9. Practical Recommendations

Table 7.

Practical recommendations developed in the study

No.	Proposal	Expected management outcome

This is an open-access article distributed under the terms of CC BY License

1	Introduce behavioural and harm indicators alongside prevention reach	Distinguishing the volume of activity from real outcomes
2	Systematise depersonalised cybercrime statistics by mechanism and loss	Risk-proportionate preventive content
3	Pilot safe "Cyber Case Lab" scenario exercises in educational institutions	Turning knowledge into decision-making skills
4	Promote the "independent verification" principle against deepfake and AI-enabled fraud	Reducing the risk of over-trusting voice and images
5	Deliver short rapid materials on confirmed new fraud schemes to mahallas and educational institutions	Shortening the time between a threat and a preventive message
6	Treat technological anti-fraud, institutional response and human behaviour as a single protection system	Not placing responsibility solely on citizens
7	Test the MKP-5 model in a pilot region or educational institution using a pre-test/post-test and follow-up design	Evaluating the model's real causal effectiveness

Source: *the author's research-based recommendations.*

The "Cyber Case Lab" does not require the creation of a separate new subject in educational institutions. Within law, computer science or civic education classes, students justify their decisions in a short (15–20 minute), safe, near-realistic scenario. All materials must be purpose-built training simulations; no real phishing websites, malicious files, bank cards, PINs, one-time passwords or passwords may be used.

Further empirical testing of the MKP-5 model may use a pre-test → training → post-test → 30-day follow-up design. Where feasible, including a comparison group would allow stronger conclusions about the model's causal effect. If such research involves minors, the ethical review and consent procedures of the educational institution must be strictly followed.

10. Scientific Novelty, Practical Significance and Limitations

10.1. Scientific novelty

The scientific novelty of the study consists of the following: first, the concepts of "complaint", "recorded crime", "solved crime", "prevention reach" and "blocked financial transaction" found in open statistics were clearly distinguished; second, the "reach-behaviour gap" was formulated as the central methodological problem in assessing prevention effectiveness; third, linking the structure of cybercrime to a risk-proportionate distribution of preventive content was proposed; fourth, the MKP-5 adaptive model and a four-level evaluation architecture were developed; and fifth, the "independent verification principle" was substantiated as a new universal element of safe behaviour in the era of generative AI and deepfakes. M.M. Umarov's earlier study empirically synthesised open data on cyber fraud in Uzbekistan and proposed a four-level countermeasure model combining legal, technical, organisational and educational measures [17]. The independent contribution of the present article lies in transforming specifically the preventive-

This is an open-access article distributed under the terms of CC BY License

educational line of that broader system into the MKP-5 cycle, based on the updated 2025–2026 statistical base, the reach–behaviour distinction and measurable feedback.

10.2. Practical significance

The MKP-5 model can serve as a methodological basis for planning cybercrime-prevention information campaigns, designing targeted scenario-based sessions in mahallas and educational institutions, improving the system of prevention indicators, and rapidly updating content in response to new fraud schemes. The model is intended not to replace the existing system, but to add feedback and outcome-measurement mechanisms to it.

10.3. Limitations

The first limitation is that open official statistics do not provide a complete cybercrime series compiled using a consistent methodology for all years; consequently, no artificial values were calculated for missing years. The second limitation is that different sources use the terms "cybercrime", "crime committed using information technology" and "crime committed using ICT"; the extent to which open information allows verification that their statistical classification was identical across all periods is limited. The third limitation is that no open individual-level or control-group data are available to assess the causal effect of the 23-million reach on behaviour. The fourth limitation is that effect sizes from the international meta-analysis cannot be directly projected onto the population of Uzbekistan. The fifth limitation is that MKP-5 is currently an evidence-informed conceptual and applied model, and its effectiveness must be tested in a pilot empirical study.

11. Conclusion

The analysis has shown that the importance of cybercrime in Uzbekistan has increased sharply not only in absolute numbers but also in terms of its share in the overall structure of crime. The increase from 863 cases in 2019 to 58,800 in 2024, and the fact that 76,852 cybercrimes accounted for 49.6% of all crimes in 2025, mean that digital security has become one of the central areas of prevention policy [6, 7].

The fact that 97% of the more than 18,000 ICT-enabled crimes committed in the first quarter of 2026 involved the theft of citizens' funds through electronic payment systems marks digital financial security as a distinct priority [9]. At the same time, data from the Central Bank and the MIA confirm the need for technological anti-fraud, card blocking, additional identification and loss-recovery mechanisms [10, 16].

The central conclusion of the article is that prevention reach and prevention effectiveness are not the same concept. Reaching more than 23 million people with awareness campaigns is an important output, but citizens' ability to recognise risk, make safe decisions and experience a real reduction in harm requires separate outcome indicators [10]. The international meta-analysis shows that the effect on knowledge and attitudes is markedly stronger than the effect on actual behaviour [11].

On this basis, the proposed MKP-5 model transforms prevention from static awareness-raising into an adaptive cycle: DIAGNOSIS → SEGMENTATION → SCENARIO-BASED PREVENTION → RAPID WARNING → OUTCOME MEASUREMENT → RE-DIAGNOSIS. The scientific and practical value of the model lies in linking the risk

This is an open-access article distributed under the terms of CC BY License

structure to preventive content, and that content to measurable behavioural and harm outcomes.

As generative AI and deepfake technologies develop, the new rule of digital security should not be "I saw or heard it, so it is real", but "I verified it through an independent channel, and only then do I act". A task for future research is to pilot the MKP-5 model with a real audience in accordance with ethical requirements and to evaluate empirically its effect on behaviour and on the risk of victimisation.

Declarations

Funding. This research received no external funding.

Conflict of interest. The author declares no conflict of interest.

Data availability. All data used in this study are drawn from publicly available official sources and published literature listed in the References.

Ethics statement. This study did not involve human participants or the collection of personal data; ethical approval was therefore not required.

Note. The article was prepared on the basis of open official data and research literature. The author does not claim to have conducted an independent empirical survey or experiment; the MKP-5 model is proposed as a research-based applied model for subsequent pilot testing.

References

1. Law of the Republic of Uzbekistan No. ZRU-371 of 14 May 2014 "On the Prevention of Offences" [in Uzbek]. National Database of Legislation. Available at: https://lex.uz/docs/-2387357 (accessed 17 September 2026).

2. Law of the Republic of Uzbekistan No. ZRU-764 of 15 April 2022 "On Cybersecurity" [in Uzbek]. National Database of Legislation. Available at: https://lex.uz/uz/docs/-5960604 (accessed 17 September 2026).

3. Resolution of the President of the Republic of Uzbekistan No. PP-153 of 30 April 2025 "On Measures to Further Strengthen the Fight against Crimes Committed Using Information Technology" [in Uzbek]. Available at: https://lex.uz/uz/docs/-7511145 (accessed 17 September 2026).

4. Decree of the President of the Republic of Uzbekistan No. UP-38 of 10 March 2026 "On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for Preventing Cybercrime" [in Uzbek]. Available at: https://lex.uz/docs/-8079286 (accessed 17 September 2026).

5. Resolution of the President of the Republic of Uzbekistan No. PP-314 of 4 September 2026 "On Measures to Introduce a New Working System in the Activities of Internal Affairs Bodies to Ensure Public Safety" [in Uzbek]. Available at: https://lex.uz/docs/-8452371 (accessed 17 September 2026).

6. Ministry of Internal Affairs of the Republic of Uzbekistan. Creating a Safe Cyberspace by Curbing Cybercrime: Uzbekistan's Experience in the Early Prevention of Cybercrime in the Context of Digital Transformation [in Uzbek]. 7 May 2025. Available at: https://gov.uz/oz/iiv/news/view/52319 (accessed 17 September 2026).

7. Ministry of Internal Affairs of the Republic of Uzbekistan. Criminogenic Situation and Main Performance Indicators for 12 Months of 2025 [in Uzbek]. 2026. Available at:

This is an open-access article distributed under the terms of CC BY License

https://api-portal.gov.uz/uploads/11/2026/03/06/a96d8f40-67dc-2262-e23e-9f3908f74281_media_.pdf (accessed 17 September 2026).

8. Official website of the President of the Republic of Uzbekistan. The Fight against Organised Crime and Cybercrime Will Be Improved [in Uzbek]. 12 March 2026. Available at: https://president.uz/oz/lists/view/9009 (accessed 17 September 2026).

9. Ministry of Internal Affairs of the Republic of Uzbekistan. "Openness and Dialogue with the People Is the Main Criterion": Analytical Report for the First Quarter of 2026 [in Uzbek]. 11 April 2026. Available at: https://gov.uz/oz/iiv/news/view/152591 (accessed 17 September 2026).

10. Ministry of Internal Affairs of the Republic of Uzbekistan. Ensuring Public Safety, Combating Crime and Improving Service Efficiency: Performance Review for the Second Quarter of 2026 [in Uzbek]. 11 August 2026. Available at: https://gov.uz/oz/iiv/news/view/204415 (accessed 17 September 2026).

11. Prümmer J., van Steen T., van den Berg B. Assessing the effect of cybersecurity training on end-users: A meta-analysis. Computers & Security. 2025;150:104206. https://doi.org/10.1016/j.cose.2024.104206

12. Marshall N., Sturman D., Auton J.C. Exploring the evidence for email phishing training: A scoping review. Computers & Security. 2024;139:103695. https://doi.org/10.1016/j.cose.2023.103695

13. Schmitt M., Flechais I. Digital deception: generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review. 2024;57:324. https://doi.org/10.1007/s10462-024-10973-2

14. INTERPOL. Asia and South Pacific Cyberthreat Assessment Report 2025/2026. Lyon: International Criminal Police Organization; 2026. Available at: https://www.interpol.int/content/download/24327/file/CYBER_ASP%20Cyber%20Threat%20Assessment%20Report_2025_2026_v4.pdf (accessed 17 September 2026).

15. Syafitri W., Shukur Z., Mokhtar U.A., Sulaiman R., Ibrahim M.A. Social engineering attacks prevention: A systematic literature review. IEEE Access. 2022;10:39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

16. Central Bank of the Republic of Uzbekistan. Annual Report 2024. Section 4.4: Ensuring Information Security and Cybersecurity in Payment Systems and Information Systems of Commercial Banks [in Uzbek]. Tashkent: Central Bank of the Republic of Uzbekistan; 2025. Available at: https://cbu.uz/upload/medialibrary/f09/97s10c90awxkge6q19qc1r5b6ok10lxi/Markaziy-bank-yillik-hisoboti-2024.pdf (accessed 17 September 2026).

17. Umarov M.M. Trends in cybersecurity and the surge of cyber-fraud against citizens in Uzbekistan: An empirical analysis of open data. European Journal of Economic Dynamics and Policy. 2026;2(8):3–17. Available at: https://nordascend.com/index.php/ejedp/article/view/58 (accessed 17 September 2026).

This is an open-access article distributed under the terms of CC BY License