

Russia

Population 144 million · Latest figures: 2025

The Ministry of Internal Affairs, which includes the police, recorded 663,000 cybercrimes in Russia in 2025, down 12% from 775,000 in 2024. The Ministry says each new measure brought a sharp fall, followed by a partial rise, because criminals adapt. Its three main groups all fell: fraud by 9%, thefts by 23.8% and unlawful access to computer information by 44%.

The Ministry of Internal Affairs leads the policing, and the Bank of Russia, the central bank, sets the anti-fraud rules that banks must follow. The main recent law is Federal Law 41-FZ of 1 April 2025, which set up a state information system against crimes committed with information and communication technologies.

From 1 September 2025 banks must run anti-fraud checks before they issue consumer loans or cash from ATMs. A mandatory cooling-off period also applies to consumer loans: money of 50,000 to 200,000 roubles is available only 4 hours after signing, and larger sums after 48 hours. From 1 October 2025 the mobile apps of the large banks must offer victims a service for reporting an unauthorised operation. The deputy minister, Andrei Khrapov, credited the anti-fraud legislation that took effect in April 2025 with cutting the weekly count of cybercrimes from more than 9,000 in January 2025 to fewer than 6,000 in December.



PEOPLE SCAMMED

7,393,938

6.5% of adults

Scammers reach people by phone and through fake websites, and they usually start by persuading the person to act. The Bank of Russia describes one common route in 2025. A caller claims to be from a delivery service, a flower shop, a cafe or a restaurant, and says there is an order or a gift that needs a code from a text message to confirm it. Once the code is given, the call is ended by a recorded voice that says it was a scam. A text message then follows, claiming that a loan has been taken out in the victim's name or that the victim's account on Gosuslugi, the state services portal, has been hacked, and giving a number to ring. The person who rings is then persuaded, under the pretence of saving their money, to move their savings to the scammers' accounts or to hand the cash over.

Other people are sent a phishing link or malicious software, and the criminals gain remote access to their online banking. In some schemes card details are passed on through special software, in a method the Bank of Russia calls NFC Gate. The largest thefts from individuals combine these tricks with social engineering, which means persuading people to act against their own interests, and with fake versions of the websites of companies, federal bodies and state services.

PEOPLE WHO LOST
MONEY

4,368,715

59% of victims

Victims lost money from bank accounts, payment cards and electronic wallets. The Bank of Russia counts operations made without the customer's consent, which it describes as unauthorised operations. In 2025 their value rose 6.4% and their number rose 31.2%, so the average amount per operation fell. For individuals the average was 18,000 roubles, down from 22,400 roubles in 2024. For businesses the average was 373,200 roubles, down from 467,700 roubles.

Losses from accounts were the largest, at 10,628.41 million roubles for individuals, while card operations were the most frequent, at 980,460 in 2025. The Bank of Russia says the fall in the average followed its systematic work to improve the anti-fraud systems of banks. From 1 September 2025 banks must run anti-fraud checks on consumer loans and on cash taken from ATMs, which the Bank of Russia says reduces the total of the largest thefts.

The Bank of Russia reports operations by channel: card, account, the Faster Payments System (SBP), electronic wallet and operations without opening an account. It says criminals combined these channels, which increased operations for individuals. Unauthorised operations made up 0.00071% of the value of all transfers in 2025, up from 0.00066% in 2024.

MONEY LOST

US\$2.7b

RUB 225.65b in a
year, 0.11% of GDP

Banks returned 5.9% of the money taken in unauthorised transfers in 2025, which was 1,731.3 million roubles, against 9.9% (2,713.58 million roubles) in 2024. The share fell even as the value of those operations rose 6.4%. The largest part of the money returned in 2025, 700.41 million roubles, came from account operations.

Under Article 8, part 3.13 of Federal Law 161-FZ on the national payment system, a bank that fails to run proper anti-fraud checks on a transfer to details in the Bank of Russia's database of fraudulent operations is financially liable to its individual customer. That route returned 3.16 million roubles in 2025, against 1.23 million roubles in 2024. The Bank of Russia says the small sum reflects banks meeting the required anti-fraud rules. A borrower who was tricked into taking a loan is released from repaying it, and from the interest, until a court verdict takes effect, if the lender broke the anti-fraud rules and a criminal case has been opened over the theft of the loan money.

Banks have reported to the Bank of Russia since 2023 the value of the thefts they prevented. In 2025 that was 13,895.4 billion roubles, and 134.16 million fraudulent operations did not go through, against 72.17 million in 2024.

REPORTED

75%

of victims reported it

Victims report to the police and to their bank. The Ministry of Internal Affairs, which includes the police, counted 534,500 victims of cybercrime in 2025, down 5.5%. From 1 October 2025 the mobile apps of the large banks must include a service for victims. It lets a customer register an unauthorised operation in the app and receive an electronic certificate of it for the police. The Bank of Russia says this service has proved popular with victims who lost small sums and who had not previously gone to their bank or the police, and that it changed the recorded count of operations.

Banks also send the Bank of Russia details of fraudulent operations, which feed the database that banks use in their anti-fraud checks. Criminal phone numbers are passed on to telephone operators. In 2025 the Bank of Russia sent operators 69,091 numbers that criminals had used to steal money from people. It also sent registrars details of 1,002 internet addresses in the .ru, .pф and .su zones so they could be taken down, and registrars took on average from three hours to several days to remove them.

The Bank of Russia says the number of phishing sites has fallen for the last two years, although such attacks remain relevant. Since 2023 banks have also sent it the value of the thefts they prevented, so that figure comes from banks rather than the police.

POLICE RECORDS

663,000

cases recorded by the authorities

The figure shown on this page is the 663,000 cybercrimes that the Ministry of Internal Affairs recorded in Russia in 2025, the latest full year. The total is wider than scams, because it also includes thefts and unlawful access to computer information. Of the 663,000, the Ministry gives 344,000 fraud cases, down from 378,000 in 2024, 80,000 thefts, down from 105,000, and 58,000 cases of unlawful access to computer information, down from 104,000. The Ministry put the material damage it registered at 189.5 billion roubles in 2025, down from 205 billion roubles in 2024.

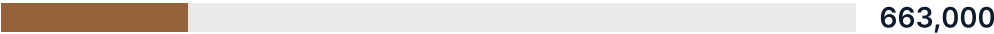
In January 2025 it recorded more than 9,000 cybercrimes a week, and by December fewer than 6,000 a week. The deputy minister said each new measure was followed by a sharp fall and then a partial rise, because criminals adapt. The Ministry also counted 534,500 victims, down 5.5%. That is a count of victims, not of cases. The total of 663,000 is down 12% from 775,000 in 2024.

The figures were given by the deputy minister of internal affairs, Andrei Khrapov, at the Cybersecurity in Finance forum, and were reported by Interfax on 18 February 2026. Asked by the governor of the Bank of Russia, Elvira Nabiullina, whether the Ministry felt cautious optimism about the fight against cyber fraud, he said that he supported it.

Victims who told the police (estimated)



Cases recorded by the authorities



MOST COMMON

1. Online shopping
2. Card fraud

The largest group the Ministry names is fraud, with 344,000 cases of the 663,000 cybercrimes in 2025. Thefts came to 80,000 cases and unlawful access to computer information to 58,000.

The Bank of Russia says the biggest thefts from individuals come from schemes that combine social engineering with phishing, where a person is persuaded to act by a call or a message and is sent to a copy of an official website of a company, a federal body or a state service. Card operations were the most frequent kind of unauthorised operation for individuals in 2025, at 980,460, while account operations had the largest value, at 10,628.41 million roubles. In 2025 criminals often persuaded people not only to make a payment but to follow a phishing link or install malicious software, which gave them remote access to online banking. Schemes that draw in people's money under the pretence of investing, often mentioning cryptocurrency, are becoming more widespread.

Of the internet resources the Bank of Russia acted on in 2025, 43% were phishing sites copying the names of well-known banks and investment companies, about 36% were businesses offering unlicensed securities trading or non-existent lenders, and 21% were financial pyramids, often disguised as online games. For businesses, the average unauthorised operation was 373,200 roubles in 2025, against 467,700 roubles in 2024.

GOVERNMENT RESPONSE

The Bank of Russia works with banks, telephone operators and the Ministry of Digital Development, and it sets the rules that banks must follow. In a pilot in 2025 it worked with operators and banks to use criminal phone numbers in banks' anti-fraud checks, which let banks suspend suspicious operations worth more than 100 million roubles and mark the accounts that fraudsters might use to move stolen money. The rules now in force include mandatory anti-fraud checks before consumer loans and ATM cash, a cooling-off period for loans, and a rule that a bank must refuse to issue a card or online banking access to a person whose details are in the Bank of Russia's database. Such a person can take no more than 100,000 roubles a month from an ATM, and more only at a bank branch with identity papers. Federal Law 41-FZ of 1 April 2025 set up a state information system against these crimes.

The results so far are uneven. The police count fell 12%, and the deputy minister said each measure brought a sharp fall followed by a partial rise. Over the same year the number of unauthorised operations rose 31.2%, and the share of money returned to customers fell from 9.9% to 5.9%. The deputy minister said criminals move to areas that are not yet well regulated, such as SIM boxes, whose main SIM cards are machine-to-machine (M2M) cards, and whose sale and circulation he said are insufficiently regulated.

Calculation Methodology & Sources

People scammed

- 6.5%. Where reliable survey data is not available, we estimate using mobile and broadband penetration.
- 6.5% of 114,400,570 adults.

People who lost money

- 59.1%. Where reliable survey data is not available, we estimate using mobile and broadband penetration.

Money lost

- RUB 189.5b was lost in cases recorded by the authorities. Adding the 3,705,715 victims who lost money but are not in those records, at RUB 9,754 each, gives RUB 225.65b.
- 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\$116.60 = RUB 9,753.92.
- US dollars at 0.011954215 per RUB.
- Share of GDP: US\$2.7b against GDP of US\$2.56tn in 2025. World Bank, GDP (current US\$) 2025.

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%).
- 663,000: Cybercrime cases recorded by the Ministry of Internal Affairs.

Most common

- Borrowed from the United Kingdom, the Netherlands and Greece: ranked by the average of the scam types their victims named (no survey of Russia's own). 8.6% of answers are methods such as phishing, or other, and are not ranked.

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/
- Bank of Russia, Cooling-off period for consumer loans and credits: questions and answers (27 August 2025). Official source. Bank of Russia FAQ on the cooling-off period, card refusal, ATM limits and loan release, from 1 September 2025. Original https://cbr.ru/faq/information_security/cooling-off_period/
- Bank of Russia, Review of operations without voluntary consent of clients of financial organisations, 2025 (13 February 2026). Official source. Bank of Russia review of unauthorised transfers in 2025: values, counts, returns, prevented operations, victim service, phone numbers and domains. Original https://www.cbr.ru/analytics/ib/operations_survey/2025/
- Interfax, reporting the Ministry of Internal Affairs, The Ministry of Internal Affairs reports a fall in cybercrime in Russia in 2025 by 12 percent (18 February 2026). News report. Report of the deputy minister's statement at the Cybersecurity in Finance forum: 663,000 cybercrimes in 2025, down from 775,000, and RUB 189.5 billion of material damage registered by the Ministry of Internal Affairs. The Ministry's own publication was not opened (see open questions). The live page was saved on 22 October 2026. Original <https://www.interfax.ru/1073418>

- Office for National Statistics, Crime in England and Wales: appendix tables, year ending March 2026 (23 July 2026). Survey. The national crime victimisation survey for England and Wales; fraud questions cover the 12 months before interview. Original <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables> ·
- Official publication portal of legal acts of Russia, Federal Law No. 41-FZ of 1 April 2025 on creating a state information system to counter crimes committed with information and communication technologies (1 April 2025). Official source. Title, number and dates from the official portal. The page did not show the article text. Original <https://publication.pravo.gov.ru/document/0001202504010010> ·
- 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/> ·
- 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> ·