Trends in Cybersecurity and the Surge of Cyber-Fraud Against Citizens in Uzbekistan: An Empirical Analysis of Open Data

Mukhiddin Muysinovich Umarov
Academy of Ministry of Internal Affairs of Republic of Uzbekistan

Abstract: *Rapid digitalization of payments has been accompanied in Uzbekistan by an extraordinary rise in cybercrime, dominated by cyber-fraud that directly drains citizens' money. Drawing only on open official and authoritative sources, this paper assembles the fragmented public record into a single empirical picture and reads it against global trends. Official figures indicate a roughly 68-fold growth of cybercrime over 2019–2024, about 59,000 cybercrimes in 2024 (a 9.1-fold rise on 2023), a jump in the cybercrime share of all registered crime from 6.2% in 2023 to about 42% by mid-2025, and citizen losses exceeding 1.9 trillion UZS over 2021–2024, of which 603 billion UZS fell in 2024 alone. Bank cards are implicated in 98% of cases, and the episode structure is led by malware (60%), phishing for one-time codes (16%), marketplace fraud (11%), direct social-engineering deception (9%), and fraudulent online lending (4%). These national patterns mirror the global shift, documented by ENISA and the FBI IC3, toward human-centered social engineering increasingly amplified by artificial intelligence. We analyse drivers, situate the national response (the 2022 Cybersecurity Law, an ITU Global Cybersecurity Index score of 89.20, and dedicated police capacity), and propose a four-level countermeasures model (legal, technical, organizational, educational) in which each measure is tied to the evidence and to the role of law-enforcement bodies. The study is a secondary-data analysis; its limitations and the need for primary, victim-level data are discussed.*

Keywords: *Cybercrime; Cyber-Fraud; Social Engineering; Financial Fraud; Uzbekistan; Threat Intelligence; Phishing; Cybersecurity Policy*

1 Introduction

Across the world the cost of cybercrime is climbing, and its centre of gravity is moving from purely technical intrusion toward the manipulation of people. In Uzbekistan this shift has been unusually abrupt. Fast adoption of bank cards, mobile banking, and online marketplaces has expanded the attack surface faster than public awareness or institutional safeguards could keep pace, and the result has been a steep rise in cyber-fraud that takes money directly from citizens.

The scale is now hard to overstate. According to the Cybersecurity Centre of the Ministry of Internal Affairs (MoIA), cybercrime in the country grew roughly 68-fold between 2019 and 2024, and by mid-2025 cyber-enabled offences accounted for close to half of all registered crime. Citizen losses over 2021-2024 exceeded 1.9 trillion UZS. For a Track-5 cybersecurity venue, this is not only a technical problem but a societal and law-enforcement one, which is the vantage point of this paper. The harm is not abstract: it falls on individuals who can lose their savings to a single phone call, and on a financial system whose usefulness depends on the trust of the people it serves, which is why a policing and prevention perspective, rather than a purely technical one, is appropriate here.

The public record, however, is scattered across press briefings, a central-bank report, and international indices, and it has not been consolidated into a single evidence-based picture

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

or compared systematically with global trends. This paper closes that gap. Its contributions are: (i) an empirical synthesis of open data on the dynamics, structure, and financial impact of cyber-fraud in Uzbekistan over 2020–2025; (ii) a comparison with global threat-intelligence findings showing that the national pattern is a local instance of a worldwide turn toward AI-amplified social engineering; and (iii) a four-level countermeasures model in which legal, technical, organizational, and educational measures are each grounded in the evidence and in the role of law-enforcement bodies.

The remainder of the paper is organized as follows. Section 2 reviews global trends and threat-intelligence methods. Section 3 describes the data and method. Section 4 presents the empirical analysis for Uzbekistan. Section 5 discusses drivers and the national-versus-global comparison. Section 6 sets out the countermeasures model. Section 7 states limitations, and Section 8 concludes.

2 Related Work: Global Trends and Threat Intelligence

The global backdrop frames the national case. The FBI Internet Crime Complaint Center recorded 859,532 complaints in 2024 with reported losses of about USD 16.6 billion, a 33% rise on 2023 [1]. The European Union Agency for Cybersecurity reports that phishing is now the leading vector for initial intrusion, present in roughly 60% of observed cases, and that by early 2025 more than 80% of observed social-engineering activity drew on artificial intelligence, from generative phishing text to deepfake voice and purpose-built malicious language models [2]. In the finance sector specifically, ENISA finds that social-engineering attacks led to financial loss in about half of incidents and to fraud in a further quarter, with banks the most frequently targeted organisations and SMS-based phishing (smishing) the most common channel [3].

Two themes from this literature matter here. First, the dominant risk is human-centered: attackers increasingly bypass technical controls by deceiving the user rather than breaking the system, a shift long studied in the social-engineering literature [12] and visible in breach data where external actors and stolen credentials dominate [9, 10]. Second, threat intelligence, the systematic collection and analysis of indicators and tactics, has become the organising discipline for anticipating these attacks [3]. The economic-measurement literature further cautions that headline loss figures are hard to compare across jurisdictions because definitions, reporting incentives, and recovery rates differ [11]. These themes guide both the interpretation of the Uzbek data and the design of the countermeasures model.

It helps to fix terms. Social engineering covers a family of techniques that manipulate people into disclosing information or authorizing transfers. Phishing uses fraudulent email or web pages; smishing delivers the lure by SMS; vishing does so by voice call; and quishing hides a malicious link inside a QR code. International reporting finds smishing especially prominent in finance and quishing rising quickly [3]. The Uzbek pattern, in which the decisive step is persuading a victim to read out a one-time SMS code, is squarely a smishing-and-vishing problem, and that shapes the design of defences.

A second strand of recent work concerns the amplification of these techniques by artificial intelligence. Generative models can produce fluent, localized phishing text at scale; voice-cloning and deepfake tools can imitate a bank officer or a relative; and purpose-built malicious models lower the skill barrier for attackers. ENISA reports that AI featured in the majority of observed social-engineering activity by early 2025 [2]. For a country where

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

impersonation of banks and officials already drives losses, this is a direct forward risk, because it raises the credibility of exactly the scripts that are most damaging locally.

Against this backdrop, threat intelligence has become the organizing discipline of defence. By collecting indicators, tracking the tactics, techniques, and procedures of fraud operations, and sharing them across institutions, defenders can anticipate campaigns rather than only react to them [2, 3]. The approach is inherently collaborative: ENISA repeatedly stresses sector-wide intelligence sharing among financial institutions, a point that returns in the organizational level of the model proposed below.

Methodologically, the analysis of cyber-threats rests on a few now-standard constructs: indicators of compromise that flag known-bad artefacts, the tactics, techniques, and procedures that describe how an adversary operates, and frameworks such as the cyber kill chain and ATT&CK-style matrices that map an attack from initial contact to objective. For fraud specifically, the most informative layer is behavioural, the recurring scripts of persuasion, because the same social-engineering playbook is reused across many technical guises. Reading the Uzbek schemes as scripts, rather than only as malware families, is what allows them to be matched to defences and to be recognized when they recur.

Finally, the economics-of-cybercrime literature warns that headline numbers must be read with care: reported losses, recovery rates, and even the definition of an incident vary widely across jurisdictions, so cross-country comparison is fraught [11]. This caution shapes the present analysis, which treats the Uzbek totals as indicators of trend and magnitude rather than precise accounting. Regionally, rapid digitalization across Central Asia, together with cross-border call-centre operations documented in neighbouring markets, suggests that the drivers identified here are not unique to Uzbekistan and that cooperation beyond national borders will matter.

The concrete scam types reported locally fit these categories. They include calls and messages impersonating bank security services or the regulator, fraudulent listings and buyers on classified-ad and marketplace platforms, and the circulation through messengers of forged documents bearing the Central Bank's insignia in order to induce victims to install malware. Each of these is a social-engineering script built on the appearance of authority, and each maps onto a row of the typology developed in Section 4.

2.1 From Technical Intrusion to Human-Centered Fraud

A useful way to read these trends is as a migration of risk from the machine to the person. As organizations hardened networks and adopted multi-factor authentication, attackers shifted to eliciting or stealing the authentication factors themselves: industry data show credential-based attacks rising sharply year on year, and stolen credentials overtaking email phishing as an initial access vector in some datasets [9, 10]. The one-time SMS code at the centre of Uzbek card fraud is exactly such a factor, which is why a posture that still depends on a shareable code remains exposed. The lesson from the global record is that controls must assume the user can be deceived and must limit the damage when they are.

The prevention literature offers a parallel lesson. Because technical controls cannot fully close a human vulnerability, effective programmes combine system design that reduces opportunities for disclosure with sustained education that raises the cost of deception. Awareness decays without reinforcement, and design cannot anticipate every script, so the

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

two are complements rather than alternatives, a principle reflected in the four-level model of Section 6.

3 Data and Methodology

This study is a secondary-data analysis. It triangulates open, authoritative sources rather than collecting primary data: statements and statistics from the MoIA Cybersecurity Centre [5], registered-crime data attributed to the Statistics Agency [6], the Central Bank of Uzbekistan Annual Report 2024 [7], the ITU Global Cybersecurity Index [4], a UNODC/UNDP programme document [8], and global threat-intelligence reports for comparison
[1, 2, 3]. Indicators were extracted, cross-checked for internal consistency, organized into a common frame (dynamics, structure, financial impact, response), and visualized.

The analysis is organized around four dimensions that also structure Sections 4 to 6: dynamics (how fast and how far the problem has grown), structure (which schemes and channels dominate), financial impact (losses and the sums recovered or prevented), and response (the measures in place). Each extracted indicator was assigned to one of these dimensions, which makes the descriptive picture comparable across sources and maps directly onto the countermeasures model.

Three cautions apply and are carried through the analysis. First, several national figures originate in press briefings rather than peer-reviewed statistical releases, so definitions and counting rules may vary across years; where a value is derived rather than directly reported, it is labelled as such (for example, the 2023 cybercrime count in Fig. 2a is inferred from the reported 6.2% share). Second, as a secondary analysis the study describes and compares but does not establish causation. Third, monetary values are stated in Uzbekistani som (UZS); at the 2025 exchange rate of roughly 12,900 UZS per USD, 1.9 trillion UZS is on the order of USD 145–150 million, but readers should treat cross-currency comparison as indicative. Despite these limits, the sources are mutually consistent (Section 4) and sufficient for a descriptive baseline.

Source quality was appraised by tiering: the central-bank report and statistical releases were treated as the most reliable, press briefings by the responsible agencies as authoritative but less granular, and international indices and threat reports as comparators rather than as evidence about Uzbekistan specifically. The study raises no ethical concerns of its own, since it uses only aggregate, already-public figures and contains no personal data, which is appropriate to a topic where victim information is sensitive.

For the international comparison, national indicators were placed beside the corresponding global findings on a like-for-like basis where possible, for example matching the local phishing-for-codes pattern to ENISA's smishing finding and the local loss trajectory to the FBI IC3 totals, while respecting the warning from the economics literature that absolute figures are not directly commensurable across systems.

The temporal scope is 2020 to mid-2025 for national indicators, with the global comparators drawn from 2024 and 2025 reports. Where a single year is cited it is the most recent available from the responsible body at the time of writing; where a range is cited it reflects the cumulative reporting used by the source, as with the 2021 to 2024 loss total.

4 Empirical Analysis: Uzbekistan

4.1 Overall Crime and the Rise of Cyber-Offences

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

Registered crime in Uzbekistan rose from 62,081 in 2020 to 132,298 in 2024, with a sharp increase in 2021 and a renewed jump in 2024 (Fig. 1); registered fraud alone reached 29,252 in 2024, up 58.2% year on year [6]. Against this background the cyber component grew far faster. The MoIA reports an approximately 68-fold increase in cybercrime over 2019–2024 and about 59,000 cybercrimes in 2024, a 9.1-fold rise on 2023 [5]. The share of cyber-enabled offences in all registered crime climbed from 6.2% in 2023 to roughly 42% by the first half of 2025 (Fig. 2) [5]. These figures are mutually consistent: a 6.2% share of the 2023 total implies about 6,500 cybercrimes, which scaled by 9.1 yields the reported 2024 figure, and that figure is close to 45% of all 2024 crime, in line with the statement that cyber-offences now make up almost half of the total.

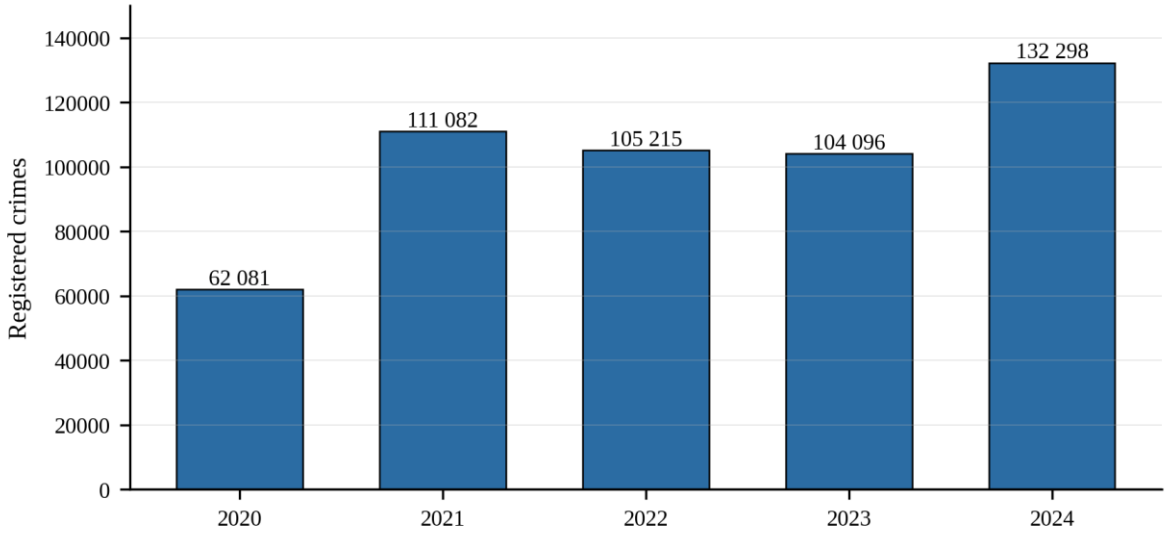

Fig. 1. Registered crimes in Uzbekistan, 2020–2024 (Statistics Agency / MoIA).

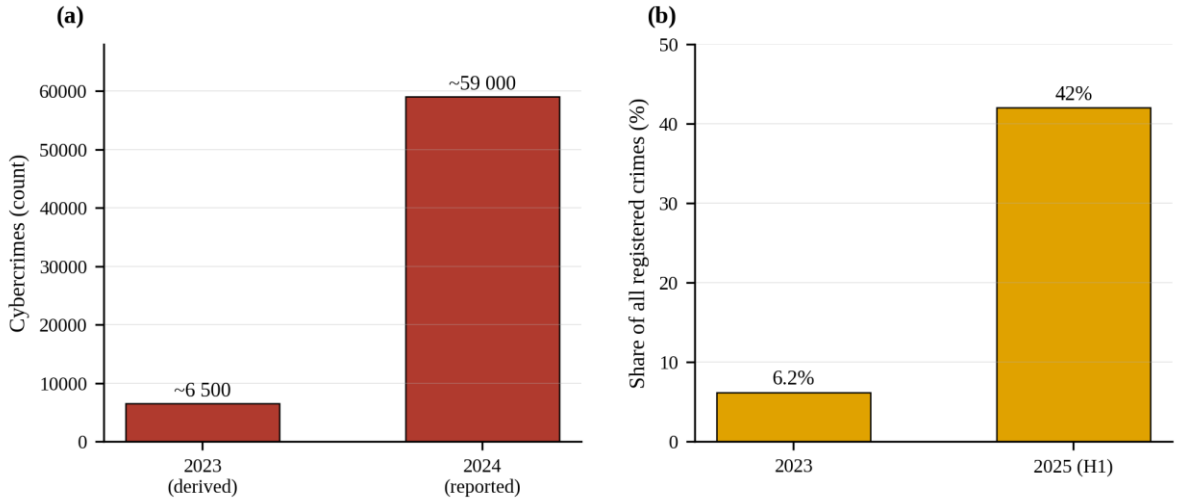

Fig. 2. Cyber-offences in Uzbekistan: (a) approximate counts for 2023 (derived from the reported share) and 2024 (reported); (b) share of all registered crime.

The shape of the trend is informative. The 2021 surge and the renewed jump in 2024 coincide with waves of digital-payment adoption, while the cyber share rises throughout the period, indicating that the growth is not an artefact of broader crime movements but a genuine change in how offences are committed. Even where total crime fluctuates, the cyber component keeps climbing, which is the defining feature of these years.

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

The recorded-fraud series tells a complementary story. Registered fraud reached 29,252 cases in 2024, a rise of 58.2% in a single year [6]. Not all recorded fraud is cyber-enabled and not all cyber-fraud is booked under that article, so the two series are related but not identical; read together, however, they move in the same direction, a fast-growing category of acquisitive crime in which deception, increasingly mediated by digital channels, is the common thread.

4.2 Structure of Cyber-Fraud Schemes

The composition of cyber-fraud is striking in its concentration on the banking channel: the MoIA reports that 98% of cybercrimes are related to bank cards [5]. By method, the Cybersecurity Centre attributes about 60% of episodes to malware and viruses, 16% to phishing aimed at extracting one-time SMS codes for cards and accounts, 11% to fraud on online marketplaces and classified-ad platforms, 9% to direct deception that persuades victims to part with money, and 4% to fraudulent online loans taken out in a victim's name (Fig. 3, Table 1) [5]. Although malware leads by count, the phishing, marketplace, deception, and online-loan categories are all, at root, social-engineering attacks on the user, so the human-facing share of the problem is larger than any single bar suggests.

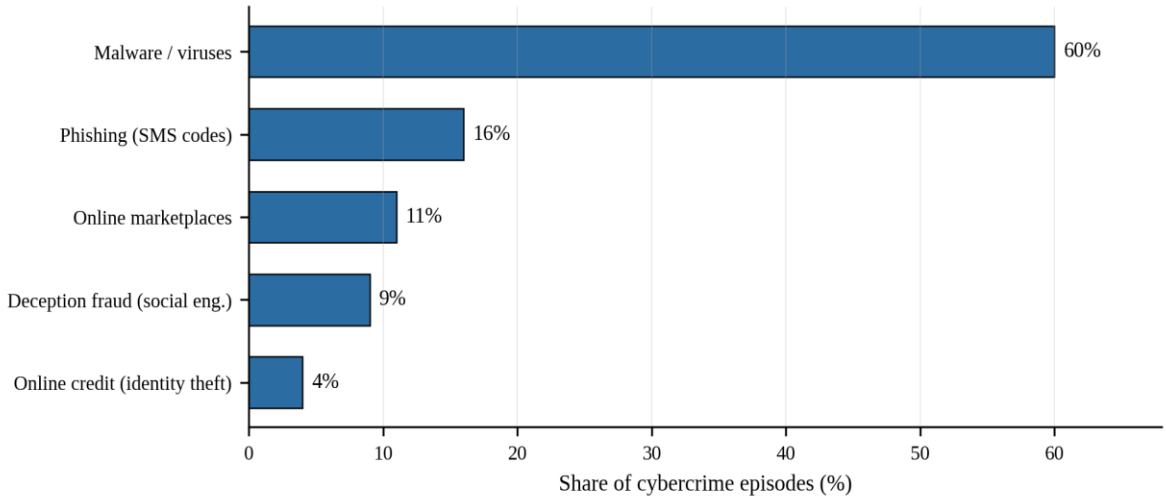

Fig. 3. Structure of cyber-fraud episodes by method (MoIA Cybersecurity Centre).

Table 1.

Typology of cyber-fraud schemes and primary countermeasures. *Shares by method, per the MoIA Cybersecurity Centre.

Scheme	Mechanism / channel	Share*	Primary countermeasure (level)
Malware / viruses	Malicious apps and links; device compromise to intercept codes	60%	Endpoint protection, app-store hygiene, awareness (technical / educational)
Phishing (SMS codes)	Tricking victims into revealing one-time codes for cards and accounts	16%	Anti-phishing filtering, never-share-OTP messaging (technical / educational)
Online marketplaces	Fake listings on classifieds and trading platforms	11%	Escrow, verified sellers, platform controls (organizational)

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

Deception fraud (social engineering)	Impersonation of banks, regulators or officials by call or messenger	9%	Call-ID verification, public awareness, bank call-back (educational / organizational)
Online credit (identity theft)	Loans taken out in the victim's name online	4%	Extra verification before disbursement (legal / organizational)

The mechanism behind most of these schemes is the same. Uzbek card payments are confirmed by a one-time code sent by SMS; if an attacker can persuade the holder to disclose that code, through a fake call, a spoofed message, or a malicious app that reads it, the transaction proceeds as if authorized. This is why phishing and deception loom so large despite strong cryptographic protection on the cards themselves: the weak link is the human confirmation step, not the cryptography. Defences that reduce reliance on shareable codes, or that make the moment of disclosure harder to exploit, therefore strike at the structural core of the problem.

It is worth stating the implication plainly. Although malware is the single largest category by count at 60%, it is frequently the delivery mechanism for the same goal, capturing the codes and credentials that authorize a transfer. When malware, phishing, marketplace fraud, deception, and fraudulent lending are read together as attacks on the user rather than on the cryptography, the human-facing share of the problem is overwhelming, and the design of countermeasures should reflect that balance.

4.3 Financial Impact and Protective Action

The monetary toll is heavy. Citizen losses exceeded 1.9 trillion UZS over 2021–2024, with 603 billion UZS lost in 2024 alone (Fig. 4a) [5]. Against this, protective action has begun to register: in 2024 the Central Bank, acting on citizens' complaints, blocked about 9.5 billion UZS of stolen funds on cards, and new verification rules introduced from November 2024 prevented the fraudulent issuance of online loans worth 304.1 billion UZS across 28,138 cases (Fig. 4b) [7]. The gap between losses and recovered or prevented sums underlines that interception after the fact cannot substitute for prevention, which motivates the model in Section 6.

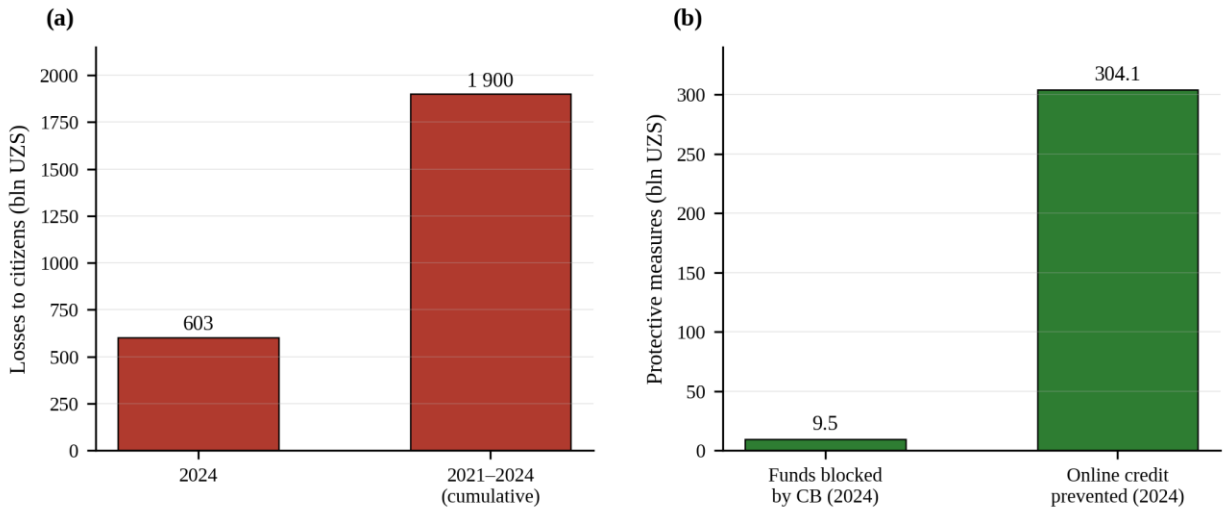

Fig. 4. Financial dimension (billion UZS): (a) losses to citizens; (b) funds blocked and fraudulent online loans prevented (CBU Annual Report 2024).

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

The contrast between the two panels of Fig. 4 is itself a finding. The 9.5 billion UZS blocked in 2024 is a small fraction of the 603 billion UZS lost that year, on the order of a few per cent, which shows that after-the-fact interception, however valuable, cannot match the scale of harm. The far larger sum prevented through online-loan verification, 304.1 billion UZS, carries the opposite lesson: prevention designed into the process, rather than recovery after the loss, is where the leverage lies.

Put as a ratio, the funds blocked in 2024 amount to roughly 1.6% of the losses recorded that year. Even allowing for sums recovered through channels not captured here, the order of magnitude makes the point: recovery operates at the margin, while losses occur at scale. This asymmetry is the strongest single argument in the data for moving investment from after-the-fact interception toward prevention at the point of attack.

A consolidated set of indicators is given in Table 2. The youth dimension deserves emphasis: a UNODC/UNDP programme reports that online fraud, gambling, and harassment among Uzbek youth aged 14–30 rose from about 20,000 cases in 2022 to over 30,000 in 2023, with associated financial losses climbing from USD 8.5 million to USD 25 million, and with disproportionate impact on women and vulnerable groups [8].

Table 2.

Consolidated indicators of cyber-fraud in Uzbekistan (open sources).

Indicator	Value	Source / status
Cybercrime growth, 2019-2024	×68 (about a 68-fold increase)	MoIA Cybersecurity Centre (press, 2025)
Cybercrimes, 2024	about 59,000 (×9.1 vs 2023)	MoIA (press, 2025)
Cybercrime share of all crime	6.2% (2023) -> about 42% (2025, H1)	MoIA (press, 2025)
Registered crimes, 2024	132,298 (+27.1% vs 2023)	Statistics Agency / MoIA
Registered fraud, 2024	29,252 (+58.2%)	Statistics Agency / MoIA
Losses to citizens, 2021-2024	over 1.9 trillion UZS	MoIA Cybersecurity Centre
Losses to citizens, 2024	603 billion UZS	MoIA (press, 2025)
Bank-card-related cybercrime	98% of cases	MoIA (press, 2025)
Funds blocked by Central Bank, 2024	9.5 billion UZS	CBU Annual Report 2024
Online loans prevented, Nov-Dec 2024	304.1 billion UZS in 28,138 cases	CBU Annual Report 2024
ITU Global Cybersecurity Index	89.20 in 2024 (from 71.11 in 2020), Tier 2	ITU GCI 2024

4.4 Who Is Harmed

The aggregate figures conceal an uneven distribution of harm. The UNODC and UNDP evidence indicates that young people, particularly those aged 14 to 30 and those not in

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

education or employment, are among the most affected, and that women and other vulnerable groups bear a disproportionate share [8]. A newly-banked, digitally-active but not yet digitally-cautious population is exactly the profile that social-engineering operations exploit. The practical consequence is that generic awareness efforts will under-serve the groups most at risk, so targeting, by age, by platform, and by language, is part of an effective response.

The language dimension deserves particular weight. Uzbekistan is a multilingual environment, and fraud scripts are localized in Uzbek and Russian; awareness materials that reach only one language community, or that use officialese rather than the plain phrasing of the scams themselves, will miss the people most exposed. Effective messaging mirrors the channel and register of the attack: short, concrete, and delivered where victims actually meet the lure.

5 Discussion: Drivers and the National–Global Comparison

Read together, the data point to a small number of drivers. The first is a mismatch between the speed of payment digitalization and the level of public cyber-hygiene, which leaves a large, newly-banked population exposed. The second is the dominance of social engineering: phishing, marketplace, deception, and online-loan fraud are all attacks on the user's judgment rather than on cryptographic or network defences, and together they account for the bulk of citizen-facing harm even though malware leads the count. The third is the bank card as the common point of failure, implicated in 98% of cases, which concentrates risk at the moment a one-time code is shared.

These drivers align closely with global findings. ENISA's identification of social engineering as the principal route to financial loss, and of smishing as the dominant channel in finance, is reproduced almost exactly in the Uzbek phishing-for-SMS-codes pattern [3]. The worldwide turn toward AI-amplified deception, deepfake voices and generative phishing now exceeding four-fifths of observed social-engineering activity, is a forward-looking risk for Uzbekistan, where the same techniques can be expected to raise the credibility of impersonation scams [2]. At the same time, the global measurement literature warns against over-reading headline loss figures, since reporting and recovery differ across systems [11]; the Uzbek totals should therefore be read as indicative of trend and order of magnitude rather than as precise accounting.

Table 3 summarizes this national-global correspondence.

Table 3.

Correspondence between the Uzbek pattern and global benchmarks.

Dimension	Uzbekistan (this study)	Global benchmark
Headline metric	losses over 1.9 trillion UZS (2021-2024); about 68x growth	FBI IC3: USD 16.6 billion in 2024, +33% [1]
Dominant attack form	social engineering (phishing, deception, marketplace, loans)	social engineering causes loss in about 50% of finance incidents [3]
Main channel	one-time SMS codes (smishing / vishing)	smishing the most common phishing channel in finance [3]

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

Primary target	bank cards (98% of cases)	banks the most targeted finance organisations (46%) [3]
AI involvement	emerging risk for impersonation scripts	over 80% of observed social engineering used AI by early 2025 [2]

The structural comparison reinforces the point. ENISA's finding that credit institutions are the entities most often impersonated, and that smishing is the dominant phishing channel in finance, lines up almost one to one with the Uzbek picture, where impersonation of banks and the regulator and the theft of SMS codes are the recurring moves [3]. Where the two diverge is in concentration: the Uzbek 98% card share is unusually high, which both raises exposure to a single failure mode and makes that mode an unusually clear target for intervention.

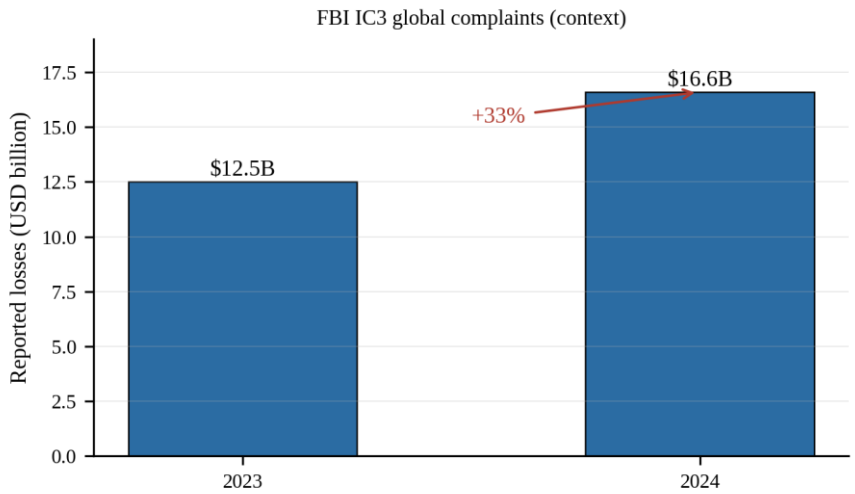

Fig. 5. Global context: reported losses to the FBI Internet Crime Complaint Center, 2023-2024 [1].

Two features of this benchmark (Fig. 5) carry forward. First, even in a mature reporting environment recorded losses understate the true total, because many victims never report; the same is certainly true in Uzbekistan, so the official figures are best read as a floor rather than a ceiling. Second, the steady year-on-year rise internationally indicates that the threat is structural rather than a passing spike, which is consistent with the sustained climb observed nationally.

Stepping back, the Uzbek case illustrates a general pattern in rapidly digitalizing economies: the security frontier moves to wherever value is easiest to extract, and at present that is the lightly defended human step in a card payment. As that step is hardened, displacement to other channels, instant-payment systems, investment scams, or account takeover, should be expected, so the picture here describes a moving target. The implication is that continuous monitoring and adaptation, rather than a one-time fix, must be built into the response.

The comparison also clarifies what is distinctive locally. The extreme growth multiple (about 68-fold) reflects a low starting base and very rapid digital adoption, while the 98% card concentration is sharper than in more diversified economies, suggesting that interventions targeted at the card-and-OTP pathway would yield outsized returns.

5.1 The AI Inflection

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

The most consequential near-term change is likely to be AI-amplified fraud at scale. The scripts that already cause the most harm in Uzbekistan, a caller claiming to be from a bank or a regulator, depend on credibility, and credibility is exactly what voice cloning and generative text improve. A deepfaked voice in Uzbek or Russian, or a flawless localized phishing message, removes the linguistic and tonal cues that currently help some victims detect a scam. Because the country's loss profile is concentrated in impersonation, it is unusually exposed to this shift, and defences that rely on users spotting clumsy fakes will weaken. This raises the premium on structural and technical controls that do not depend on the victim's vigilance.

The implication is not that awareness becomes useless but that its content must change. As fakes grow more convincing, advice shifts from spotting an error in the message toward never acting on an inbound contact and instead verifying independently through a known channel, a rule that holds even against a perfect imitation. Building systems and habits around independent verification is the most robust hedge against AI-amplified impersonation.

5.2 The Policy-Practice Gap

A second observation is worth naming. Uzbekistan scores highly on the ITU Global Cybersecurity Index, 89.20 in 2024, reflecting real progress in laws, institutions, and strategy [4]. Yet victimization rose steeply over the same period. The two are not contradictory: the index measures commitments and capacity, not outcomes, and institutional maturity takes time to translate into fewer victims, especially when adoption races ahead. The gap nonetheless argues for shifting emphasis from building capacity on paper to measuring and reducing actual citizen losses.

The 2025 requirement that financial institutions compensate clients harmed by the institution's own security failures is notable in this light, because it changes incentives. When a bank bears part of the cost of a successful fraud, it gains a direct reason to invest in detection, friction at the moment of disclosure, and customer education. Aligning incentives in this way is often more durable than mandates alone, and the planned public reporting of banks by incident frequency works in the same direction.

5.3 Speed of Adoption as a Driver

Underlying all of this is the pace of change. The same period that saw cybercrime grow roughly 68-fold also saw the mass adoption of cards, mobile banking, and online marketplaces by a population much of which had only recently entered the formal financial system. Rapid inclusion is a development success, but it concentrates a large number of inexperienced users into a short window, and fraud operations scale to meet them. The policy challenge is therefore not to slow inclusion but to pair it with proportionate, just-in-time protection at the moments of greatest risk.

The comparison with global figures should be read in this light. A 68-fold national rise is far steeper than the 33% annual increase in reported losses recorded internationally, but it begins from a much lower base and reflects an economy moving online very fast. The steepness signals urgency rather than exceptional criminality, and it implies that the window for building habits of caution among new users is now.

International experience with reimbursement is instructive here. Several jurisdictions have moved toward making financial institutions bear more of the cost of card and

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

authorized-payment fraud, on the reasoning that the party best able to detect and prevent abuse should hold the incentive to do so. Uzbekistan's 2025 compensation requirement places it within this trend, and the early prevention figures suggest the incentive is already producing protective behaviour; the open question is how far liability should extend before it begins to discourage legitimate service.

6 A Four-Level Countermeasures Model

The evidence supports organising responses on four interacting levels, each tied to specific findings and to the role of law-enforcement and regulatory bodies.

Why four levels, and why these? The structure follows the causal chain of a successful fraud. A scheme must be met legally to deter and prosecute it, technically to detect and block it, organizationally to coordinate the bodies that each see only part of the attack, and educationally to reach the user at the point of decision. Omitting any one leaves a gap the others cannot fill, which is why the model treats the levels as a set rather than a menu.

- Legal level. Sustain and refine the 2022 Cybersecurity Law and the 2025 measures that require financial institutions to compensate clients harmed by the institution's own security failures, and that tighten penalties. The verification rules that prevented 304.1 billion UZS of fraudulent online lending show that well-targeted regulation produces measurable prevention [7].
- Technical level. Concentrate defences on the card-and-OTP pathway that accounts for 98% of cases: anti-phishing and anti-smishing filtering, transaction monitoring and rapid blocking (which already recovered 9.5 billion UZS in 2024), and device-level protection against the malware that leads the episode count [5, 7].
- Organizational level. Strengthen threat-intelligence sharing between the MoIA Cybersecurity Centre, the Central Bank, and platforms, and operationalize the planned public reporting of banks by incident frequency to align institutional incentives; marketplace operators should add verified-seller and escrow controls for the 11% of fraud routed through them [3, 5].
- Educational level. Because most harm is social-engineering harm, sustained public awareness, never share a one-time code, verify any caller claiming to be a bank or official, is the highest-leverage cheap intervention, with particular attention to youth and other vulnerable groups identified by UNODC/UNDP [8].

The four levels are complementary rather than substitutable. Legal and technical measures harden the system and the card pathway; organizational measures align incentives and share intelligence; and educational measures address the human vulnerability that the other three cannot fully close. For a law-enforcement academy, the model also frames a training agenda: investigators need combined competence in financial forensics, threat intelligence, and the psychology of social engineering.

6.1 Implications for Law-Enforcement Capacity

For law-enforcement bodies, and for the academies that train their staff, the model implies a specific capability agenda. Investigating cyber-fraud requires a blend that traditional policing curricula seldom combine: financial forensics to follow money across cards and accounts, threat-intelligence skills to recognize and attribute recurring scripts, and a working understanding of the psychology of social engineering to reconstruct how victims were manipulated. Cross-border cooperation is increasingly necessary, since

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

infrastructure and proceeds often cross jurisdictions. The recent creation of dedicated cyber units and a specialized faculty within the police-education system is well aligned with the threat, and this analysis suggests prioritizing the card-and-OTP pathway, social-engineering literacy, and inter-agency intelligence sharing within that training.

A cross-border dimension also bears on the response. Fraud infrastructure, call centres, money-mule networks, and the reuse of stolen personal data, frequently spans national boundaries, as cases in the region illustrate. Effective countermeasures therefore reach beyond domestic policy to mutual legal assistance, joint operations, and the sharing of threat indicators with partner agencies abroad. For a national police academy, this argues for building investigators' fluency in international cooperation mechanisms alongside their technical skills.

Sequencing matters. In the short term, the highest-return steps are public-awareness campaigns focused on never disclosing one-time codes and on verifying callers, together with faster transaction blocking. In the medium term, reducing reliance on shareable SMS codes, strengthening marketplace controls, and institutionalizing intelligence sharing would address the structural core. In the longer term, anticipating AI-amplified fraud, through detection of synthetic voices and content and through continuously updated public guidance, will be necessary to keep pace with the adversary.

6.2 Measuring Success

Finally, the model needs metrics. Capacity indices such as the ITU GCI measure inputs and commitments; what is missing is a small set of outcome indicators that track whether citizens are actually safer. Candidates include total and per-capita losses, the recovery and prevention rates (the share of attempted theft blocked or reimbursed), the share of victims in targeted demographics, and the time from report to blocking. Publishing such indicators alongside the planned bank-level reporting would let policy be steered by outcomes rather than activity, and would make the contribution of each measure in the model visible.

Coordination ties the levels together. A technical block is only as fast as the intelligence that triggers it, a law is only as effective as the awareness that lets citizens benefit from it, and education is only credible when backed by visible enforcement and recovery. A standing mechanism that convenes the police cyber centre, the central bank, telecom operators, and platforms, with shared indicators and clear escalation paths, is the organizational backbone the model assumes.

The educational level deserves a concrete form. For the public it means continuous, plain-language campaigns delivered through the same channels the fraud uses, banks, telecom operators, and messengers, and reinforced rather than run once. For professionals it means embedding cyber-fraud literacy across the police-training curriculum, not as a niche specialism but as a routine competence, since almost every acquisitive-crime investigator now meets a digital element. A specialized faculty within the police academy is the natural vehicle for the latter.

7 Limitations

Several limitations follow from the data. Much of the national evidence comes from official press briefings rather than disaggregated statistical releases, so year-to-year definitions may shift and some values are derived rather than directly reported (Section 3). The analysis is descriptive and cannot establish causal effects of specific interventions.

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

Monetary comparisons across currencies are indicative only. Victim-level and demographic detail, which would reveal who is most affected and through which exact scripts, is largely unavailable in open sources. These gaps point to the value of primary research, anonymized victim surveys and case-file analysis conducted with the relevant authorities, to refine the descriptive baseline established here.

A further limitation concerns the attribution of effect. Where prevention figures are encouraging, such as the loans blocked by new verification rules, open data alone cannot separate the effect of the rule from concurrent changes in behaviour or enforcement; disentangling them would require administrative microdata under appropriate safeguards. And because the threat evolves quickly, any descriptive baseline dates rapidly, so the value of this synthesis lies in serving as a reference point against which future data can be compared.

These limitations define a research agenda. Priorities include anonymized victim surveys to map exact scripts and demographics, case-file analysis with the relevant authorities to trace money flows and recovery, evaluation studies that test which awareness messages and verification designs actually reduce losses, and monitoring of AI-enabled fraud as it emerges in the local language environment. Such work would convert the descriptive baseline established here into the evidence needed to target prevention precisely.

It should also be acknowledged that the author's institutional vantage point within the law-enforcement system shapes the emphasis of the countermeasures model toward policing and regulation; the educational and design dimensions, equally important, would benefit from the perspectives of educators and system designers in future collaborative work.

8 Conclusion

Cyber-fraud against citizens has become one of the defining security challenges in Uzbekistan: cybercrime has grown roughly 68-fold since 2019, now approaches half of all registered crime, and has cost citizens more than 1.9 trillion UZS over 2021-2024, overwhelmingly through the bank-card channel. Consolidating the open record shows that the national pattern is a sharp local instance of a global shift toward human-centered, increasingly AI-amplified social engineering. Because the harm is concentrated on the user and the card-and-OTP pathway, the most effective response is a coordinated four-level effort, legal, technical, organizational, and educational, that pairs system hardening and intelligence sharing with sustained public awareness. The early results of regulation and rapid blocking show that targeted measures work; the task now is to scale prevention ahead of an adversary that is itself adopting new tools.

For a law-enforcement academy the implications are concrete. The same evidence that describes the problem also defines a curriculum and an inter-agency agenda, and it identifies the card-and-OTP pathway and the human confirmation step as the points where prevention will pay off most. Translating this descriptive baseline into measured reductions in citizen losses, and doing so before AI-amplified fraud matures, is the central task ahead.

In sum, consolidating the open record is valuable in two ways. It gives policymakers and trainers a single, internally consistent picture of where harm is concentrated, and it sets a baseline against which the effect of new measures, and the arrival of new threats, can be

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

judged. The direction of travel is clear; the priority now is to measure progress and to act before the next wave of tools reaches the attacker.

References

1. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3): Internet Crime Report 2024. FBI, Washington, DC (2025). https://www.ic3.gov

2. European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape 2025. ENISA (2025). https://www.enisa.europa.eu

3. European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape: Finance Sector (January 2023 – June 2024). ENISA (2024). https://www.enisa.europa.eu

4. International Telecommunication Union (ITU): Global Cybersecurity Index 2024, 5th edn. ITU, Geneva (2024). https://www.itu.int

5. Ministry of Internal Affairs of the Republic of Uzbekistan, Cybersecurity Centre: Press briefing on cybercrime statistics, 29 May 2025. Reported by Gazeta.uz and Spot.uz (2025)

6. Statistics Agency under the President of the Republic of Uzbekistan: Registered crime statistics, 2020–2024 (2025). Reported by Gazeta.uz, 3 March 2025

7. Central Bank of the Republic of Uzbekistan: Annual Report 2024. CBU, Tashkent (2025). https://cbu.uz

8. United Nations Office on Drugs and Crime (UNODC), United Nations Development Programme (UNDP): Strengthening Resilience of Youth to Cybercrime and Digital Violence in Uzbekistan. Programme document (2025)

9. Verizon: 2024 Data Breach Investigations Report. Verizon Business (2024)

10. IBM Security: X-Force Threat Intelligence Index 2025. IBM (2025)

11. Anderson, R., Barton, C., Böhme, R., Clayton, R., et al.: Measuring the changing cost of cybercrime. In: Workshop on the Economics of Information Security (WEIS) (2019)

12. Hadnagy, C.: Social Engineering: The Science of Human Hacking, 2nd edn. Wiley, Indianapolis (2018)

13. Republic of Uzbekistan: Law on Cybersecurity, No. ZRU-764 (2022)

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