Federal State Autonomous Educational Institution of Higher Education

Peoples' Friendship University of Russia

Named after Patrice Lumumba

RUDN University

**Methodical Recommendations for Preparing and Conducting**

**Thematic Lesson Dedicated to:**

**Not Child’s Play: How to Avoid Becoming a Participant in Financial Crimes**

Moscow, 2024

Contents

Section 1. Easy money - hard consequences: ways to involve young people in criminal
activities[. 5](#_Toc156245260)

[1.1. Children are victims of financial fraudsters. 5](#_Toc156245261)

[1.2. Children are accomplices of financial fraudsters. 17](#_Toc156245262)

Section 2. Neural network as a modern tool for financial crimes. Fraudulent schemes using artificial intelligence..[. 21](#_Toc156245263)

Section 3. Protected means armed: how to protect yourself from financial fraud[. 23](#_Toc156245264)

Applications

[Appendix No. 1. Glossary. 26](#_Toc156245266)

[Appendix No. 2. Resources. 28](#_Toc156245267)

**Abstract**

Methodological recommendations have been prepared to help teachers of educational institutions. They are aimed at providing methodological guidance on organizing and conducting a thematic lesson dedicated to countering the involvement of young school-age people in financial crimes as victims and accomplices.

The methodological recommendations propose substantive, methodological and technological approaches to conducting a lesson, and reveal a set of issues related to conducting this event. The proposed materials are advisory in nature, so the teacher can conduct a lesson based on these developments, relying on their own experience taking into account the age characteristics, students’ level of training, as well as the traditions of the region.

**Explanatory Note**

Financial literacy among young people contributes to making smart decisions, minimizes risks and thereby can increase financial security of the population. Low financial literacy levels can lead not only to bankruptcy, but also to poor retirement planning, vulnerability to financial fraud, excessive debt, and social problems including depression and other personal problems.

According to statistics, nowadays young people (under 18 years old) are increasingly becoming victims of scammers: taking advantage of the children and teenagers’ inexperience and gullibility, criminals steal money from their cards and from their parents’ accounts. Games, prizes, and even offers for part-time jobs are used to deceive. Along with the development of online and digital services, fraud involving the theft of personal funds of individuals has become one of the main risks in many countries. Moreover, they also affect children - in Russia, the youngest victim of financial scammers is only 11 years old. Such threats are noted not only in Russia and may be relevant for the CIS and other foreign countries.

According to psychologists, victimization - the tendency to become a victim of crime - starts in childhood. The goal of the lesson is to reduce this very victimization relying on the knowledge about the types and forms of financial fraud and experience in resisting the criminal’s manipulations.

Therefore, it is important to provide an explanation to young people about such threats in real life, the Internet, social networks and instant messengers and teach them to independently identify scammers based on their distinctive features.

In this regard, the topic discussed in this lesson is highly relevant.

**The purpose of the lesson** isto motivate students to develop a personal strategy for competent behaviour in situations of growing financial risks and financial fraud.

**Lesson objectives:**

* instill the attitude of competent financial behaviour in students;
* form students’ understanding of the signs of financial fraud situations, phishing and other fraudulent sites.

**Teach students to:**

* recognize the threat of fraud and not make payments and transfers to fraudsters;
* use action algorithms in typical situations related to possible or already committed financial fraud;
* take precautions when using different types of money and transactions with it; and
* be critical of proposals which show signs of pressure, manipulation, or fraudulent actions.

**Provide insights** into the funds owner’s responsibility for all financial decisions (with their own money), even if the decisions are made under the influence of advertising and under pressure from scammers.

The methodological material is advisory in nature; the teacher can vary the tasks, their number, and change the stages of the lesson taking into account the students’ characteristics.

**Main theses of the lesson to be considered:**

1. Easy money - hard consequences: ways to involve young people in criminal activities.
	1. Children are victims of financial fraudsters.
	2. Children are accomplices of financial fraudsters.
2. Neural network as a modern tool for financial crimes. Fraudulent schemes using artificial intelligence.
3. Protected means armed: how to protect yourself from financial fraud.

# Section 1. Easy money - hard consequences: ways to involve young people in criminal activities.

## Children are victims of financial fraudsters.

In real life, children and youth become victims of scammers just like adults. The number of remote frauds against minors is growing steadily[[1]](#footnote-1).

As a rule, attackers try to get to the parents or children’s bank card. “They manage to unmistakably play on the qualities inherent in children and adolescents - gullibility, inability to think critically, easy attitude towards money, lack of communication and a thirst for encouragement and recognition.” [[2]](#footnote-2)

There are more and more forms and types of financial fraud against minors. Fraud schemes are becoming more and more complex with the development of information and communication technologies. However, our task is to learn to recognize such threats and counter them.

Here is a real example of a **phone scam**: Criminals convinced a 12-year-old girl that her grandmother had been hit by a car, so she gave a stranger cash for medical treatment.

*On 21 November, 12-year-old girl’s home phone rang - someone was crying a lot on the other end of the line. The schoolgirl thought that it was her grandmother’s voice. Afterwards, she immediately received a call on her cell phone, an unknown person said that her grandma had been hit by a car -**she was seriously injured, the treatment required 600 thousand conventional units. The girl promised to help: according to the instructions from the caller, she prepared a towel, paper, bed linen, took 50 thousand from her father and packed it so that no one could see what was inside.*

*Soon an unknown man came to her place - he was wearing sweatpants and had a dark beard. The girl gave him the money, hoping that grandma would get better soon.*

*Later, the father learned about his daughter’s feat - the man immediately guessed everything and wrote a report to the police.*

This example is a very common example of scammers deceiving children and teenagers. Next, we will take a closer look at how this scheme is implemented in life.

Let us consider the following example of **using a fake social media account**.

*In early October, a 14-year-old girl received a message on a social network allegedly from a friend. He claimed that the schoolgirl’s parents’ accounts and money were in danger. This was due to their personal data being available on the Internet, which can be used by scammers.*

*The “friend” immediately offered a solution to the problem. He told the girl how to save her family savings. The schoolgirl followed the advice. She took her parents’ bank cards, which were on the ottoman in the entrance hall, photographed them from all sides and sent the pictures to her friend.*

*As a result, 280 thousand conventional units disappeared from the adults’ accounts. The victims contacted the police. It was established that the girl’s friend’s page was hacked, and scammers communicated with her on his behalf.*

In this case, we see that the scammers used a scheme to create a fake account that was not related to the user and conducted correspondence on behalf of another person.

Unfortunately, these examples are far from the only forms of fraud that adults, children and teenagers face. The most vulnerable link in this chain is still **the person, their reactions and emotions**. If you “hack” into a person, you will hack into anything else. This is exactly what scammers take advantage of.

A fraudster has two goals: to deceive and to steal. This is a gambling person, a player. They do not feel any remorse for their actions, and it is naive to hope that they will come to their senses or stop.

Moreover, the behavior of a scammer and a victim are somewhat similar.[[3]](#footnote-3)

For a fraudster, their actions always imply excitement, desire to get adrenaline, and over time, crime becomes their favorite business. The portrait of a fraudster looks like this: it is an intelligent, artistic, talkative, enthusiastic person, a performer who makes a good impression, they are constantly developing new options for deception.

Psychology of the victim also implies the personality traits which allow them to fall for the scammer’s trick, plus a special social programme of behavior. For example, someone wants to save the world, and then receives an SMS message which says that a relative is in danger. Someone is afraid of the police, and they call this person and introduce themselves as police officers.

In this case, fraudsters use social engineering techniques.

**Social engineering is:**

...psychological manipulation of people to perform certain actions or disclose confidential information.

**Social engineering is evil.**

Social engineering underlies all methods and types of cyber and telephone fraud:

1. fraud or breach of trust;
2. psychological pressure; and
3. manipulation.

Under the influence of social engineering, the victim voluntarily parts with money or reveals personal and financial data the attackers need to steal funds.

**How this method works:**

*1. Attackers use feelings and emotions:*

* Inattention
* Greed
* FEAR
* Trust
* Sympathy

*2. Attackers use the news agenda.*

Attackers always exploit the hottest topics:

* Mobilization
* Special military operation
* COVID-19
* Elections
* Gaming and sports championships

There are two types of **emotions** evoked by information from scammers:

1) negative

* fear, panic
* feeling of shame

*“All the money has been debited from your account.”*

*“Your relative has had an accident and hit a person.”*

*“This is an investigator; your mother is a participant in a corruption or... case”*

*2) positive*

* joy, hope
* desire to get money.

*“You’ve won a large sum of money.”*

*“You are entitled to bonuses in the game.”*

**FORMULA FOR SCAM SUCCESS**

* unexpectedness
* emotions
* psychological pressure

Stage 1 - scammers influence basic emotions (fear, joy, sadness, surprise, curiosity, anger). These feelings come to the fore in any stressful situation as a human defense mechanism when we unexpectedly hear some news.

Stage 2 **-** after activating basic emotions, scammers use certain **psychological techniques[[4]](#footnote-4)**, which are successfully used especially in oral and telephone conversations:

• A set of short questions practiced by scammers hundreds of times. By quickly answering them without interrupting the scammer, the person enters a state close to trance or hypnosis.

• A certain tone of voice: formal, or insinuating and confidential, or joyful and enthusiastic. This heightens the victim’s emotional response.

• Haste and acceleration of events, in which the victim temporarily loses the ability to logic and analysis and follows the scammers’ instructions.

• Threats, intimidation, false information.

• If a person turns out to be in a whirlpool of deception, they may be told that everyone around them is an enemy, and that no one needs to be trusted, or share what is happening to you with. That is why it is so difficult to dissuade the victim, and they do not say anything to their family and others.

We have already looked at several real examples of scammers’ actions. Let’s take a closer look at the forms of fraud that minors can fall into.

1. ***Telephone and Mobile Scam*[[5]](#footnote-5)**

Someone calls/SMS message is sent to a potential victim.

“*My phone rang. Who is speaking?..”*

And then you can hear different options on the other side of the line:

* *Bank security service*
* *Bank employee*
* *State Security Officer*
* *Police captain*
* *Senior investigator*
* *Daughter, it’s me….*
* *This is your father’s friend….*

If a scammer poses as a bank security officer, they usually say the following:

*“Your card (account) is blocked.”*

*“They are trying to transfer money from your card.”*

*“Criminals have gained access to your accounts (your father’s accounts) and the money needs to be transferred to a secure bank account...”*

*“Suspicious transactions have been detected on your card...”*

*“They are trying to take out a loan in your name...”*

When a “police lieutenant” calls, a law enforcement officer may say the following phrases:

*“Your relative has hit a man...”*

*“Using your fake documents, someone is trying to take out a loan for a large sum... We need to clarify its details...”*

*“You became a witness in a criminal case against your classmate...”*

In such schemes, attackers offer to solve the problem in the following way and offer this to their victim:

* Withdraw all money from the victim or their parents’ bank cards and transfer it to a “safe” account or to a special bank account.
* Exhaust the credit limit on the card and transfer it to a “safe” account.

False employees of banks or law enforcement agencies, government agencies send their victims false documents made through online document editors. Communication takes place via instant messengers and social networks. The avatar often bears the icon of a bank or government agency. More than one person is often involved in the scheme, and after a call from one employee, another employee calls from another department, office and from another number.

If the scammer introduces themselves as a relative / friend / acquaintances’ son, they usually say:

*“Our grandmother has had an accident; she urgently needs medicine...”*

*“I’ve hit a child with my car, but I’ve already agreed on a bribe, I urgently need money.”*

*“Your father has just hit a man in a car accident. I'm ready to help avoid punishment.”*

In such schemes, scammers often report that a relative was hospitalized or had an accident. All this is said quickly and with the most authentic acting to put the potential victim under stress and prevent them from thinking rationally.

Then the “alien voice” asks you to collect all the money in the house, any items and put them in a bag. The attackers send a courier to the victim’s address to collect the money. The “parcel” is picked up by a special courier. Then both the money and the scammers disappear. More than one person is often involved in the scheme.

Scammers steal parental card data without the participation of couriers and cash in the same way. Example:

 *On 21 November, 15-year-old schoolboy’s cell phone rang. On the other end of the line, the scammer introduced himself as a streamer. He said that he randomly chose him to participate in the online stream and was ready to pay him a ticket to another city to participate in the stream, but he would need boy’s passport and his or his parents’ bank card photos for this.*

The **signs** that a scammer called or wrote may include the following:

* Call late in the evening, at night or early in the morning at weekends.
* You are required to take immediate action.
* They rush and intimidate, put pressure on emotions.
* They require that you provide confidential information: card details, PIN code or one-time password from the SMS message.
* If you refuse to give your details, they threaten that the money from your card will go to the scammers immediately.

**2. Cyber Fraud**

The gradual IT development of the world has led to the emergence of a new type of villains - cyber fraudsters.

During the Covid pandemic, many areas of life moved online, and cybercriminals (**scammers, black hats[[6]](#footnote-6),** fraudsters) have also intensified their activities on the Internet.

Researchers define cybercrime as any illegal act which violates human rights and freedoms through computer systems and networks.

Cyber fraud is one of the types of cybercrime.

The purpose of a *cybercrime* is to cause material or other damage by stealing the user’s personal information (bank account numbers, passport details, codes, passwords, etc.). It is implemented in different forms we will discuss further on.

There are a lot of forms of cyber fraud which target minors. Let’s look at a few of them.

**2.1. Phishing**

... a type of fraud in which attackers send emails and try to deceive recipients into doing some action:

* follow a malicious link;
* download an infected attachment; and
* provide personal data and other confidential information.

In English “phishing” is consonant with “fishing” (catching fish).

Phishing often underlies most financial cybercrimes.

Example of a phishing scheme:

***A phishing email*** is an email which contains a malicious attachment, a link to a fraudulent site, or malicious software.

Viral malware disrupts the system on your phone or computer, collects data, copies or destroys files.

These letters may look like messages from completely respectable sources: online stores, banks, services, etc.

Scammers use the following tricks in such letters:

* Delivery services
* Marketplaces
* Cryptocurrency
* Breaking news
* Lotteries
* Additional income and investments
* Tour operators and holidays
* Event tickets
* Subscriptions and online services

The final goal is most often to gain access to the finances or personal data of defrauded users.

Still, criminals are interested in login passwords which can be used to log into various services, as well as information contained in laptops and computers. **Trap links** help them take possession of them. They are sent to teenagers with an offer to look at some interesting photos “from a party or concert,” and when they click on the link or open the file, malicious software is installed on their computer or phone.

Scammers offer to register on special websites for other children in order to participate in voting, after which the child’s phone is infected with malware, and the scammers have access to the personal information.

***Fake Websites and Applications***

Fraudsters may create phishing sites which offer goods and services, e.g., computer equipment, *at lower prices*. There are a lot of fraudulent sites which resell in-game currency, skin graphics (skin design) or items for computer and telephone games.

After selecting a product or service and form of payment, the user is asked to enter their bank card details (card number, CVV code). After they agree to make a payment, the credit card details are transferred to the attackers, which the user is not even aware of.

The method of cyber fraud in various areas of business aimed at appropriating funds is called **fraud[[7]](#footnote-7)**.

In addition, scammers create fake bank websites to obtain customer data from their personal account. The domain name usually differs from the real one in such Internet resources.

Phishing gaming resources are also created to **steal accounts** from gamers and then extort money in exchange for returning access.[[8]](#footnote-8)

*In 2022, 183 domains with names related to the Warface online game appeared on the RuNet. All links to resources open a website with the same design. The page depicts four classes of fighters from Warface with premium ammunition and the text encouraging people to receive expensive items as a gift. When you click the “Login and Pick Up” button, an authorization window where you need to enter your login and password for your account in the game opens. After stealing the game account, the attacker evaluates the character and ammunition and addresses to the victim with a ransom offer. The amount that scammers ask from Warface players varies from 100 to 4 thousand conventional units.*

The fraudulent scheme is as follows: a person thinks that they are participating in a promotion from the developers, enters their login and password on a fake site and loses access to the account, since the login and password fall into the attackers’ hands.

Another wave of fraud is the emergence of resources which offer users who became the victims of the Internet criminals to receive compensation for participating in popular fake surveys, “unfair” lotteries or tax compensation, but they write off money and steal bank card data instead[[9]](#footnote-9).

This scheme is called "Double Deception". Its authors will use the so-called “defrauded investor syndrome,” when deceived victims give their money in order to be helped to recover the lost funds.

**2.2. Cyber Threats in Games, Social Networks and Instant Messengers**

Fraud using instant messengers and social networks has been increasingly gaining momentum recently.

It is implemented in various forms, the most common examples of which we will consider below:

* Fraud on social networks and instant messengers, including
* Voting
* Account hacking
* Digital cloning
* Quick earnings
* Online pyramids
* Online marketing fraudsters

Fraud on **social networks and instant messengers** is often similar to telephone scam, but first there may be correspondence, and then the deception scheme can be implemented in various ways - by telephone, through phishing, etc. The most popular purpose of such fraud is fraud with bank cards, that is, obtaining card details.

One of the methods of deception: a message arrives on behalf of a popular blogger about a gift or a potential bonus, to receive which you need to send the card details. The “coveted winnings” will be received to the card. In this state, children and teenagers send their own or their parents’ cards’ details, as well as passwords or personal data. Next, the fraudster steals all funds from the card account.

The described scheme is one of the popular deception methods - a message comes, for example, on behalf of a popular blogger about a gift or a potential bonus, to receive which you need to send the card details.

*A woman applied to the police and said that an unknown person had contacted her son on the Telegram social network posing as a blogger. The “blogger” reported that the boy had won the competition, and he needed to take his mother’s phone and take a photo of the screen to receive the reward. The scammers needed it to see what applications were installed on the phone and find out which bank’s application the boy’s mother used. Thus, the scammers understood which remote access application could be installed. Then the teenager acted on the instructions of the fraudulent bloggers but does not remember what exactly he did. The next day after communicating with the “blogger,” the correspondence was automatically deleted, and 235 thousand conventional units disappeared from the boy’s mother’s account.*

Cyber fraud is often associated with various games.

*Scammers came up with a scam based on a popular mobile game. They created a telegram channel for online shooter fans and offered to place bets promising to make money in tournaments for this game. A 14-year-old teenager made very large bets and transferred 100 thousand conventional units from his mother’s account to a Qiwi wallet and phone numbers. As a result, he did not receive any money.*

What kind of fraud scheme is used here: communication goes to the messenger, which is the first suspicious sign. The player is asked to place bets with real money, which is also a suspicious sign. Official payment is used not through a game account, but through third-party wallets and applications, payment in favor of individuals, which is a confirming sign of a fraudulent operation.

Recently, online (multiplayer) games, where you can spend money to increase the player’s level, buy additional features and move to a higher gaming level, have become especially popular. Players must enter bank card details to pay for these upgrades or purchase in-game currency, and these data are stored in their personal game account.

Scammers catch the player in the game by offering in-game currency, graphic designs (skins) or items. ***Communication takes place in the messenger*.** Thenfraudsters may ask for your account login and password by offering a “good buy” that is difficult to turn down.

So, a substantial bonus in the form of a large sum of money, gold using a promotional code, or rare skins is promised for personal data. Children and teenagers may not immediately understand that they have fallen into the scammers’ trap, but the result remains the same - the scammers steal all the money and personal data.

Exactly the same fraud scheme is used with the purchase of improvements for games, in-game currency, etc., various goods and services through free advertisement sites or private advertisement sites.

*A teenager lost money due to scammers on New Year’s Eve when he tried to buy a gift on a free classifieds website. The headphone seller offered to communicate on WhatsApp. He wrote that the goods and delivery needed to be paid for. The teenager transferred the money for everything, but the seller stopped communicating.*

In this case, the sites on which the advertisements are posted are well-known and reputable, however, the advertisements are posted by scammers. Correspondence is conducted with them, a product or service is paid for, but in return, at best, the buyer receives nothing, and, at worst, they give fraudsters access to their bank cards and personal data.

Deception when dating online is another type of cyber fraud with young people. The main goal of scammers operating under this scheme is to obtain personal data of a potential victim and access to their accounts.

The dating scam is designed for young men and women. A guy meets a girl online, she offers to spend time and makes a first date in a specific place - in a theater, at a concert. She sends a link to purchase tickets; the site is fake. The victim loses all the money from the card.

Let’s give another example.

*A young man met a girl on social networks and communicated with her for two weeks. Periodically, she asks to pay her for all sorts of inexpensive “goodies” so that they could meet - put money on the phone, buy her a comic book, pay for a manicure, etc. And so, she writes: “I’ve booked movie tickets for us, now you will receive an SMS with a payment code, can you, please, dictate it to pay for these tickets.”*

*The guy dictates the codes from the SMS message to her. After that, all the money is debited from the card, and the girl stops responding to messages and calls and deletes her account.*

In such cases, suspicion of fraud should arise when strange offers, primarily, of a financial nature, appear.

Fraud on social networks and instant messengers is also linked with scammers’ hacking into other people’s accounts, creating digital doubles of some familiar faces or other people. This is the so-called scheme to ***take over a messenger or social network account***[[10]](#footnote-10).

Often, children and teenagers become objects of deception on behalf of their “friends/acquaintances” who ask for a loan for a couple of days or find themselves in a “difficult life situation.”

Fraudsters gain trust and establish contact from fake accounts, sometimes by faking the pages of adults the child knows. While communicating, attackers are trying to find out all sorts of details about family life from children and teenagers: where parents work, when they are at home, who they communicate with, what they buy, where they go, what the names of family members are, what kind of cars mom and dad have. They do not act head-on, they ask questions carefully, from afar. Fraudsters can quietly obtain all this information from a child by communicating with them on social networks.

Then they skillfully use this information. As they know the names and details of someone else’s family life, they call the children and teenagers’ parents, their relatives and use the information that is credible for potential victims and blunts their vigilance. Next, the fraudster tries to take possession of the victim’s funds in every possible way.

In this case, after receiving the information from the child, the fraudster can call some grandmother and not only say that “your daughter has had an accident,” but he calls this daughter by name, knows the make of the car, the names of her friends and relatives, and her place of employment.

Moreover, a message can come from a friend or acquaintance with various requests: to vote, like, lend money, buy a ticket, etc.

*Will you vote for me, please at* [*https://goo.su/CTcZ34nN*](https://goo.su/CTcZ34nN)*», if it’s no bother for you.*

The link sent by the attackers is made using a link shortening service. This tool is often used when the sender does not want the real website address to be visible.

When you enter your phone number on the scammer’s website, you will immediately receive a confirmation code, which will be used to “hijack” your account. In this case, this scheme can be classified as phishing.

**Fraudulent Schemes to Make Quick Money**

People are constantly offered to make quick money or invest money in supposedly profitable projects on the Internet or instant messengers. Popular schemes with quick money for children and teenagers include money for watching videos from popular bloggers, rating pictures and hotels, and voting in rankings.

Before starting the “work,” the scammer sends a link and asks to enter the bank card details (their own or their parent’s), as well as the code from the SMS notification, explaining that these details will be used to pay for the service in future or it is necessary to pre-pay the tax. After entering the details, all funds from the account are debited.

Criminals advertise to older teenagers how to make quick money using bookmaker bets on their resources[[11]](#footnote-11).

The attackers establish contact with a teenager and offer them to make quick money by placing bookmaker bets on their resources. The systems visually show the supposed success of such a child’s activity. To withdraw supposed earnings, teenagers are asked to pay a commission. As a result, money along with card details ends up in the hands of cybercriminals.

In addition, according to available statistics, the number of financial pyramids disguised as economic or business online games has increased[[12]](#footnote-12).

More than 22% of such projects attracted users by the opportunity to make money quickly and easily within the game - in the “pay and win” format.

A feature of such projects is the *absence of a competitive element*. *You pay - you win*.

Most of these pyramids are small anonymous projects with a short duration and a small sum for participation.

Their organizers target offers taking into account the age and preferences of potential participants, and use social networks and instant messengers for promotion.

The mechanics of such games is as follows. At the first stage, users are asked to register, then, to purchase a character or certain game attributes, which should generate “income” in future. These could be cheerful gnomes mining ore, birds laying golden eggs, or fishermen catching fish. After “mining,” the resource is converted into in-game gold, which can be exchanged for real money in theory. The catch is that despite the promises of the organizers, withdrawing money to a card will not work out just like that. Since the main goal of all financial pyramids is to attract as many new players as possible, you will be asked to “bring” a certain number of referrals to the game before withdrawing. To do this, the creators advise disseminating information about the project on social networks, instant messengers and personal blogs. The invested funds end up in the organizers’ pockets, and, at best, the players get back a small part of their investments, and, at worst, they are left with nothing[[13]](#footnote-13).

The main signs of a financial pyramid include:

* Lack of gameplay - lack of a competitive element, routine and repeated actions. The simpler the mechanics, the greater the likelihood of a fraudulent scheme.
* Paying money for attracting new participants. If you need to attract new players, this is a sign of a fraudulent scheme.
* Complex income calculation scheme. If generating income is very difficult, requires a lot of actions, there is some kind of formula for calculating income, it is most likely that the purpose of this is to confuse the player.
* Guarantee of high income without any risk and aggressive advertising on social networks. If game adverts are very aggressive, promise to earn money without risk, then this is most likely to be a fraudulent scheme.

Quick money adverts, as a rule, promise high income with a minimum waste of time and risks. In the first case, scammers convince people to pay for current expenses (e.g., drawing up questionnaires, taxes) or ask them to pay for services; in the second one, they ask people to transfer as much money as possible for a profitable investment by showing fictitious profit graphs. Always remember that any investment may result in losses.

All projects with signs of illegal activity are added to a special blacklist by government agencies[[14]](#footnote-14). Before investing money, you must check the resource in the registry and do not invest in it if it is on this list.

**Cryptocurrency and ICO Fraud Scheme**

In recent years, one of the most popular types of fraud has been fraud with cryptocurrencies, in particular, with fundraising for launching various blockchain projects, as well as crowdfunding (collective fundraising) for various new projects (be it the creation of a new game, the translation of a book, etc.). People invest, but there are no results, the invested money disappears. Such fraudulent projects are called **scam projects (scam)**.

Example of implementing such a scheme.

On special websites, attackers present a supposedly good project whose implementation required funds. For this, the so-called fake ICO (Initial Coin Offering - initial placement of **tokens** (coins) is used. This is a format for raising funds to develop cryptocurrency projects. Hiding behind this tool, scammers sell fake cryptocurrency for Bitcoin or Ethereum, which have real value (you need to pay real (fiat) money to buy them).

After several rounds of fundraising, the “innovators” (fraudsters) disappeared without a trace along with the collected funds. At the same time, it was almost impossible to track them, because all funds collected can be used anonymously.

The second scheme of cryptocurrency scammers is **Rug n Pull[[15]](#footnote-15)**. The point of the scheme is to issue tokens, most of which are kept by scammers, and only a small part of the coins is distributed among “investors”.

An important characteristic of possible “rugging the pull” is a coin that rapidly increases in value within a few hours. After a pump (artificial rise) in the token rate, scammers sell all their coins and withdraw funds, while ordinary users are left with tokens they do not need, which depreciate by almost 100%. Such a token cannot be sold (it becomes illiquid).

In 2023, scammers stole over $32 million from approximately 42,000 users using this scheme[[16]](#footnote-16).

The third scheme of cryptocurrency scammers is **pump and dump**[[17]](#footnote-17)- a type of scam which creates a false excitement, hype around a coin. Fraudsters create or buy (usually dubious) tokens at a low and favorable price for them. Then an imaginary excitement is created with the help of various chats and news posts. Hype and misinformation are used to create false interest in coins which have no known or immediate value.

People who do not know how to conduct a competent analysis of cryptocurrencies are starting to buy coins. A wave of such purchases comes, and the value of the token begins to rise significantly. When the price peaks and misinformation results in a buying frenzy, scammers and influential investors “dump” all their cryptocurrencies and cash them out for huge profits. As a result of the sale, the price of the coin will drop significantly below the original price, and it will be impossible to sell them[[18]](#footnote-18).

Therefore, before you start investing real money in various projects, you first need to study the cryptocurrency market and the project creators in more detail. You should not buy tokens that you do not understand.

ReasonLabs specialists noticed that ***several malicious extensions disguised as VPNs*** began to be installed en masse in the Chrome browser. Now the demand for VPNs has grown significantly; similar extensions are installed in many browsers. However, in this case, we are talking about malware.

The source of infection was the installers of the pirated games (Grand Theft Auto, Assassin's Creed and The Sims 4) downloaded from torrent trackers. A fake VPN was received along with the game.

The extension installed on the computer received extensive powers. For example, it could launch other malicious scripts, steal confidential data, change web requests, and disable extensions installed in the browser.

## Children are accomplices of financial fraudsters.

At the same time, children and teenagers do not always become victims of financial fraudsters as criminals involve them in their criminal activities.

Teenagers and young adults often look for part-time job on the Internet. Fraudsters take advantage of this by luring minors into their criminal networks. Dangerous money-making schemes include those when teenagers are offered for a percentage or fee to act as intermediaries or couriers in the transfer of money earned illegally.

There are different schemes for involving minors.

For example, they call a teenager and ask them to **provide courier services**: personally pick up money from one person and transfer it to the bank account of another and keep a percentage for themselves for the work done.

As a rule, such criminal activity is initiated from abroad using telephone calls, instant messengers, and computer programs. Teenagers receive clear instructions in the messenger from scammers on how to behave with people from whom they take money and how to transfer funds.

Before this, scammers fraudulently extort money from citizens by telling stories about the need to help a close relative in trouble. Citizens give money to underage couriers. They transfer the remaining amount to the attackers’ bank card for a reward and become **accomplices in committing the crime**.

*The courier collected more than a million conventional units from three elderly women. He turned out to be a 16-year-old young man. He admitted that he had wanted to quickly earn pocket money. A criminal case was opened on this fact.*

Participation in such schemes may result in criminal liability, and the punishment will be not only fines and the obligation to return the money, but actual imprisonment.

Another type of scammers among minors is those who call and lure money to “solve” the problem **posing as** a son, daughter or grandson in trouble (for example, an accident). Then an allegedly police officer joins the conversation and, without giving anyone time to come to their senses, says that the money urgently needs to be transferred through a courier. Older people who are taken by surprise often fall into this trap. The courier can also be a minor (including one who called under the guise of another person) who is found on the Internet. At the same time, swindlers who hired minors entrust the dirtiest work - taking the money - to special couriers.

*17-year-old teenager came into view of police investigators when an 81-year-old pensioner who the former took 100 thousand conventional units from contacted the police. The grandmother thought she was helping her granddaughter, who allegedly got into an accident and asked for money on the phone. The pensioner spared all her savings so that a case would not be opened against the young woman, but she thought of calling her family only after the courier left.*

*When the police detained the young man, he said that he had left a request in a group with vacancies on social networks in search of a part-time job. Soon he was offered a job at an investment company: collecting money from clients and sending it through an ATM to certain accounts. The young man agreed, sent his passport details to the “employer” and became a courier.*

*The investigators found out that the minor participated in several other similar crimes in the region of his residence. He also offered to a friend of his age to earn extra money. They went together to a neighboring town to do this “job”. And while one was monitoring the situation in the street, the other took more than 700 thousand conventional units from a 12-year-old girl who believed that her mother had been in an accident and needed expensive treatment. Such a large sum of money was at home at that moment, and the child knew about it.*

The next fraudulent financial scheme is the one of **illegal cash withdrawals and nominee directors**.

*Teenager wants to find a part-time job in his free time.*

*He sees an advertisement on one of the job search sites:*

*“An employee is required to work remotely with money transfers. Serious earnings for a few hours a day. Employment without checks and filling out documents. No work experience required. High income guarantee. Requirements: availability of a card from any bank of the Russian Federation.”*

These schemes use, among others, physical persons who help cash out and withdraw money after criminals commit a financial crime– so called **money mules**[[19]](#footnote-19).

This term is not used in legislation; however, government organizations and law enforcement agencies are increasingly using it due to the lack of comprehensive English-language analogues[[20]](#footnote-20). We will also use this term further in the text, as well as “a person cashing out funds obtained by criminal means.”

Most often, money mules do not even suspect that they are part of a large criminal puzzle. Money mules are not the initiators of the crime, but they *carry out instructions* and receive money for it. Most often, these people provide their bank card details to criminals for a reward. Sometimes an unsuspecting teenager is asked to have several bank cards.

Fraudsters transfer the stolen funds to the teenager’s cards, and then the teenagers transfer the funds to another person along the chain. Thus, criminals make it difficult for law enforcement to find funds and final recipients. In addition, teenagers are asked to cash out the money received on the card at various ATMs and take a small percentage for themselves.

Most often, the least financially literate, trusting people, and those who believe that they can make money quickly and easily become money mules.

There are two types of money mules:complicit and duped[[21]](#footnote-21).

The first type includes people who are aware of the criminal component of their activities and act voluntarily and intentionally.

Those who do not understand that they are in the scammers’ trap, and do not realize that they are participating in a scheme which violates the laware engaged in the second.

There are different schemes for recruiting money mules by fraudsters, for example:

1) Fraudsters place advertisements in the streets and on the Internet, including on social networks, offering work related to the transfer of money and cashing it.

2) Fraudsters post advertisements on telegram channels and social networks about interesting jobs in IT with rapid growth in earnings.

3) Fraudsters, when posting job advertisements, create phishing (fake) sites of large companies to lull vigilance and offer such part-time jobs.

4) Under the guise of law enforcement officers, scammers call the teenager with an offer to officially get a job searching for criminals and promise a monthly income. If a person agrees, scammers transfer the stolen money to their bank card and then demand to withdraw this money from an ATM under the guise of bank employees.

5) Scammers “accidentally” transfer money to a bank account under the guise of a mistaken person and then ask for it to be returned in cash or transferred to a card.

Attackers strive to make it as difficult as possible for law enforcement agencies to identify and track funds passing through cash-out chains. Scammers themselves resort to the services of dummies – money mules – to avoid responsibility for transferring or cashing out funds. Most of the scam organizers live abroad and even identifying them is very difficult, but almost all the money mule messengers are caught. They also face real imprisonment and will have to compensate for the damage caused.

Fraudsters can cover up the traces of payments for very serious crimes, they can evade paying taxes, and the teenager becomes an accomplice of the scammer.

When money mules agree to such activities, they bear very serious consequences which can affect not only their own and their parents’ money and property, but also their own and their family’s life and freedom.

What **consequences** can money mules’ actions result in: [[22]](#footnote-22)

1. Fraudsters may threaten the money mule and their relatives, blackmail.
2. Money mules become a participant in money laundering schemes, the sale of weapons or drugs.
3. Money mules will be looked for by law enforcement and tax authorities and other structures.
4. Money mules will become a defendant in a criminal case.
5. Money mules are responsible with their property and money, as well as their parents and foster parents’ property and money.
6. They will have to pay large sums of money for years.
7. Money mules create a negative financial rating for themselves and undermine their reputation.
8. A money mule can be killed to get rid of a witness.

Criminal legislation does not regard being a money mule as a crime, however, this action can be qualified **as theft, fraud, legalization (laundering) of funds obtained from crime**.

*A 19-year-old resident of the N region, who worked for scammers, was ordered to pay the victims 800 thousand conventional units, and she earned only 15 thousand conventional units. If the courier is a minor, this burden will fall on the parents.*

The victim of fraud must be compensated. And from the age of 14, a teenager must do this themselves: they pay the fine either from their earnings, scholarship, alimony or another type of income. If there are no opportunities to earn money, movable or immovable property (e.g., a computer, telephone, set-top box) may be used to offset the damage. But if the fine is quite large and the teenager does not have enough personal funds, the money is paid by parents or foster parents.

Also, the data on the offense will be sent to the authorities for the affairs of minors and protection of their rights.

What liability can minor fraudsters bear?[[23]](#footnote-23)

If we look at the definition of this act, fraud is a crime that consists of appropriating other people’s money through deception or misrepresentation. Well, a person most often transfers their money voluntarily to a criminal.

And taking advantage of the fact that criminal and administrative liability for most crimes begins at a certain age, adult fraudsters often attract minors to commit fraudulent acts by promising quick and “easy” money.

That is why teenagers should know that they will also have to be responsible for their actions.

Money mules’ services for cashing out criminal proceeds can also be qualified as legalization (laundering) of funds and committing it entails criminal liability.

Bank cards (drop cards) are often issued in the name of money mules; their number can reach more than 2-3, or even 10. **Criminal legislation** provides for criminal liability for illegal circulation of payment instruments, which means the production, acquisition, storage, transportation for use or sale, as well as sale of counterfeit payment cards, orders for the transfer of funds, documents or means of payment, as well as electronic means, electronic storage media, technical devices, computer programs intended for unlawful acceptance, issuance, transfer of funds.

**Immaturity and a frivolous attitude towards financial instruments can be very expensive!**

# Section 2. Neural network as a modern tool for financial crimes. Fraudulent schemes using artificial intelligence.

Artificial intelligence (AI) provides incredible new opportunities for business, industry, science, and education. But at the same time, cybercriminals (black hats, scammers) began to use neural networks.

Experts note that there is a growing wave of fraud cases related to the theft of personal accounts on Telegram.

Attackers increasingly use machine learning algorithms and neural networks to gain access to people’s personal information to defraud them. Criminals can use AI algorithms to create fake identities and conduct fraudulent transactions which are difficult to detect.

The main strategies of fraudsters using artificial intelligence include the following:

1. Attackers can create **fake documents** using artificial intelligence: the neural network will falsify bank statements, create a fake passport or driver’s license.
2. Neural networks are skilled at **creating pictures and illustrations**. This means that such images are easily used for fake fees. So before sending financial assistance to someone, it is worth checking if the recipient on other social networks and the Internet is real.
3. Fraudsters can use neural networks to create **fake news and newsletters**. They include various links to resources. If you click on them, you can lose your bank card details or other personal information.
4. **Phishing, fraudulent websites**: AI is used to create fake emails (generating any letters) and websites (parsing and reading any WEB files, even those closed from indexing, and immediately generating any unique materials in return) to deceive users and gain access to their personal data and financial resources.
5. **Social bots and manipulation in social networks**: AI is used to create (telegram) chat bots for payment and the ability to save payment data. All these schemes use the need to enter your phone number and SMS code. Then the obtained data are used by attackers to gain unauthorized access to your account and send spam or extort money after that.
6. Neural networks learn to **maintain a conversation**. Artificial intelligence can take on the role of imaginary employees of contact centres of banks and other organizations, which scammers pose as to deceive their victims, and conduct a conversation.
7. AI can create a **‘clone’ of the person’s voice or image (deepfake).**

Moreover, deepfakes include manipulated videos in which AI algorithms superimpose one person’s face onto another’s body making it appear as if the person in the video is saying or doing something they have never actually done or said.

Taking into account the development of biometrics and the ability to apply for a loan over a call (modern technologies identify a person by the timbre of their voice), deepfake will be one hundred percent similar to the original, which means that the victim risks remaining in debt without knowing anything about it.

In addition, criminals began to use artificial intelligence to fake voice messages in Telegram to steal money and accounts. Let’s cite a real example.[[24]](#footnote-24)

*Telegram users are faced with a new type of fraud - first, criminals gain access to the account, then begin writing to potential victims from the owner’s contact list with a request to transfer money. The criminals reinforce the story about the need for help with a voice message supposedly on behalf of the account owner. The audio message uses clips from their actual old voicemails.*

*The audio message is duplicated in personal correspondence and in all the chats where the owner of the stolen account is a member. Then a photo of the bank card with the first and last name is sent. Moreover, the first and last name of the affected interlocutor on social networks differed from the information in the passport, and the scammers used the passport data. The amount that the criminals wanted to get was 200 thousand conventional units.*

At the first stage, a Telegram or WhatsApp account is hacked, for example, through fake voting. Then the scammers download the saved voice messages and synthesize new voice messages with the necessary context using artificial intelligence services. Finally, messages are sent in private messages or group chats with a request to borrow a large sum of money; artificial intelligence-generated voice messages and a photoshopped bank card with a fake recipient’s name are used to be more convincing.

This scheme is dangerous because scammers use several factors to identify the victim - **account, voice and bank card**.

In order not to lose money, you need to double-check whether the account owner is really making such a request, for example, by calling them back on the phone.

There is no fundamental difference in whether you are communicating with a real attacker or a robot. Security rules do not depend on the schemes used by fraudsters – using AI or not.

1. Attackers can also use a fraud scheme related to **false registration in** **ChatGPT**[[25]](#footnote-25)**.**

This chatbot is banned in a number of countries. However, scammers offer to “facilitate” access to a popular foreign neural network using a special service or application. In turn, a link to the service can lead to phishing resources disguised as services for selling accounts in the ChatGPT neural network for little money. Most often, scammers create fake websites that are **very similar** to the official ChatGPT website.

When registering on this resource, you will need to fill out a form with payment information, or you will be provided with a link to a malicious program, for example, a remote device control program. When attackers install it, they gain full control over the user’s gadget. Ultimately, all this will lead to loss of money.

# Section 3. Protected means armed: how to protect yourself from financial fraud.

# .

We have considered various types of fraudulent schemes used to commit financial crimes. Victims of such crimes can be people of **any age, both adults and young people**. Therefore, it is necessary to remember a number of techniques which will allow you to protect yourself from financial fraud and avoid becoming a victim of criminals. Let’s consider them from the general to the specific.

First of all, scammers use methods of social engineering and psychological pressure.

In this case, experts[[26]](#footnote-26) offer the most effective recommendation - stop talking, switch off, look around, look at the situation in the room, return to reality and calmly think about everything in silence.

Any situation must be approached **with a critical perception**. It is recommended to view with a dose of skepticism all calls when the interlocutor sends you somewhere, persuades you to take some action, demands to transfer money or formalize something.

You need to remember a few **simple general rules**:

- If strangers begin to dictate the course of action, it means they are trying to pull a fast one on you.

- Promises of quick profits are always a warning sign.

- Do not follow unfamiliar links.

- Do not give bank card details to strangers.

You should not respond to alarm calls, letters, SMS messages or messages on social networks saying that a relative or friend needs money. In this case, you must try to contact this relative or friend and inform them that such messages are being sent on their behalf; perhaps their account has been hacked.

If even one doubt arises, or some incomprehensible or frightening action we talked about earlier occurs you need to stop and **ask for advice from family and friends**! If you cannot reach them by phone, you need to call the police on 112.

Next, we will consider the algorithm of actions in typical fraudulent schemes which will minimize or prevent financial risks.

**Action Rules for Phone Calls:**

1. Check the incoming number carefully.
2. Do not answer unknown and dubious numbers at all or call them back. Even if the phone number seems correct, you should always check the numbers in official directories and on official websites.
3. It is MANDATORY to call your family or friends/bank/organization/police yourself and ask them for help.
4. Stop the conversation if it concerns financial issues.
5. Remember that the financial intelligence and banking regulators never call individuals.
6. Do not perform any operations or actions following the instructions of the caller.
7. Never share verification codes from SMS messages with anyone.
8. Do not provide CVV/CVC and other bank card details over the phone or in correspondence.

9. Do not rush to make a decision.

10. End the conversation immediately if any doubt arises.

11. Install an application to filter incoming calls. Block calls from suspicious numbers.

12. Check whether there were any questionable transactions during the conversation (on a card, in an SMS message).

13. Play a game with your parents which simulates calls from a bank representative or the police. You need to answer clearly and quickly: “Thank you, goodbye, I’ll call you back.” And repeat this 10 times so that the person develops a model of behavior. And then call the bank back and find out what they wanted from you and whether they wanted it.

14. With your parents and family, you can come up with a code word which will show that something is wrong.

**Action Rules with Bank Cards and Payment Transactions:**

1. Do not give your bank card to strangers. Demand that operations with it be carried out only in personal presence and try never to lose sight of it.
2. Do not make purchases or enter the CVV/CVC code on dubious sites. The website of a reliable online store will never ask for personal information: card PIN code, passwords for mobile banking and electronic mailboxes linked to plastic. These data must not be left anywhere!
3. Card details (number, PIN code, CVC code) must not be disclosed to anyone, even bank employees.
4. You must not write the PIN code on the card and store it separately. When entering a PIN code, you should always cover the keyboard with your hand, including when paying in cafés and shops.
5. If your bank card is lost, you must immediately notify your parents, then contact the bank and block it. You should do the same if you receive an SMS message about a purchase or withdrawal of money from an ATM, but you haven’t done it. For this purpose, it is useful to have the bank support phone number at hand.
6. If you receive suspicious SMS messages indicating that the card is blocked or funds were transferred from it for a transaction that was not made, you must inform your parents. **You must not** call back the number from which the message came.
7. Always inspect the ATM before using it. You need to make sure that there are no foreign objects attached above the keyboard and on the card reader, and that the keyboard does not wobble.
8. Do not use free Wi-Fi hotspots (Internet in public places: transport, cafés, cinemas) when accessing online banking or using a mobile banking application.
9. Payment in an online store should not occur as a transfer of funds to someone’s **personal account**. If this happens, **you must not send money**. In this case, you need to contact your parents to help you choose a reliable store.
10. Mobile devices on which online banking applications are installed cannot be transferred to unauthorized persons.

**Action Rules on the Internet and in Correspondence to Protect against Phishing and Cyber Fraud:**

1. You should not believe information about winnings, pay money to participate in challenges and be deceived by easy earnings.
2. Do not click on links in letters or messages about winning money, a gadget or other prize, and do not click on suspicious objects. If you follow the link, you are most likely to only receive a virus. Hover your mouse over a suspicious link/object and you will see where it actually leads. Compare it with the company’s official website.
3. It is dangerous to download any applications at the request of strangers or open unfamiliar and strange links. Even if the link seems reliable, you should always check the addresses with the domain names of the official websites of the organizations.
4. **Never** communicate confirmation codes from SMS messages **to anyone** in correspondence.
5. Pay attention to the email domain which the letters come from. Fraudsters usually use public domains gmail.com, mail.ru, etc., or domains similar to official company names (e.g., sberbankc[.]ru, lc-sberbank[.]com, etc.).
6. Study the subject of the letter or message, the content of the letter and the file names. Pay attention to proper writing. If the message encourages you to take immediate action, this is a suspicious sign.
7. Pay attention to the address and signature. If they are impersonal, or there is a sign of auto substitution in the address, it is highly likely to be phishing.
8. Be careful with attachments to letters or messages. Open only those attachments that you have been waiting for. Check the attachment extension.
9. If a letter or message requires that you enter data (login, password) on suspicious websites or in questionnaire forms, you must delete this letter.
10. If a bot or robot asks you to enter personal financial information (codes from SMS messages from the bank, full card details, full name, passport details, etc.), during communication in the messenger, you must interrupt the communication, contact the bank branch, or independently contact the organization using official contacts listed on the company’s official website.
11. Passwords on social networks in honor of your favorite pets and birthdays are, of course, easy to remember, but it’s better to choose something more complicated. Because scammers will easily pick them up. And if they are written down somewhere, you must not take a picture of this piece of paper and send it somewhere.
12. You must not take photographs and send your personal data and parents’ data, copies of passports and other documents, bank cards and money to strangers.
13. You must not share information with anyone about the home, school, place of work of parents’ address, what applications family members have on their phones, any passwords and PIN codes.
14. It is better to communicate only with friends and relatives who write from familiar numbers and pages. And if a stranger wrote and asked to be your friend, and then started asking for the information listed above, they definitely cannot be your friend.
15. It is necessary to personally verify all information received from friends or relatives on social networks and instant messengers. That is, if a friend suddenly asks for money to pay for a parcel, it is better to call back and hear the request in conversation.
16. You can make purchases only with your parents’ consent, in trusted online stores; you must not transfer full prepayment for the goods if you are not sure of the reliability of the seller.
17. It is dangerous to purchase virtual money, game improvements, as well as paid game content and other bonuses.
18. An offer to communicate via messenger, and **NOT THROUGH** the official websites of online trading platforms is the first sign of a scammer. It is necessary to check the seller ratings and reviews. It is advisable to make a purchase together with your parents or pay for goods only through a secure transaction on the free classifieds site.
19. You need to protect your accounts - you need to enable two-factor authentication wherever possible.
20. The security of your profile on social networks should be ensured - access to personal information on social network pages should be blocked for outsiders by making them private.
21. It is important to use antivirus software and update it regularly to protect your computer from malware.
22. If you decide to use the services of a neural network yourself, make sure that you are actually on the official resource. Do not click on dubious links that ask you to enter payment information and do not install unknown applications on your devices.
23. If you feel something is wrong in a conversation, it would be best to ask your interlocutor a random question - this will help you understand that you are communicating with a real person and not with a bot.

# Appendices

# Appendix No. 1. Glossary

**Money mule** – a fictitious individual who has registered payment means (bank plastic cards, bank accounts, electronic wallets, crypto wallets, etc.) and/or registered themselves as an individual entrepreneur (IE) and/or director and/or founder of a legal entity without the purpose of real participation in business activities with subsequent transfer (sale) of electronic means intended for managing their means of payment and/or bank accounts and the financial activities of organizations registered in their name and/or individual entrepreneur to third parties for monetary compensation or other tangible or intangible values. Money mules also include individuals who provided their personal data and documents for identification when conducting financial transactions with cash belonging to third parties and in their interests.

**ICO** (Initial Coin Offering) - initial coin offering or initial placement of tokens - a form of attracting investments through the issuance and sale of digital tokens for fiat money or other cryptocurrencies to investors.

**Investments** – cash, securities, other property, including property rights, other rights with a monetary value invested in objects of business and (or) other activities in order to make a profit and (or) achieve another useful effect.

**Investor** – a person making investments.

**Investment project** – a set of measures limited in terms of implementation time and expended resources aimed at the creation and subsequent operation of new objects (e.g., goods, services) or modernization of the existing ones through investments (e.g., financial).

**Crowdfunding** –financing collectively a project, a company, producing a product or service, etc. It is implemented in various forms.

**Cryptocurrency** – ***digital currency*** – a set of electronic data (digital code or designation) contained in an information system that is offered and (or) can be accepted as a means of payment which is not a national monetary unit, a monetary unit of a foreign state and (or) an international monetary unit or a unit of account, and (or) as an investment and in respect of which there is no person obligated to each owner of such electronic data, with the exception of the operator and (or) information system nodes obliged only to ensure the compliance with the procedure for issuing these electronic data and implementing them in relation to actions to make (change) records in such an information system and its rules.

**Crypto market** – cryptocurrency market – a platform on which cryptocurrencies are traded.

**Scam project** (scam) – a fraudulent investment project created to obtain quick profits.

**Social engineering –** deception and manipulation which tricks victims into doing things they should not (e.g., making electronic fund transfers, revealing credentials, etc.).

**Fiat money** – (from the Latin “fiat” - decree, instruction, “so be it”) – money not backed by gold or other precious metals, whose nominal value is established and guaranteed by the state, regardless of the cost of the material used for its manufacture. In other words, this is the legal currency of any state, for example, rouble, yuan, dollar.

**Financial pyramid** – a type of fraudulent scheme in which the founders cover obligations to investors with money from new investors.

**Black hats** – criminals who maliciously hack into computer networks. They also create malware which destroys files, locks computers, and steals passwords, credit card numbers, and other personal information.

# Appendix No. 2. Resources

**Materials:**

Как защититься от кибермошенничества. Правила безопасности в киберпространстве. Банк России [How to protect yourself from cyber fraud. Security rules in cyberspace. Bank of Russia] [Electronic resource]. - Access mode: <https://dni-fg.ru/16>

Чадо кутежа: преступники подбираются к счетам россиян через детей. [Child of revelry: criminals are approaching the accounts of Russians through children] [Electronic resource]. - Access mode: <https://iz.ru/1592828/ivan-petrov/chado-kutezha-prestupniki-podbiraiutsia-k-schetam-rossiian-cherez-detei>

Как защитить себя и близких от киберугроз? Минцифры РФ [How to protect yourself and your family from cyber threats? Ministry of Digital Development of the Russian Federation] [Electronic resource]. - Access mode: <https://киберзож.рф>

Кибербезопасность - это просто на ГосУслугах [Cybersecurity is easy on GosUslugi (State Services)] [Electronic resource]. - Access mode: <https://www.gosuslugi.ru/cybersecurity>

Ассоциация Развития Финансовой Грамотности [Financial Literacy Development Association] [Electronic resource]. - Access mode: <https://fincubator.ru/company/>

Международный учебно-методический центр финансового мониторинга. Медиатека [International educational and methodological centre for financial monitoring. Media library] [Electronic resource]. - Access mode: <https://mumcfm.ru/mediateka>

Международная Олимпиада по финансовой безопасности. Материалы для подготовки [International Olympiad in Financial Security. Materials for preparation]: <https://rosfinolymp.ru/prepare>

***Video Presentations***

Кибермошенники: новые сценарии [Cyber fraudsters: new scenarios] [Electronic resource]. - Access mode: <https://iz.ru/1592828/ivan-petrov/chado-kutezha-prestupniki-podbiraiutsia-k-schetam-rossiian-cherez-detei>

Безопасность в онлайн-играх [Security in online games] [Electronic resource]. - Access mode: <https://rosfinolymp.ru/prepare>

Фишинг [Phishing] [Electronic resource]. - Access mode: <https://моифинансы.рф/materials/video-lekcii-o-tom-kak-ne-popast-na-ulovki-finansovyh-moshennikov/>

Фишинг в социальных сетях [Phishing on social networks] [Electronic resource]. – Access mode: <https://rosfinolymp.ru/prepare>

Современные финансовые пирамиды [Modern financial pyramids] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/13408>

Дропперы [Money mules] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/13326>

Безопасность персональных данных [Personal data security] [Electronic resource]. - Access mode: <https://rosfinolymp.ru/prepare>

Безопасность мобильных устройств [Mobile device security] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/13321>

Противодействие псевдоинвестиционным проектам [Countering pseudo-investment projects] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/13320>

Кибербезопасность. Виды мошенничества [Cybersecurity. Types of fraud] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/12931>

Не сообщайте мошенникам ваши личные данные! [Do not give your personal information to scammers!] [Electronic resource]. - Access mode: <https://mosobr.shkolamoskva.ru/release/12385>

1. В Москве аферисты стали чаще похищать деньги у детей [Swindlers more often steal money from children in Moscow] // РИА НОВОСТИ. 18.12.2023. URL: https://1prime.ru/finance/20231218/842595387.html [↑](#footnote-ref-1)
2. Россиян предупредили, что новая цель мошенников — дети [Russians warned that children are the new target of scammers] // Прайм. Агентство Экономической информации. 24.11.2023. URL: https://1prime.ru/exclusive/20231124/842355112.html [↑](#footnote-ref-2)
3. Федяшева Е. Как не стать жертвой кибермошенников: новые схемы обмана, портрет афериста и правила безопасности от воронежских экспертов. [How to avoid becoming a victim of cyber fraudsters: new deception schemes, portrait of a swindler and security rules from Voronezh experts] 24.11.2023. URL: <https://www.vrn.kp.ru/daily/27586.5/4856275/> [↑](#footnote-ref-3)
4. Халезова Н. «Я была одурманена»: реальные истории жертв мошенников. Как их распознать и можно ли помочь? [Khalezova N. “I was stupefied”: real stories of scammers’ victims. How to recognize them and is it possible to help?] // LifeProfit, 15.08.2023. - URL: https://life.akbars.ru/personal-finance/istorii/ya-byla-odurmanena-realnye-istorii-zhertv-moshennikov-kak-ikh-raspoznat-i-mozhno-li-pomoch/ [↑](#footnote-ref-4)
5. Кибербезопаность\_как\_не\_стать\_жертвой\_в\_финансовом\_мире. [Cybersecurity: how not to become a victim in the financial world] SBER Cyber Security. [↑](#footnote-ref-5)
6. Хакеры Черные шляпы, Белые шляпы и Серые шляпы – определение и описание. [Hackers. Black Hats, White Hats and Grey Hats – Definition and Description] URL: https://www.kaspersky.ru/resource-center/definitions/hacker-hat-types [↑](#footnote-ref-6)
7. «Назовите пароль от своей карты»: как защитить себя и ребёнка от кибермошенников? [Give me the password for your card”: how to protect yourself and your child from cyber fraudsters?] / Е. Полякова // Где мои дети. URL: https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov [↑](#footnote-ref-7)
8. От фишинга до вирусов: как мошенники обкрадывают российских геймеров [From phishing to viruses: how scammers rob Russian gamers] // Газета.ru. 06/07/2022. URL: https://www.gazeta.ru/tech/2022/07/06/15079700.shtml [↑](#footnote-ref-8)
9. Как защититься от кибермошенников — шесть основных схем обмана [How to protect yourself from cyber fraudsters - six main deception schemes] // РБК. URL: https://trends.rbc.ru/trends/industry/6027ef6c9a7947206e6aec96?from=copy y[ [↑](#footnote-ref-9)
10. Памятка УБК МВД России: актуальные способы совершения мошеннических действий. [Memo from the Department for Organizing Fight against Illegal Use of Information and Communication Technologies of the Ministry of Internal Affairs of Russia: current methods of committing fraudulent actions.] URL: [https://78.мвд.рф/citizens/ваша/security/item/45404472](https://78.мвд.рф/citizens/%D0%B2%D0%B0%D1%88%D0%B0/security/item/45404472) [↑](#footnote-ref-10)
11. Мошенники стали красть у россиян деньги с помощью их детей [Fraudsters begin to steal money from Russians with the help of their children] // Правмир. 23.10.2023. URL: https://www.pravmir.ru/moshenniki-stali-krast-u-rossiyan-dengi-s-pomoshhyu-ih-detej/ [↑](#footnote-ref-11)
12. Центробанк зафиксировал рост финансовых пирамид под видом онлайн-игр [The Central Bank records growth of financial pyramids under the guise of online games] // РБК, 24.07.2023. URL: https://www.rbc.ru/rbcfreenews/64be1dbf9a794745f0991516?from=copy [↑](#footnote-ref-12)
13. Финансовые пирамиды в России маскируются под онлайн-игры: как распознать мошенников [Financial pyramids in Russia disguised as online games: how to recognize scammers] // Mail.ru. URL: https://hi-tech.mail.ru/review/101527-finansovye-piramidy-pod-vidom-onlajn-igr/ [↑](#footnote-ref-13)
14. Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке [List of companies with identified signs of illegal activity in the financial market] // Банк России. URL: <https://cbr.ru/inside/warning-list/> [↑](#footnote-ref-14)
15. Что такое скам в криптовалюте [What is scam in crypto currency] // Banki.ru. URL: https://www.banki.ru/news/daytheme/?id=10979400 [↑](#footnote-ref-15)
16. Эксперты выявили автоматизированную скам-схему на $32 млн. [Experts identify an automated scam scheme worth $32 million] URL: https://forklog.com/news/eksperty-vyyavili-avtomatizirovannuyu-skam-shemu-na-32-mln [↑](#footnote-ref-16)
17. Как вас могут скамнуть в щитках? Все виды скама в DEFI в одной статье. [How can you get scammed in your shields? All types of scam in DEFI in one article] URL: <https://vc.ru/u/2548531-nikita-slimkobag/927300-kak-vas-mogut-skamnut-v-shchitkah-vse-vidy-skama-v-defi-v-odnoy-state> [↑](#footnote-ref-17)
18. Как уберечься от мошенничества при “накачке” и “сбросе” криптовалют [How to protect yourself from fraud when “pumping” and “dumping” cryptocurrencies] URL: https://bit.team/blog/ru/kak-uberechsya-ot-moshennichestva-pri-nakachke-i-sbrose-kriptovalyut/ [↑](#footnote-ref-18)
19. Мошенник не по своей воле. Как не стать соучастником киберпреступления [Fraudster against their will. How to avoid becoming an accomplice to a cybercrime] // Рамблер. URL: <https://finance.rambler.ru/money/52094791-moshennik-ne-po-svoey-vole-kak-ne-stat-souchastnikom-kiberprestupleniya/> [↑](#footnote-ref-19)
20. Прокурор разъясняет. Прокуратура Хабаровского края. [Prosecutor explains. Prosecutor's Office of the Khabarovsk Territory] 11.07.2023. URL: <https://epp.genproc.gov.ru/web/proc_27/activity/legal-education/explain?item=89000905>

Об ответственности владельцев денежных счетов (дропперов») в связи с использованием их в мошеннической схеме. Янтиковский муниципальный округ Чувашской Республики. [On the liability of owners of money accounts (money mules) in connection with their use in a fraudulent scheme. Yantikovsky municipal district of the Chuvash Republic] URL: <https://yantik.cap.ru/action/activity/pravoohraniteljnaya-deyateljnostj/prokuratura-yantikovskogo-rajona/prokuratura-razjyasnyaet/2023-god/ob-otvetstvennosti-vladeljcev-denezhnih-schetov-dr>

Дропперы: преступление и наказание. [Money mules. Crime and punishment] URL: <https://nefteyuganskij-r86.gosweb.gosuslugi.ru/netcat_files/userfiles/Finansovaya_gramotnost_/Info_materialy/Droppery_prestuplenie_i_nakazanie_.pdf>

Банки отбили более 20 млн попыток похитить деньги клиентов. [Banks fight off more than 20 million attempts to steal customer money] 31.01.2024 ЦБ РФ. URL: <https://cbr.ru/press/event/?id=18382> . [↑](#footnote-ref-20)
21. Дроппер поневоле: как не стать соучастником мошеннической схемы с банковскими картами [Money mule against their will: how not to become an accomplice in a fraudulent scheme with bank cards] // HSE.Daily. URL: https://economics.hse.ru/ecjourn/news/847434104.html [↑](#footnote-ref-21)
22. For more detailed information see: https://cloud.mail.ru/public/bfkn/2QSFPyEyJ [↑](#footnote-ref-22)
23. А если ребенок совершил мошенничество? Что ему за это будет? [What if a child commits fraud? What will happen to them for this?] // Я.Кью. URL: https://yandex.ru/q/article/a\_esli\_rebenok\_sovershil\_moshennichestvo\_41010554/ [↑](#footnote-ref-23)
24. Вымогатели начали использовать ИИ для подделки голосовых в Telegram Чем новая схема опасна для пользователей [Extortionists begin using AI to fake voices in Telegram. Why the new scheme is dangerous for users] // РБК. 10.01.2024. URL: https://www.rbc.ru/technology\_and\_media/10/01/2024/659d37899a79473f8a99e35f [↑](#footnote-ref-24)
25. Темная сторона искусственного интеллекта. Криминальные таланты нейросетей. [The dark side of artificial intelligence. Criminal talents of neural networks] URL: https://neuralinsight.ru/kriminalnye-talanty-nejrosetej/ [↑](#footnote-ref-25)
26. Как не стать жертвой кибермошенников: новые схемы обмана, портрет афериста и правила безопасности от воронежских экспертов. [How to avoid becoming a victim of cyber fraudsters: new deception schemes, portrait of a swindler and security rules from Voronezh experts] URL: https://www.vrn.kp.ru/daily/27586.5/4856275/ [↑](#footnote-ref-26)