mamlakatda xavfsiz ijtimoiy muhitni mustahkamlash, jinoyatchilikning oldini olish hamda huquq-tartibot organlari faoliyatini raqamli va intellektual asosda rivojlantirishning muhim omillaridan biri hisoblanadi. Loyiha talabnomasida ham “Criminology AI” tizimi O‘zbekiston sharoitiga moslashtirilgan, o‘zbek tilida ishlovchi, real ma’lumotlar bilan ishlaydigan va jinoyatchilikni barvaqt oldini olishga xizmat qiluvchi milliy platforma sifatida asoslangan.

**Foydalanilgan manbalar / References**


1. O‘zbekiston Respublikasi Prezidentining “Jamoat xavfsizligini ta’minlash va jinoyatchilikka qarshi kurashish sohasini ilmiy tadqiq qilish faoliyatini sifat jihatidan yangi bosqichga ko‘tarish chora-tadbirlari to‘g‘risida”gi Farmoni. 2024-yil 15-yanvar, PF–10-son // Qonunchilik ma’lumotlari milliy bazasi. — URL: https://lex.uz/docs/-6755597
2. O‘zbekiston Respublikasi Prezidentining “Kriminologiya sohasida ilmiy-amaliy tadqiqot ishlarini tashkil etish chora-tadbirlari to‘g‘risida”gi Qarori. 2024-yil 15-yanvar, PQ–22-son // Qonunchilik ma’lumotlari milliy bazasi. — URL: https://lex.uz/docs/-6755253
3. O‘zbekiston Respublikasi Vazirlar Mahkamasining “Kriminologik faoliyatni ilmiy ta’minlash chora-tadbirlari to‘g‘risida”gi Qarori. 2024-yil 24-iyul, 445-son // Qonunchilik ma’lumotlari milliy bazasi. — URL: https://lex.uz/docs/-7034904
4. O‘zbekiston Respublikasi Prezidentining “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi Qarori. 2024-yil 14-oktyabr, PQ–358-son // Qonunchilik ma’lumotlari milliy bazasi. — URL: https://lex.uz/docs/-7158604
5. National Institute of Justice. Artificial Intelligence [Electronic resource]. — Washington, D.C.: National Institute of Justice. — URL: https://nij.ojp.gov/topics/artificial-intelligence
6. National Institute of Justice. Overview of Predictive Policing [Electronic resource]. — Washington, D.C.: National Institute of Justice. — URL: https://nij.ojp.gov/topics/articles/overview-predictive-policing
7. Perry W.L., McInnis B., Price C.C., Smith S.C., Hollywood J.S. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. — Santa Monica: RAND Corporation, 2013. — 186 p.
8. Mohler G.O., Short M.B., Brantingham P.J., Schoenberg F.P., Tita G.E. Randomized Controlled Field Trials of Predictive Policing // Journal of the American Statistical Association. — 2015. — Vol. 110, № 512. — P. 1399–1411.
9. Ratcliffe J.H. Intelligence-Led Policing. — 2nd ed. — London; New York: Routledge, 2016. — 234 p.
10. Ferguson A.G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. — New York: New York University Press, 2017. — 272 p.
11. https://www.gazeta.uz/oz/2025/11/05/cybercrime/


# FINANCIAL FRAUD THROUGH THE THEFT OF BANK CARD DATA: A SYSTEMATIC ANALYTICAL REVIEW


**Ulugbek Choriyev**

*Research fellow of Research Institute of Criminology of the Republic of Uzbekistan*

*O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti ilmiy xodimi*

*Исследовательский институт криминологии Республики Узбекистан, научный сотрудник*



***Abstract.*** *Theft of bank payment card data is among the most widespread forms of financial fraud, yet the techniques involved are frequently studied in isolation rather than as components of a single monetization process. This article addresses that gap by systematizing, within one analytical framework, the principal methods of obtaining payment card credentials – the card number, expiry date, security code, and one-time confirmation password – together with the subsequent use of the stolen data and the mechanism through which financial harm accrues. The study is analytical rather than empirical: it applies comparative, systematic, and descriptive-statistical approaches to a body of secondary material comprising peer-reviewed publications, industry security reports, and international legal instruments. The analysis classifies the theft techniques by their technical features, distinguishing device-based methods (skimming and shimming) from digital methods (phishing, fake payment pages, and electronic skimming), and then traces how the resulting credentials circulate through underground carding markets before being converted into monetary loss and proposes directions for further research, particularly empirical measurement in the context of Uzbekistan.*



***Keywords:*** *financial fraud; bank card data; phishing; skimming; e-skimming; carding; one-time password; cybersecurity.*


***MOLIYAVIY FIRIBGARLIK: BANK KARTA MA’LUMOTLARINING O‘G‘IRLANISHI***


***Annotatsiya.*** *Bank to‘lov kartalari ma‘lumotlarini o‘g‘irlash moliyaviy firibgarlikning keng tarqalgan shakllaridan biri hisoblanadi, ammo jalb qilingan usullar ko‘pincha yagona iqtisodiy jarayonining tarkibiy qismlari sifatida emas, balki alohida o‘rganiladi. Ushbu bo‘shliqni bitta tahliliy doirada, to‘lov kartasining hisobga olish ma’lumotlarini olishning asosiy usullarini – karta raqami, amal qilish muddati, xavfsizlik kodi va bir martalik tasdiqlash paroli, shuningdek, o‘g‘irlangan ma’lumotlardan keyingi foydalanish va moliyaviy zarar yetkazish mexanizmini tizimlashtirish orqali hal qiladi. Tadqiqot empirik emas, balki analitikdir: u ko‘rib chiqilgan nashrlar, sanoat xavfsizligi hisobotlari va xalqaro huquqiy hujjatlarni o‘z ichiga olgan ikkilamchi materiallar to‘plamiga qiyosiy, tizimli va tavsifiy-statistik yondashuvlarni qo‘llaydi. Tahlil o‘g‘rilik usullarini texnik xususiyatlariga ko‘ra tasniflaydi, qurilmaga asoslangan usullarni (skimming va shimming) raqamli usullardan (fishing, soxta to‘lov sahifalari va elektron skimming) ajratadi, so‘ngra natijada olingan hisob ma’lumotlari pul yo‘qotishga aylantirilgunga qadar yer osti kartalari bozorlarida qanday aylanayotganini kuzatib boradi va keyingi o‘lchovlar uchun, xususan, O‘zbekistonda empirik o‘lchash yo‘nalishlarini taklif qiladi.*



***Kalit so‘zlar:*** *moliyaviy firibgarlik; bank kartasi ma’lumotlari; fishing; skimming; elektron skimming; karta ma’lumotlarini qidirish; bir martalik parol; kiberxavfsizlik.*

The rapid expansion of digital payments has produced convenience alongside a new field of risk: the credentials of a bank payment card have become a highly liquid commodity for cybercriminals. Bank card data – the primary account number (PAN), expiry date, cardholder name, and, most critically, the security code (CVV/CVC) together with the one-time password (OTP) confirming a transaction – becomes a target of theft precisely because it can be converted directly into monetary value.

The relevance of the subject is confirmed by statistical indicators. According to data attributed to the United States Federal Trade Commission, card fraud was the most frequently reported type of identity theft in 2024, with more than 449,000 reports recorded approximately 8 per cent higher than in 2023 – while consumer losses to fraud exceeded USD 12.5 billion, a 25 per cent increase over the preceding year [1]. The theft of card data is also large-scale in international markets: more than 119 million payment card credentials were reportedly posted or offered for sale online during 2023 [2, 3].

The matter is of particular significance in the context of Uzbekistan. As the use of bank cards and mobile payment applications has spread, cases of card-data theft through phishing and fake payment pages have risen sharply. According to figures attributed to the Cybersecurity Centre of the Ministry of Internal Affairs of the Republic of Uzbekistan, the number of crimes committed with the aid of information technology grew from 863 in 2019 to 58,800 in 2024; over 2021 – 2024 more than USD 148.9 million was stolen from citizens, with approximately 98 per cent of cases relating to theft or fraud involving bank cards [4]. The trend has intensified further: cybercrime cases reportedly increased roughly elevenfold over five years – from 4,865 to 62,440 with damage of 3.73 trillion sum, and 483 phishing programmes and 1,508 malicious links were blocked [5].

The scholarly problem is that the methods of card-data theft (phishing, skimming, e-skimming, carding, and others) are often examined separately in the literature, while their connection as a single economic chain – from theft through to the monetization of stolen data on the carding market – remains insufficiently systematized. This fragmentation in turn leads to the piecemeal application of protective measures.

This article is analytical (review) in character: it does not conduct a new empirical experiment but rather synthesizes existing scholarly literature, industry reports, and international instruments through comparative and systematic analysis in order to generalize the methods of card-data theft and their consequences. The **aim** of the study is to systematize the methods of stealing bank card data and to analyze their role in the formation of financial harm. From this aim, the following **objectives** were defined:

1. to analyze and classify the principal methods of card-data theft (phishing, fake payment pages, skimming/e-skimming, carding, CVV/OTP deception);
2. to examine the subsequent use of stolen data and its circulation on the carding market;
3. to generalize the mechanism by which financial harm is formed;
4. to outline the context of legal qualification and to formulate practical recommendations.

This analytical work is based not on empirical testing but on the systematic study of existing sources and financial-sector reports. The following methods were applied:

• **Comparative-analytical method**, used to compare the methods of card-data theft with one another according to their technical features and effectiveness.

• **Systematic approach**, used to consider individual methods as links in a single economic chain extending from theft to monetization.

• **Descriptive-statistical analysis**, used to aggregate the quantitative data contained in reports on financial fraud.

• **Formal-legal method**, used to delineate the context of the legal qualification of the conduct concerned.

**Source base.** Several categories of source were drawn upon: (a) peer-reviewed international scholarly publications (academic research on the cloning of EMV cards, defence against e-skimmers, and the detection of payment fraud through machine learning) [6, 7, 8, 9]; (b) industry and security reports and statistical sources [1, 2, 3, 10, 11, 12, 13, 14, 15]; (c) official and academic sources relating to Uzbekistan (statistics of the Ministry of Internal Affairs Cybersecurity Centre and national peer-reviewed analyses) [4, 5, 16]; and (d) international and national legal instruments – the Council of Europe Convention on Cybercrime [17] and the Criminal Code and sectoral laws of the Republic of Uzbekistan [18, 19, 20, 21]. The legal norms should be additionally verified by the author against the current redaction via lex.uz.

A **limitation** of the study is that the statistical indicators cited reflect the state of affairs at the time the sources were published and remain relative in a rapidly changing field.

**A general framework for card-data theft**

It is expedient to divide the methods of stealing payment card data into two broad groups: (1) **physical/device-based methods** – skimming and shimming, that is, the capture of data from physical devices such as ATMs or payment terminals; and (2) **digital/online methods**–phishing, fake payment pages, and e-skimming, that is, the acquisition of data within the internet environment. Both groups ultimately produce the same product – saleable card credentials–and therefore feed into a common "carding" economy (Section 3.5).

**Phishing and fake payment pages**

Phishing is a method of deceiving a user, in the name of a trusted organization (a bank, payment system, or government service), into voluntarily entering card credentials. According to the Verizon [15] *Data Breach Investigations Report*, phishing remains one of the principal vectors in credential-related breaches, and users often respond to a phishing message in less than a minute: on average 21 seconds elapse before a link is clicked and a further 28 seconds before data is entered [15]. In its analysis of the finance sector, ENISA [11] notes that phishing, smishing (phishing via SMS), and vishing (deception via telephone call) are the principal forms of social-engineering attack, with individuals targeted in approximately 38 per cent of cases and banks in 36 per cent.

A fake payment page is the technical manifestation of phishing, operating through a page that imitates the interface of a legitimate bank or payment system. When a user is directed to such a page (typically via a malicious link), they enter the card number, expiry date, and CVV code, and these data are transmitted directly to the attacker's server. The ENISA [11] report specifically emphasizes the large-scale theft of card data resulting from the impersonation of banks and from successful phishing and smishing.

**Skimming, shimming, and e-skimming (Magecart)**

**Skimming** is a method of capturing the data on a card's magnetic stripe together with the PIN by installing a concealed device on the card-reading mechanism of an ATM or point-of-sale (POS) terminal. According to industry data, card skimming remains a serious threat causing financial institutions and consumers more than a billion dollars in losses annually [12]. **Shimming** is an advanced variant carried out through a thin device inserted inside the card reader and adapted to obtain data from EMV chip cards [12]. The academic literature has demonstrated certain vulnerabilities of the EMV protocol, including the possibility of cloning chip cards through the "pre-play" attack [6]; this implies that stolen data may be transferred to a counterfeit card.

**E-skimming**, or the **Magecart** attack, is a method in which malicious JavaScript code is covertly placed on the checkout page of an e-commerce site so that the card credentials entered by a user are stolen in real time. According to Imperva [13], Magecart is a generic term applied to criminal groups that steal payment data from online payment pages, with the attack carried out by injecting malicious code into a legitimate page (web skimming). Researchers observe that the malicious script "reads" the fields for the card number, expiry date, and security code (CVC) and sends the data to the attacker's server; to avoid detection, the code is heavily obfuscated and sometimes equipped with a self-deleting mechanism [13, 14]. Such campaigns have been reported to target several major payment networks, including American Express, Discover, and Mastercard [14]. The academic literature has also proposed defences against e-skimmers, including a reverse-proxy approach [9].

**CVV and OTP deception (social engineering)**

In modern payment systems the one-time password (OTP) is used as an additional protective layer confirming a transaction. However, although the OTP is more advanced than a static password, it can be circumvented through social engineering and interception: fraudsters frequently impersonate bank employees to induce a user to disclose a temporary code [22]. The OTP delivered via SMS is especially vulnerable to SIM-swap and network-level attacks [22]. According to the United Kingdom fraud-prevention organization Cifas, the number of unauthorized SIM-swap cases in 2024 rose from 289 in 2023 to almost 3,000 – a sharp increase of 1,055 per cent [23]. CVV and OTP deception thus relies more on the human factor than on technical compromise – persuading the user to disclose a secret code – and enables the credentials to be completed into a full "set" with which a transaction can be finalized.

**Use of stolen data and the carding market**

Stolen card data, regardless of the method by which it was obtained, is often monetized not directly by the person who stole it but through hidden (dark-web) markets where it is first sold. **Carding** is the general term for the use of stolen card credentials in fraudulent transactions and their trade. According to analyses, dark-web markets operate similarly to legitimate e-commerce sites: they feature vendor ratings, buyer reviews, and escrow services that ensure "trust" among criminals while anonymity is maintained through the Tor network [2, 24]. At the end of 2023, card data was the most heavily advertised type of threat on dark-web channels, accounting for approximately 81 per cent of illicit offerings [2]. One of the largest markets – Yale Lodge – accounted for nearly half of the Bitcoin payments directed to vendors of stolen data in May 2023 [24]. The instability of such markets (exit scams and closure by law enforcement) is also observed [10].

From an economic perspective, this market specializes the act of theft: the person who steals the data (skimmer/phisher), the person who sells it (vendor), and the person who uses it (carder) are often different individuals. In this way the individual technical methods (Sections 3.2-3.4) become entry points into a single distributed economic chain.

**The mechanism of financial harm**

Financial harm is formed in several stages: (a) **direct harm** – the withdrawal of funds from the cardholder's or bank's account through a fraudulent transaction; (b) **indirect harm** – the bank's chargeback obligations, investigation costs, and reputational damage; and (c) **systemic harm** – the decline of consumer trust and the additional expenditure devoted to protective measures. The Federal Trade Commission data reported by The Motley Fool [1] and the card-fraud statistics [2] reflect precisely the aggregate scale of this harm

**Summary table of results**

**Principal methods of bank-card fraud**

Each method is characterized by its mechanism of action, the credential data it targets, and its principal consequence.

| METHOD | PRINCIPAL MECHANISM | TARGET DATA | PRINCIPAL CONSEQUENCE |
|---|---|---|---|
| 01 Phishing / fake page | Deceptive entry of credentials on a counterfeit page [11, 15] | PAN, Expiry, CVV | Full disclosure of credentials |
| 02 Skimming / shimming | Copying card data via a physical device at the terminal [6, 12] | Magnetic stripe / chip, PIN | Creation of a counterfeit card |
| 03 E-skimming (Magecart) | Malicious JavaScript injected into the checkout page [13, 14] | PAN, Expiry, CVC | Real-time mass theft |
| 04 CVV / OTP deception | Social engineering and SIM-swap interception [22, 23] | CVV, OTP | Completion of a fraudulent transaction |
| 05 Carding | Sale and use of data on hidden (darknet) markets [2, 24] | Stolen credentials | Monetization of the stolen data |

*Note: the table is an analytical generalization; in a concrete attack scenario the methods may be used in combination.*

**Context of legal qualification**

The conduct described above combines several distinct criminal elements in legal terms. The Convention on Cybercrime [17] defines illegal access to computer systems, illegal interception of data, data interference, and computer-related fraud as separate offences. In the Republic of Uzbekistan, such conduct is qualified primarily under the fraud provisions of the Criminal Code (Article 168–the acquisition of another's property or of a right to property through deception or abuse of trust) and under the articles of the chapter on "Crimes in the field of information technology," including the provision (Article $278^2$) concerning the unlawful (unauthorized) use of computer information [18]. The precise dispositions and sanctions of these articles should be verified against the current redaction via lex.uz [VERIFY against current redaction at lex.uz]; the article numbers cited here must not be relied upon until confirmed. The object of such conduct – payment relations and personal data – is regulated at the national level by sectoral laws: the Law on Payments and Payment Systems [20], the Law on Banks and Banking Activity [19], and the Law on Personal Data [21]. These instruments must likewise be confirmed by the author in their current redaction [VERIFY against current redaction at lex.uz].

The results of the analysis advance several generalized conclusions. **First**, the technically diverse methods of card-data theft (from physical skimming to digital e-skimming) produce the same end product – saleable card credentials – and it is therefore more effective to consider them not separately but as links in a single economic chain, which enhances the efficacy of protection.

**Second**, the "division of labour" underlying the theft is noteworthy: owing to the existence of the carding market, the person who steals the data and the person who uses it are often different individuals [2, 24]. This circumstance complicates legal qualification – theft, the sale of data, and the fraudulent transaction may constitute separate acts – and renders international cooperation, within the framework established by the Convention on Cybercrime [17], necessary.

**Third**, the predominance of the social-engineering factor is evident: CVV and OTP deception, as well as phishing, rely more on the abuse of user trust than on technical compromise [11, 15, 22]. The sharp rise in SIM-swap cases [23] indicates that SMS-based OTP cannot remain the sole protection and makes the transition to phishing-resistant authentication methods a pressing concern.

**Fourth**, for the context of Uzbekistan these results have practical significance: as digital payments spread, user-awareness programmes should not remain at the level of "do not click links" but should also encompass the skills of recognizing a fake payment page, never disclosing the CVV or OTP to anyone, and verifying the official channels of banks. This observation stands in a complementary relation to the earlier analyses in this series devoted to phishing links and fake websites.

The **limitations** of the study are acknowledged: the article relies on secondary sources and does not present its own empirical measurements; the statistical indicators reflect the state of the sources at the time of their publication; and the national figures relating to Uzbekistan are drawn from official reports (the Ministry of Internal Affairs Cybersecurity Centre), whose categorization changes rapidly. The classification presented should therefore be interpreted as an analytical framework rather than a universal regularity.

The study systematically analyzed the methods of stealing bank card data and their financial consequences, arriving at the following principal conclusions:

**1. The methods are links in a single chain.** Although phishing, fake payment pages, skimming/shimming, e-skimming (Magecart), CVV/OTP deception, and carding differ technically, they constitute a single economic chain extending from theft to monetization.

**2. The human factor is the central point.** Many methods (phishing, CVV/OTP deception) rely on the abuse of user trust rather than on technical compromise; reliance on technical protection alone is insufficient.

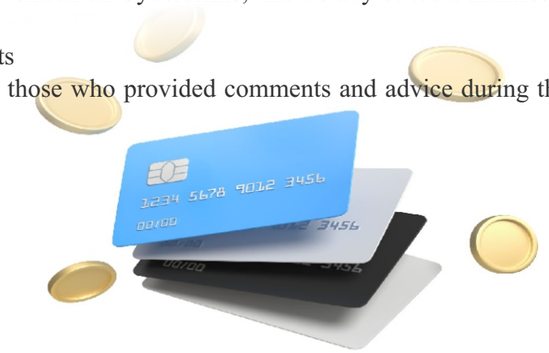
**3. Protection must be layered.** Measures appropriate to each link of the chain (user, bank, commercial platform) – training, transaction monitoring, page-integrity control, and phishing-resistant authentication – are effective only in combination.

Practical recommendations: (a) to extend user training with the skills of recognizing a fake payment page and not disclosing the CVV/OTP; (b) to strengthen the real-time detection of anomalous transactions and card-tokenization mechanisms at banks; (c) to monitor the integrity of the payment page (script monitoring, Content Security Policy) on e-commerce platforms; and (d) to transition gradually from SMS-based OTP to more phishing-resistant authentication methods.

As **directions for further research**, the following are proposed: the empirical measurement of card-fraud incidents in Uzbekistan, an analysis of the conformity of national legal qualification with the standards of the Convention on Cybercrime, and a study of local manifestations of the carding market.

Acknowledgements

The author thanks those who provided comments and advice during the preparation of this article.




**References / Foydalanilgan manbalar**

1. The Motley Fool. (2025). Identity theft and credit card fraud statistics for 2025. https://www.fool.com/money/research/identity-theft-credit-card-fraud-statistics/
2. H25. (2024). Stolen credit cards for sale: How the dark-web carding economy works. https://www.h25.io/dark-web/stolen-credit-cards-for-sale-how-the-dark%E2%80%91web-carding-economy-works/
3. Trend Micro. (2023). Over 30 million stolen credit card records being sold on the dark web. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over -30-million-stolen-credit-card-records-being-sold-on-the-dark-web
4. Gazeta.uz. (2025, May 31). Cybercrimes in Uzbekistan increase 68-fold in five years (based on data of the Cybersecurity Centre of the Ministry of Internal Affairs of the Republic of Uzbekistan). https://www.gazeta.uz/en/2025/05/31/cybercrime/
5. Kun.uz. (2025, December 23). Cybercrime cases surge elevenfold across Uzbekistan. https://kun.uz/en/news/2025/12/23/cybercrime-cases-surge-elevenfold-across-uzbekistan
6. Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. (2014). Chip and skim: Cloning EMV cards with the pre-play attack (arXiv:1209.2531). arXiv. https://arxiv.org/pdf/1209.2531
7. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University – Computer and Information Sciences, 35(1), 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008
8. Strelcenia, E., & Prakoonwit, S. (2023). Improving classification performance in credit card fraud detection by using new data augmentation. AI, 4(1), 172–198. https://doi.org/10.3390/ai4010008
9. [CITATION NEEDED – author to supply complete bibliographic details for "NAISS: A reverse proxy approach to mitigate MageCart's e-skimmers in e-commerce," Computers & Security, Elsevier. https://www.sciencedirect.com/science/article/pii/S0167404824000981]
10. Clearly Payments. (2024). Credit card fraud statistics in 2024 for USA. https://www.clearlypayments.com/ blog/credit-card-fraud-statistics-in-2024-for-usa/
11. ENISA. (2025). ENISA threat landscape: Finance sector, January 2023 to June 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf
12. Focal. (n.d.). What is card skimming and how to stay safe from ATM fraud? Retrieved June 4, 2026, from https://www.getfocal.ai/blog/what-is-card-skimming
13. Imperva. (n.d.). What is Magecart: Attack examples & prevention techniques. Retrieved June 4, 2026, from https://www.imperva.com/learn/application-security/magecart/
14. The Hacker News. (2026, January). Long-running web skimming campaign steals credit cards from online checkout pages. https://thehackernews.com/2026/01/long-running-web-skimming-campaign.html
15. Verizon. (2024). 2024 data breach investigations report: Executive summary. https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf
16. World Bulletin of Management and Law. (2025). Cybercrimes committed through phishing and ransomware attacks in Uzbekistan: Analysis and protective measures. https://scholarexpress.net/index.php/wbml/article/view/5179 [CITATION NEEDED – author(s) name(s) to supply]
17. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). https://rm.coe.int/1680081561
18. Criminal Code of the Republic of Uzbekistan (1994, as amended). Lex.uz. https://lex.uz/docs/-111453 [VERIFY against current redaction at lex.uz]
19. Law on Banks and Banking Activity of the Republic of Uzbekistan (No. ZRU-580, November 5, 2019). Lex.uz. https://lex.uz/docs/-4581969 [VERIFY against current redaction at lex.uz]
20. Law on Payments and Payment Systems of the Republic of Uzbekistan (No. ZRU-578, November 1, 2019). Lex.uz. https://lex.uz/docs/-4574008 [VERIFY against current redaction at lex.uz]
21. Law on Personal Data of the Republic of Uzbekistan (No. ZRU-547, July 2, 2019). Lex.uz. https://lex.uz/docs/-4396419 [VERIFY against current redaction at lex.uz]
22. IDlayr. (n.d.). The problem with SMS OTPs: Why this 2FA method isn't as secure as you think. Retrieved June 4, 2026, from https://idlayr.com/blog/sms-otp-2fa-fraud/
23. TechCrunch. (2024, May 13). "Got that boomer!": How cybercriminals steal one-time passcodes for SIM swap attacks and raiding bank accounts. https://techcrunch.com/2024/05/13/cyber-criminals-stealing-one-time-passcodes-sim-swap-raiding-bank-accounts/
24. Elliptic. (2023). Largest stolen credit card market shunned by cybercriminals after alleged "exit scam." https://www.elliptic.co/blog/analysis/largest-stolen-credit-card-market-shunned-by-cybercriminals-after-alleged-exit-scam