Uzbekistan



10.7% of adults in Uzbekistan are scammed each year, losing US$91.2 million.

Population 37.1 million · Latest figures: 2025

The Interior Ministry's Cybercrime Center recorded 58,800 crimes using information technology in 2024, 9.1 times the year before, and those crimes were 44.4 percent of every crime recorded that year. Citizens lost 603 billion soums in the 2024 cases. The centre had counted 863 such crimes in 2019 and 4,865 in 2021. By the end of 2025 the ministry put the annual count at 62,440. In the first nine months of 2026 it recorded 69,962 crimes using information technology, and the loss to citizens was approaching 1 trillion soums.

The Interior Ministry leads the work. A presidential resolution of 30 April 2025, in force from 6 May, made the ministry the body that sets one way of working and coordinates the police, the prosecutors, the security service, the central bank, the banks and the payment firms. Inside the ministry, 2026 is the Year of Combating Cybercrime. A decree of 10 March 2026 set a national cybersecurity strategy for 2026 to 2030, including simpler ways for people to report. A decree of 10 November 2026, in force the next day, orders a legal draft by December 2026 for a round-the-clock centre, staffed by the ministry and the banks, that follows the money when a report of online fraud or theft comes in.

PEOPLE SCAMMED

2,519,461

10.7% of adults

Scammers reach people on the phone they already use. At a press conference on 9 October 2026, the deputy head of the ministry's cybercrime department said about half of these crimes work by persuading someone to install a harmful app file. The file arrives on Telegram as a wedding invitation, a photo from a person they know, or a message of condolence. Once it is installed, the sender can reach the data on the phone and the bank card.

A second script takes the Telegram account itself. The message pretends to be a manager or a friend and asks for a login code, often dressed up as a vote in a contest. The scammers then read the chats and write to colleagues and friends asking for money, sometimes in the name of the police or an anti-corruption body. Other calls claim to be from a bank or a state office and ask for card details and a text-message code. The same official said state bodies do not ask for those details by phone. Further pitches are a seller who wants the full price before any goods are sent, and someone promising to double the money in a short time.

He said 90 percent of the crimes are run from abroad, and 10 percent are people inside Uzbekistan who help those operations. The ministry has been explaining a checker app called Qo'riqchi in workplaces, schools and among pensioners. Three million people had joined it by that October briefing.

PEOPLE WHO LOST MONEY

1,446,214

57% of victims

Almost all of the recorded crime is a payment. In 2024, 98 percent of the cybercrimes the centre counted were theft and fraud involving bank cards. In the first nine months of 2026 the deputy minister said the 69,962 crimes were mostly money taken through electronic payment systems. On reports to the ministry's Cardblock platform from 1 January to 1 October 2026, the central bank counted 18,830 cases of harmful software on a phone, worth 79.3 billion soums, and 611 cases in which the person was talked through instructions on a call, worth 27.7 billion soums. Crypto-assets move what is taken: in 2025 the ministry said 2,424 offences involved crypto, and 76 billion soums in criminal proceeds were stopped from leaving the country in that form.

A payment can be stopped while it is still in the system. The ministry, the central bank and the prosecutor general run a block on cards tied to a suspicious transfer. In the first nine months of 2026 that block stopped 77.344 billion soums from being taken out and shut 43,001 cards linked to crime. A law of 4 March 2025 lets a person ban any credit agreement in their own name, and a lender must check that ban before granting an online loan. Before a transfer in a bank or payment app is confirmed, the firm must show a warning the customer can use to confirm they are acting without a scammer. Apps are also required to warn when the phone shows signs of harmful software.

MONEY LOST

US$91.2m

UZS 1.15tn in a year, 0.06% of GDP

The 2024 cases took 603 billion soums from citizens. The centre's statement for 2021 to 2024 put the loss above 1.9 trillion soums. In a briefing on 23 December 2025 the ministry said the five years to 2025 had cost citizens 3.73 trillion soums, of which 1.89 trillion soums fell in the first 11 months of 2025. In the first nine months of 2026 the loss was approaching 1 trillion soums, and investigators had returned more than 210 billion soums of it. The ministry's October count is more than 209 billion 934 million soums handed back to more than 19,000 people, after 120.49 billion soums to more than 13,000 people in the first half of the year.

Of 278.3 billion soums reported on Cardblock between 1 January and 1 October 2026, prompt action blocked 113.1 billion soums. Where the loss is an online loan taken by fraud, a central bank regulation registered on 21 January 2026 stops the interest, the penalties and the collection once an investigator, a prosecutor or a court recognises the person as the victim. Money already taken is returned to the person's card, or to an account they name, within 15 days of the court ruling taking effect. The lender may then recover that sum from the person who committed the fraud. The April 2025 resolution also provides for loss caused by a bank or payment firm that missed its cybersecurity duties to be recovered from that firm.

MONEY RETURNED

US$2.9m

3.1% of the money lost

US$2.9m (UZS 35.96b) of it was returned to victims, 3.1% of the money lost.

REPORTED

75%

of victims reported it

People report these crimes to the Interior Ministry, and the numbers are rising. The Cybercrime Center recorded 58,800 crimes using information technology in 2024, and the ministry later put the 2025 count at 62,440. In the first nine months of 2026 the ministry recorded 69,962 such crimes. At the May 2025 press tour the centre said complaints from people and firms about offences in cyberspace had risen 34-fold. A separate national series, every fraud the police register, was 29,252 in 2024 and 44,127 in 2025.

Card and wallet complaints are logged on the ministry's Cardblock platform, which the central bank analyses. From 1 January to 1 October 2026 the central bank put the loss on those fraud reports at 278.3 billion soums, of which prompt action blocked 113.1 billion soums, and set aside a further 2,737 reports, worth 7.6 billion soums, which were automatic repayments of loans the person already had. Banks and payment firms keep a fraud-report section inside their apps, under a regulation in force from April 2026. The national computer emergency team, UZCERT, receives reports of fake pages and harmful links, while card theft is handled by the ministry's cybersecurity units. The ministry has opened contacts with Google, Meta and Telegram about who is running the scams. A decree of 10 November 2026 orders a draft, by December, for a round-the-clock centre of the ministry and the banks that tracks the money when a report arrives.

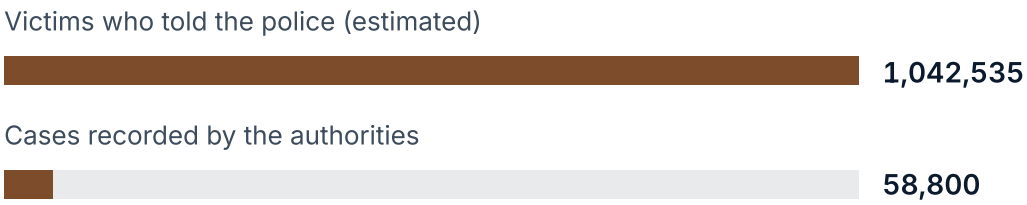
POLICE RECORDS

58,800

cases recorded by the authorities

The figure shown here is 58,800 crimes using information technology recorded by the Interior Ministry Cybercrime Center in calendar 2024, with 603 billion soums taken from citizens in those cases. The count runs across 62 categories and is wider than fraud against people: 98 percent were theft and fraud involving bank cards. It is the centre's statement at a press tour on 31 May 2025. The centre had recorded 863 such crimes, in 18 categories, in 2019. The count was 4,865 in 2021, 62,440 by the end of 2025, and 69,962 in the first nine months of 2026, when the loss to citizens was approaching 1 trillion soums.

What officers solve is a thinner slice of that book. By the ministry's meeting in October 2026 they had uncovered 17,483 cybercrimes so far in the year, 5,600 of them on their own initiative, after more than 9,000 in the first half, when 120.49 billion soums had been returned to more than 13,000 people. Over the first nine months the same work stopped more than 38,000 harmful programs aimed at emptying accounts, blocked 3,192 dangerous sites and 1,446 links set up to draw people into a scam, and blocked 43,001 cards linked to crime. The statistics office's series of registered fraud, 44,127 cases in 2025, is the police register of fraud of every kind and is kept separately from this cybercrime count. The April 2025 resolution also makes it an offence to hand over a card, a SIM card or a wallet in one's own name so that it can be used in one of these crimes.



MOST COMMON

1. Online shopping
2. Jobs
3. Card fraud

On the 2024 count the centre gave five shares that add to 100. Sending malicious links and software, to take control of a bank card or a phone, was 60 percent. Getting a text-message code by deception, then using it to open a card account or a banking app, was 16 percent. Fraud on online trading platforms was 11 percent. Other scams whose aim was to take money were 9 percent. Online loans taken out in a citizen's name were 4 percent. Alongside that split, 98 percent of the crimes were theft or fraud involving a bank card.

The 2026 complaint book shows the same methods in cases and in soums. On Cardblock from 1 January to 1 October, 18,830 reports were harmful software installed on a phone, worth 79.3 billion soums, and the cybercrime department said about half of current crimes work through those files. Debits where the person did not name the type were 11,475 reports and 98.1 billion soums, the largest sum. Paying in advance for goods or a service that never arrived was 3,571 reports and 10.5 billion soums. Taking over a Telegram account was 2,808 reports and 21.9 billion soums. Fake trading offers were 1,044 reports and 15.1 billion soums. Payments into schemes that promised to multiply the money were 1,086 reports and 14.0 billion soums. Instructions given on a phone call were 611 reports but took 27.7 billion soums. Loans opened in someone else's name, after a story about cancelling a loan, were 130 reports and 10.6 billion soums.

Scam type	People scammed	Money lost
Online shopping Borrowed from India, Indonesia, Japan and 6 more	946,830	US$6.5m
Jobs Borrowed from Australia, Canada, Colombia and 18 more	697,129	US$4.8m
Card fraud Borrowed from Australia, Canada, India and 11 more	615,124	US$4.2m
Investment Borrowed from Australia, Canada, India and 10 more	615,196	US$27.7m
Prizes Borrowed from Australia, Canada, India and 10 more	588,703	US$4.1m
Government impersonation Borrowed from Australia, Canada, India and 10 more	574,740	US$4m
Charity Borrowed from Australia, Canada, Colombia and 18 more	354,622	US$2.4m
Romance Borrowed from Australia, Canada, India and 11 more	293,664	US$2m
Threats and extortion Borrowed from Australia, Canada, India and 11 more	22,575	US$155,908
Tech support Borrowed from Australia, Canada, India and 11 more	14,886	US$102,807
Loans Borrowed from Australia, Canada, India and 11 more	10,132	US$1.3m

Scam type	People scammed	Money lost
Business impersonation Borrowed from Australia, Canada, India and 11 more	9,682	US$66,869
Friend or family impersonation Borrowed from Australia, Canada, India and 10 more	6,790	US$46,893
Other Borrowed from Australia, Canada, India and 11 more	384,912	US$6.2m
Stolen logins and devices Borrowed from Australia, Canada, India and 11 more	1,396,903	US$27.6m

GOVERNMENT RESPONSE

Since 6 May 2025 the Interior Ministry has coordinated the police, the prosecutors, the security service, the central bank and the banks. Banks and payment firms feed transactions into one central bank platform. A police request can freeze a suspect card, and a firm that misses its cybersecurity duties can be made to cover the loss. Each month the ministry names the banks and payment firms with the most of these crimes. Apps warn a customer before a transfer and carry a fraud report inside the account. A register lets a person ban a new credit agreement in their name. By October 2026, 3 million people had joined the ministry's Qo'riqchi checker, which looks for harmful app files.

The caseload has kept climbing: 4,865 crimes in 2021, 58,800 in 2024, 62,440 in 2025, and 69,962 in the first nine months of 2026, with losses approaching 1 trillion soums. Investigators returned more than 210 billion soums of that nine-month loss, and 113.1 billion of the 278.3 billion soums reported on Cardblock was blocked. On 27 January 2026 the president told the ministry and the prosecutors that the cybercrime department, set up three years earlier, had not shown a visible result, and asked when bank and payment-firm protections would be finished. Nine tenths of the crimes are run from abroad. A round-the-clock centre of the ministry and the banks, to follow the money when a report arrives, is still a legal draft the 10 November decree orders by December 2026.

Calculation Methodology & Sources

People scammed

- 10.7%. Where reliable survey data is not available, we estimate using mobile and broadband penetration.
- 10.7% of 23,634,943 adults.

People who lost money

- 57.4%. Where reliable survey data is not available, we estimate using mobile and broadband penetration.

Money lost

- UZS 603b was lost in cases recorded by the authorities. Adding the 1,387,414 victims who lost money but are not in those records, at UZS 392,418 each, gives UZS 1.15tn.
- Price of an unrecorded loss: Read off the line fitted to GDP per person in the countries where this price is measured (Canada, Chile, Mexico, Singapore and United States): US$31.20 = UZS 392,418.43.
- US dollars at 0.000079495 per UZS.
- Share of GDP: US$91.2m against GDP of US$147.04b in 2025. World Bank, GDP (current US$) 2025.

Money returned

- Estimated: the median share of money recovered in lower-middle-income countries that publish it: Bangladesh (1.1%), Egypt (7.6%), India (4.3%), Nigeria (0.3%), the Philippines (6.6%), Pakistan (6.2%), Tanzania (0.5%) and Vietnam (2.0%).

Reported

- Borrowed from Indonesia, India, Malaysia, the Philippines, Singapore, Thailand and Vietnam: 75.0%. The median of the shares measured by the non-government survey: Indonesia (48.0%), India (87.9%), Malaysia (55.2%), the Philippines (76.9%), Singapore (87.1%), Thailand (75.0%) and Vietnam (65.2%).

Police records

- Borrowed from Indonesia, India, Malaysia, the Philippines, Singapore, Thailand and Vietnam: 41.4%. The median of the shares measured by the non-government survey: Indonesia (28.0%), India (53.4%), Malaysia (41.4%), the Philippines (13.5%), Singapore (54.8%), Thailand (45.8%) and Vietnam (39.4%).
- 58,800: Cybercrime cases recorded by the Interior Ministry Cybercrime Center.

Most common

- Borrowed from Indonesia, India, Japan, South Korea, Malaysia, the Philippines, Singapore, Thailand and Vietnam: ranked by the average of the scam types their victims named (no survey of Uzbekistan's own). 34.8% of answers are methods such as phishing, or other, and are not ranked.
- Split by type using 2024 figures: How the Cybercrime Center said cybercrimes were most commonly committed, as shares that add to 100, stated with the 2024 count.
- Borrowed from Australia, Canada, Colombia, France, Greece, India, Indonesia, Italy, Japan, Malaysia, Mexico, the Netherlands, the Philippines, Singapore, South Africa, South Korea, Thailand, Ukraine, the United Kingdom, the United States and Vietnam: Online shopping, Jobs, Card fraud, Investment, Prizes, Government impersonation, Charity, Romance, Threats and extortion, Tech support, Loans, Business impersonation, Friend or family impersonation, Other and Stolen logins and devices.
- Victims can be hit by more than one type, so the people by type add up to more than the people scammed.
- Money by type adds up to the money lost.
- In UZS: Online shopping UZS 82.26b, Jobs UZS 60.57b, Card fraud UZS 53.44b, Investment UZS 347.98b, Prizes UZS 51.15b, Government impersonation UZS 49.93b, Charity UZS 30.81b, Romance UZS 25.51b, Threats and extortion UZS 1.96b, Tech support UZS 1.29b, Loans UZS 15.89b, Business impersonation UZS 841.2m, Friend or family impersonation UZS 589.9m, Other UZS 77.86b, Stolen logins and devices UZS 347.37b.

Sources

- Armidale, ASEAN Consumer Scam Report 2026 for the GSMA (figures computed from the respondent data) (4 September 2026). Survey. Online survey of adults aged 18 and over in each country (Milieu Insight panel). Original https://www.gsma.com/about-us/regions/asia-pacific/gsma_resources/asean-consumer-scam-report-2026/
- Central Bank of the Republic of Uzbekistan, Rapid analysis of fraud reports received through the Cardblock system (13 November 2026). Official source. Press release of 13 November 2026. Cardblock reports from 1 January to 1 October 2026. Stated fraud loss 278.3 billion soums, of which 113.1 billion soums was blocked. Nine rows of fraud types are listed, plus 2,737 reports worth 7.6 billion soums that were automatic loan repayments and are set outside the fraud total. Original https://cbu.uz/en/press_center/releases/4911207/ ·
- Central Bank of the Republic of Uzbekistan, Central bank note on presidential resolution PQ-153 of 30 April 2025 (6 May 2025). Official source. Note of 6 May 2025 on resolution PQ-153. Lists duties on banks and payment firms, including antivirus warnings in apps, a dropper register, and recovery of citizens' losses from firms that did not provide enough cybersecurity. Original https://cbu.uz/uz/press_center/releases/2408879/ ·
- Gazeta.uz, Cybercrimes in Uzbekistan increase 68-fold in five years (31 May 2025). News report. Press tour of the Interior Ministry Cybercrime Center on 31 May 2025. Bekzod Mamajanov, head of the centre, stated 58,800 crimes using information technology in 2024, across 62 categories, and damages to citizens in 2024 of 603 billion soums. The same statement gives the method shares 60, 16, 4, 11 and 9 percent. It is the centre's statement to the press, not the ministry's statistical yearbook. The count understates scams that were never recorded. Original https://www.gazeta.uz/en/2025/05/31/cybercrime/ ·
- Gazeta.uz, Cybercrime damage to citizens in the first 11 months of 2025 (24 December 2025). News report. The English URL for 23 December 2025 returned 404. This Uzbek page, dated 24 December 2025, reports the 23 December press conference of Ramazon Ashrapov, deputy minister and head of the Investigation Department. Cybercrimes rose from 4,865 to 62,440 across 2021 to 2025. Citizen damage over that span was 3 trillion 730 billion soums, of which 1 trillion 890 billion soums fell in the first 11 months of 2025. Not a full-year pair. Original https://www.gazeta.uz/oz/2025/12/24/cybercrime/ ·
- Gazeta.uz, Cybercrime briefing of 9 October 2026 (10 October 2026). News report. Press conference of 9 October 2026. Ashrapov: 69,962 crimes using information technology in nine months, loss approaching 1 trillion soums, Qo'riqchi at 3 million people. Sagdullayev: more than 210 billion soums returned, about 18,000 crimes solved, harmful app files in about half of crimes, 90 percent of crimes cross-border. Ministry contacts with Google, Meta and Telegram. Original https://www.gazeta.uz/oz/2026/10/10/kiberjinoyat/
- Gazeta.uz, Presidential meeting on cybercrime, 27 January 2026 (27 January 2026). News report. President Shavkat Mirziyoyev said the cybercrime department, set up three years earlier, had not yet shown a visible result, and asked when bank and payment-firm protections would be finished. The article's Tashkent city figures are left out of the descriptions. Original https://www.gazeta.uz/uz/2026/01/27/cyber-crimes/

- Interior Ministry of the Republic of Uzbekistan, Fighting cybercrime: results, criticism and firm tasks (13 October 2026). Official source. Ministry page dated 13 October 2026. In the year to the meeting: 17,483 cybercrimes uncovered, 5,600 of them on officers' initiative, and more than 209 billion 934 million soums returned to more than 19,000 citizens. Nine months: 77 billion 344 million soums stopped from leaving the country and 43,001 crime-linked cards blocked. More than 38,000 phishing programs stopped. 3,192 dangerous resources and 1,446 fraud links blocked. 2026 is the Year of Combating Cybercrime inside the ministry. Original https://gov.uz/oz/iiv/news/view/231666 ·
- National database of legislation of the Republic of Uzbekistan, Regulation 3759 on minimum information security and fraud prevention requirements for remote financial services (21 January 2026). Official source. Ministry of Justice registration 3759 of 21 January 2026, in force 22 April 2026. Amendment registered 14 August 2026, in force 16 November 2026, covers the online-loan refund in paragraphs 30 and 31. Paragraph 17 requires a warning before a mobile transfer is confirmed. Paragraph 18 requires a check of the credit-agreement ban before an online loan. Paragraph 27 requires a fraud-report section in the mobile app. Original https://lex.uz/uz/docs/8007760 ·
- National database of legislation of the Republic of Uzbekistan, Law of 4 March 2025 amending the law on exchange of credit information (4 March 2025). Official source. Adds a voluntary ban on a credit agreement in a person's own name. The credit bureau enters the ban at once. Original https://lex.uz/docs/-7417538 ·
- National database of legislation of the Republic of Uzbekistan, Presidential decree PF-242 of 10 November 2026 on measures to carry out national programmes to raise human dignity (10 November 2026). Official source. In force 11 November 2026. The saved page is the decree's record (number, title and dates) and does not include the annex. The round-the-clock centre is taken from the news report that quotes the decree. Original https://lex.uz/docs/-8582037 ·
- National database of legislation of the Republic of Uzbekistan, Presidential decree PF-38 of 10 March 2026 on the cybersecurity strategy and preventing cybercrime (10 March 2026). Official source. In force 11 March 2026. Sets the cybersecurity strategy for 2026 to 2030. Tasks include preventing fraud, a working link between the police and the public, and simpler reporting through an online service and convenient platforms. Original https://lex.uz/docs/-8079286 ·
- National database of legislation of the Republic of Uzbekistan, Presidential resolution PQ-153 of 30 April 2025 on strengthening the fight against crimes committed using information technology (30 April 2025). Official source. In force 6 May 2025. The Interior Ministry coordinates the work. Each month it names the banks and payment firms with the most cybercrimes. A police request blocks a suspect card. Paragraph 5 sets liability for handing over a card, account, SIM or e-wallet for use in a cybercrime, and provides for recovering a loss from a firm that missed cybersecurity requirements. Original https://lex.uz/docs/-7511145 ·
- Scamstats, Derived average: median share of money returned, lower-middle-income countries. Derived figure. The median share of money lost that was returned, in the lower-middle-income countries that publish it. Definition https://scamstats.org/methods/#derived-money-returned-lower-middle-income
- Scamstats, Derived average: median share who reported to any institution, non-government survey countries. Derived figure. The median share of victims who reported to any institution, in the countries with the non-government survey. Definition https://scamstats.org/methods/#derived-reported-any
- Scamstats, Derived average: median share who told the police, non-government survey countries. Derived figure. The median share of victims who told the police, in the countries with the non-government survey. Definition https://scamstats.org/methods/#derived-told-police
- National Statistics Committee of the Republic of Uzbekistan, Number of registered frauds (total), SDMX indicator 901 (22 April 2026). Official source. Indicator 2.04.09.0041, table 901, Republic of Uzbekistan row. 2024 is 29,252 and 2025 is 44,127. Primary source is the Ministry of Internal Affairs. Last modified 2026-04-22. First publication 2022-07-05. The table has no loss column. The SIAT page is https://siat.stat.uz/data/901/. Original http://api.siat.stat.uz/sdmx/901/table/download/?download_format=pdf ·
- UN DESA, World Population Prospects 2024 (medium variant) (11 July 2024). Official source. Modelled estimates built from censuses and surveys. Original https://population.un.org/wpp/ ·
- UZCERT, the state cybersecurity centre, Questions and answers (1 April 2025). Official source. UZCERT receives reports of fake pages and harmful links. Card theft is directed to the Interior Ministry's cybersecurity units. Page first published 1 April 2025 and modified 9 November 2026. Original https://uzcert.uz/savol-va-javoblar/ ·
- World Bank, Mobile cellular and fixed broadband subscriptions per 100 people (28 October 2026). Official source. ITU figures via the World Bank; the latest year for each country. Original https://data.worldbank.org/indicator/IT.CEL.SETS.P2 ·
- World Bank, Official exchange rate (local currency units per US$, period average) 2025 (8 October 2026). Official source. Annual average of official exchange rates reported by national authorities. Original https://data.worldbank.org/indicator/PA.NUS.FCRF ·
- World Bank, GDP (current US$) 2025 (8 October 2026). Official source. National accounts estimates that are revised as countries report. Original https://data.worldbank.org/indicator/NY.GDP.MKTP.CD ·

- Zamon.uz, A round-the-clock centre is to be set up when a fraud report arrives (16 November 2026). News report. Report of 16 November 2026 quoting decree PF-242. By December 2026 a draft legal act is to create a round-the-clock centre of the Interior Ministry and the banks that follows the money when a report of online fraud or theft arrives. The centre is ordered as a draft. Original https://zamon.uz/uz/2026/11/16/firibgarlik-haqida-xabar-tushishi-bilan-chora-koriladi-ozbekistonda-247-markaz-tashkil-etiladi

---