

06.03.2025

Grigory Osipov: “Russia Is Under Fraudster Attack. What Can Be Done?”

Use of artificial intelligence and Western software vulnerabilities, infrastructure attacks and identity theft are the key cyberthreats of 2025.

As reported by the Central Bank of Russia, last year fraudsters stole from private persons the largest amount on record — ₽27,5 billion, which is 74,4% more than in 2023. According to Kaspersky Lab, fraudsters managed to call up to 60% of private persons.

The situation is dire, because last year this figure was at 43%. The State Duma passes new laws, aiming to protect consumers from fraudsters, and banks are proactively “cooling down” suspicious transactions without any official guidance, but there is no change of the situation for the better. BM Moscow Foresight interviewed Grigory Osipov, Investigations Director of SHARD digital asset security platform, on which methods are used by cyber criminals to get to wallets of Russians, and why it would be impossible to defeat fraudsters without resolution of geopolitical issues.

The Ministry of Internal Affairs reported that just over the first seven months of 2024 there were 577 thousand crimes in the

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

information and telecommunications sphere, over a half of which are theft and fraud, primarily involving use of cryptocurrencies.

Last year a few popular cryptocoins went up in price. In relation to this, the number of crimes, especially investment scams, shot up pretty much pro rata. People are more prone to “swallow the bait” by fraudsters when they miss an opportunity to make money, which criminals are happy to exploit. Practical methods for efficient investigation of such crimes are under development, and far from all MIA officers have the necessary tools and skills.

It should also be recognized, that a person, who fell victim to cryprtocurrency scammers, is often clueless where to go for help, because the market is teeming with swindlers, fake lawyers, pseudo-helpers of all sorts.

How could one differentiate investment fraud from other types of crime?

Investment fraud should be described as a type of fraud, when criminals under various pretexts — helping to withdraw money, getting an education —draw a potential victim into a pseudo-investment project, promising profits, related to “FX trade transactions”, “trading securities and cryptocurrencies”, “investment into a new promising coin”. Participation in such projects always ends in loss of the victim’s money.

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.



© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

Have you met any victims of such crime?

Of course. Last year we were addressed by a man, who initially just searched the Internet for cryptocurrency training courses, but ultimately was convinced by criminals to invest funds in a lucrative pseudo-cryptocurrency project. Swindlers managed to cloud his judgement. They displayed to him a crypto wallet with a lot of coins, including fake ones, which were growing in price.

At first the victim was jubilant that his “investment amount” had doubled. The criminals then withdrew his money and decided to take their scam even further. They notified him that his accounts were blocked for withdrawal of funds for “illegal activities”. When the victim told them that he did not have any money anymore, they proposed to send a specific amount to his bank card. He was supposed to buy cryptocurrency with these funds in an exchange service and send it to the fraudsters for unblocking.

In this case the victim went along with the fraudsters and became an accomplice in the fraud, when he received money from other scammed people to his bank card.

What other schemes were used in 2024 to scam people?

Ponzi schemes are justifiably considered as a type of investment fraud scheme. These are going through a renaissance now. According to the Bank of Russia, in 2024 there were 4772 organizations, officially designated under this category. Just to give you some idea, in 2023 there were 2226, and in 2022 — 1961 of these.

Here is a general description of a Ponzi scheme — it is an organization, which pays money to its investors for the account of other participants, who invested in the scheme later on. Speaking in the language of finance, this organization uses a Ponzi scheme (named after Charles Ponzi, an American swindler, who was the first to implement this scheme in 1920s — *ed.note*).

Are there any graphic examples of modern Ponzi schemes?

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

Last year the authorities stopped activities of Sincere Systems Group LTD. Experts estimated the damages from its operation at $100 million.

It should be noted, that as per our own data and per the CBR, in 2024 more than 70% of financial Ponzi schemes raised funds in cryptocurrencies. This is related to cryptocurrency specifics — pseudo-anonymity, complicated tracking of transactions and underdeveloped regulation of the market. Moreover, almost all projects lure people into their networks online, through popular messengers and social media.

How much money do they cheat out of Russians?

Large schemes, such as Finiko, S-Group or Amir Capital, defrauded their victims of hundreds of millions of dollars, and in 2024 new projects of the kind often failed to collect such large amounts: their “average check” is much lower. But the number of smaller projects and the total damages have also increased.

Moreover, such Ponzi schemes use increasingly complex and high-tech methods, including development of proprietary cryptocurrencies and tokens, aggressive advertisement and referral systems, meaning some partner channels, which look as legit private businesses, which helps them quickly attract audience.

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.



© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

How long could such a scheme exist?

Lately new projects operate just for 2-4 months. They draw in their audience fast and collect a required amount, and then quit. But sometimes they stretch this process out, which reduces the numbers of victims going to the police. Here I would like to stress the fact that all participants in such projects go through brainwashing phases. They are taught to anticipate their profits all the time. Sometimes a person would go on for several months, being sure that his funds will be returned or that something would change, and would not go to the police.

Cryptocurrency scheme organizers often use shadow international channels and anonymous cryptocurrency networks, making the task of apprehending them significantly harder for IAM officers.

Usually, when they mention fraudsters, they primarily refer to calls from “Sberbank security service”, “Investigative Committee”, “Multi-Functional Center”, “FSB” etc. Is this social engineering in action?

The fraud type with the so-called “safe account” is still the most wide-sweeping method both in the number of recipients of such calls and in the amount of losses. These are the crimes, when swindlers over the phone convince gullible Russians to transfer their money into a “safe” or “special” account, to allegedly save their funds from theft. Fraudsters use a classic social engineering ruse, but with new elements. First criminals contact their potential victim, usually by phone or through messages, and say that there was an unauthorized attempt to steal funds from his or her account and a special operation to apprehend fraudsters is underway.

To “save” funds, swindlers propose to transfer money to the so-called “safe account”, allegedly held with “Central Bank”, “Rosfinmonitoring” or any other agency.

Criminals assure that this is a “temporary measure”, while the police is chasing criminals, and the money will be returned when the perpetrators are arrested. At the same time this “safe account” means bank cards of third persons, to which a victim transfers his funds, and fraudsters most often immediately send funds from these cards to purchase cryptocurrency and transfer the stolen money out of the country.

For greater effect, they demand from the victim not to disclose the infromation on what’s happening, prohibit to discuss this

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

subject with anybody else and threaten with criminal liability for this. This type of fraud could involve multiple roles: first a potential victim is contacted by a police officer, and then by an alleged Rosfinmonitoring or Bank of Russia official.

Were there any unconventional moves, used by fraudsters in their communication with victims last year?

Of course there were. One of the ingenious schemes presented romance fraud. This is a version of an investment fraud, when a victim, usually a well-to-do woman, is deceived by a criminal through involvement into an emotional relationship. The fraudster creates an illusion of “true love”, gradually winning trust of the victim. As soon as this “connection” is established, the criminal starts using this trust, proposing to transfer cryptocurrency under various false pretenses. For example, there could be made-up stories of urgent family issues or “profitable” investments could be proposed, which do not exist in reality.

Have you received any calls from such victims?

For example, last year a married homemaker woman with a child came to us for help. She met a man over social media, who in a few weeks of communication offered her to invest into a crypto project. But to incentivize spending more money, the fraudster purposefully romantisized their relations, took them to the level of lover talk, making joint plans, which could only come true after investments into the proposed project. To achieve his goal, the swindler used pressure, psychological manipulation with financial dependence from husband, well-being of her child. At the same time the criminal assured her that he had transferred to the project a bigger portion of funds. The woman, who communicated with the fraudster at a recommendation from her new lover, over three months transferred her husband’s funds into a service wallet and allegedly made money under control of the swindler. To raise the level of trust, the criminal even let her withdraw a small amount once, but after this the trap was shut and the victim lost a lot of money and then her family.

Are there many such sad stories in Russia?

There is no accurate statistical data, but I can share my observations: though romance frauds were becoming more popular

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

among scammers last year, but their share remains insignificant as compared to other types of fraud.

Are there any large scale projects?

There is a graphic example — “tapping” game fraud. These are simple smartphone “games”, based on constant screen tapping to perform actions, collect points or in-game currencies. Such games often feature a cyclic element, when the key objective of a player is to maintain continuous interaction with the screen, for example, by tapping buttons or objects on the screen. These games are very popular with children and young people due to their simplicity.

The trouble is that with increasing mobile game popularity, swindlers have started using this genre for various criminal schemes, especially those targeting inexperienced users. Fraudsters promise that cryptocurrency, collected in a game, could be exchanged by players for real money. But in the real world this cryptocyrrency has no real value and cannot be used at real trading platforms. And criminals also create fake sites and apps, which look like popular cryptocurrency games, such as Hamster Kombat, the notorious Hamster, which needs to be “tapped”. These sites promise profits for simple screen tapping, but are actually used for stealing cryptowallet data.

The authorities are constantly passing laws, aimed at security from fraud. Many banks have already voluntarily introduced “cooldown” periods to protect their customers. The press regularly covers the fraud issue, but the volume of these crimes continues rising. Why does this happen?

The key issue here is that fraud has become a whole separate field of the information war against Russia. After the start of the SMO in February 2022 the number of hacks of Russian corporate IT systems shot up: personal data and bank details of tens of millions of Russians were leaked, and this data is still actively used by fraud groups.

How have the activities of criminals changed over the latest year?

Fraud schemes in the banking sector have become more complex, sophisticated, manipulations and information pressure are actively used, and crime mechanisms are more tech-savvy. All of these highlight a strategic criminal approach: essentially this

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

is a systemic business, originating mostly from Ukraine and operating with support of law enforcement agencies, including SBU.

Are criminals from other countries involved in this?

Over time the situation has deteriorated. If back at the start of the special operation almost all crimes in this category were perpetrated from Ukraine, then now the very same call centers also operate in Russia and CIS countries. The same is true for the banking infrastructure attack vectors.

Why are there so few apprehended cybercriminals?

It turned out that complex modern technologies make identification of criminals very hard. For example, fraudsters use one-off social media accounts, photos of other people, artificial intelligence can even generate images for video calls. Fraudsters collect payments either directly through cryptocurrency, or to bank cards of third parties, which sell them. For now it is impossible to completely block payments to third party bank cards.

Fighting these crimes is complicated due to political aspects, making counteractions against such fraudsters much harder. Tracking down and blocking criminal schemes is difficult without cooperation with Ukrainian law enforcement, when funds are transferred to their territory in cryptocurrencies and to bank cards.

Naturally, the issue is made so much more complex not only due to rapid development of new forms of fraud, but also due to adaptation of criminals to changes in laws and improvement of their methods.

What could help reduce fraud volumes in Russia?

Today fighting cybercrime is a political issue, because it is a part of the active information war. As soon as there is some clarity

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

of the political issue, fraud will slide.

The second issue is fairly obvious — strange as it may seem, this is the question of trust. Most of victims of fraud, perpetrated under the guise of government agencies, still believe in integrity, incorruptibility of a “bank security service”, “Rosfinmonitoring officer” and “special services officer” etc. At the same time some people, especially elderly ones, distrust digital technologies and fail to understand their advantages. This needs to be taken into account for improvement of the information and awareness-raising policy in this area.

The third issue is underdeveloped domestic infrastructure and use of many foreign messengers, software, mobile phones, vulnerabilities of which are well known and actively exploited by fraudsters. The right decision in this case would be a transition to domestic software (SW) and similar security solutions.

In your opinion, will the volume of fraud go down as a result of all the passed anti-fraud laws by the end of 2025 or not?

The information field for now is quite open, and options to use third party bank cards and cryptocurrencies, wide use of foreign SW in the mid-term enable rising numbers of fraud by the end of 2025.

If the political situation is stabilized, if there is international cooperation and new efficient legal barriers to fraudsters in place, then with greater fraud awareness levels among people the situation will improve in the long-term.

What are the key threats in the cybercrime sphere in 2025?

I will highlight three clear threats. First, these are infrastructure attacks. This includes attempts to disrupt power industry, transportation, water supply and healthcare systems. There have already been such attacks, but the trend could rise in 2025. Critical infrastructure attacks can not only disrupt operations at vital assets, but also inflict major economic damage and create a national security threat.

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.

The second risk is a growing threat of artificial intelligence (AI) and automated attacks. AI and machine learning are becoming powerful tools both for cybercriminals and national intelligence services. In 2025 large-scale automated attacks, involving phyishing with deepfakes, generation of false data or multistage authetication bypasses are to be expected.

The third threat is global cyberwars between countries. Cyberwar is becoming an integral part of global geopolitics.

In 2025 we could expect stronger government-supported cyberattacks, aimed at meddling in internal affairs of other countries, influencing elections, destruction of national economies or social unrest. Cyberespionage, cyberterrorism and attacks at financial systems could become a part of broader confrontation strategies.

How can people protect their savings under these conditions?

Let us recall the “Knowledge is Power” slogan. If you want to protect your savings, invest them into those spheres that have transparent tracking mechanisms, follow the principles of diversification of funds, improve your digital literacy. Remember, fraudsters constantly improve their schemes. Do you take advertisements with a grain of salt? This is what you should do here as well! Often a person is the weakest link in a security system, prone to transferring his funds under the spell of fraudsters on his own, bypassing the security barriers, set by himself and “smart” software.

Anna SOLNTSEVA

© MOSCOW FORESIGHT - 2026. ALL RIGHTS RESERVED.