**Recommendations for Working with Presentation of**

**Thematic Lesson Dedicated to:**

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

**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 transfer to fraudsters;

• use action algorithms in typical situations related to possible or already committed financial fraud;

• take precautions using different types of money and transactions with it; and

• be critical of proposals which show signs of pressure, manipulation, or fraudulent actions.

**To 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.

|  |  |
| --- | --- |
| **Slide (Slide Content)** | **Commentary for Teachers** |
| **Slide 1**  **NOT Child’s Play: How to Avoid Becoming a Participant in Financial Crimes**  **Thematic Lesson**  Изображение выглядит как текст, снимок экрана  Автоматически созданное описание | According to statistics, young people are increasingly becoming victims of scammers nowadays: taking advantage of the children and teenagers’ inexperience and gullibility, criminals steal money from their cards and their parents’ accounts. At the same time, the number of deceived victims – teenagers and children under 14 years old – is growing.  Phone calls, instant messengers, games, prizes, and even offers for part-time jobs are used to deceive. Such fraudulent methods can have several consequences: youths become victims of financial scams or become accomplices of them.  Therefore, the goal of our lesson is to explain such threats in real life, the Internet, social networks and instant messengers, teach youth to independently identify scammers by their distinctive features and take certain actions to avoid being involved in fraudulent activities. We will separately focus on fraudulent schemes using artificial intelligence. |
| **Slide 2**  **Situation**  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 (that’s how much she found) 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. | **Assignment:**  1. Study the situation described on the slide.  2. Think about what kind of fraud scheme was implemented here.  3. How much damage was caused and to whom was it caused – to the girl only or her family?  4. Guess why the schoolgirl believed the caller?  **Suggested Answers:**  This is an example of a telephone fraud scheme which targets minors.  Damage in monetary terms amounted to 50 thousand conventional units in cash plus the cost of the items given away.  The girl’s family suffered damage because the family’s property was given away.  The schoolgirl believed the caller since the scammers influenced girl’s feelings and emotions - as if something had happened to her family. In addition, the scammers asked not only for money, but also for things for the hospital, thereby they confirmed the situation they had invented.  In this case, scammers use social engineering techniques. **Social engineering** underlies all methods and types of cyber and telephone fraud: |
| **Slide 3**  **Social engineering:**  ...psychological manipulation of people to perform certain actions or disclose confidential information.  **Methods:**  • Deception or breach of trust  • Psychological pressure  • Manipulation  Изображение выглядит как текст, снимок экрана, дизайн  Автоматически созданное описание | **Social engineering is:**  ...psychological manipulation of people to perform certain actions or disclose confidential information.  The most vulnerable link in the fraudulent 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.  The behavior of a scammer and a victim are somewhat similar.  A fraudster has two goals: to deceive and to steal.  The 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 saying a relative is in danger. Someone is afraid of the police, and they call this person and introduce themselves as police officers.  Under the influence of social engineering, the victim voluntarily parts with money or reveals personal and financial data the attackers need to steal funds. |
| **Slide 4**  **Social Engineering Scheme**  **The emotions** the information from scammers evoke are of two types:  1) negative   * fear, panic * feeling of shame   2) positive   * joy, hope * desire to get money   Изображение выглядит как текст, снимок экрана, калькулятор  Автоматически созданное описание | ***How this method works:***  **Stage 1** - scammers influence basic emotions (fear, joy, sadness, surprise, curiosity, anger, trust, greed), including using topical issues. These feelings come to the fore in any stressful situation as a human defense mechanism when we hear some news unexpectedly.  The emotions the information from scammers evoke are of two types:  *1) negative*   * fear, panic * feeling of shame   **Assignment:**  Give an example of a phrase that a scammer might use to evoke a negative emotion.  **Suggested Answers:**  *“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   **Assignment:**  Give an example of a phrase that a scammer might use to evoke a positive emotion.  **Suggested Answers:**  *“You’ve won a large sum of money.”*  *“You are entitled to bonuses in the game.”*  **Stage 2 -** after activating basic emotions, scammers use certain **psychological techniques**, which are especially successful when they are used 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.  It is using this method that allows minors to be involved in financial fraud. |
| **Slide 5**  **Telephone and Mobile Scam**  **Who can a scammer pose as:**  • Bank security service, bank employees  • Law enforcement officer  • Relatives  • Friends  **Изображение выглядит как текст, снимок экрана, мультфильм  Автоматически созданное описание** | Let’s take a closer look at the forms of fraud that minors can fall into. The first and most common form is ***Telephone Scam***.  In this case, a telephone call is made to a potential victim (on a landline or mobile phone, including through instant messengers) and various manipulation techniques are used to obtain money, other property or personal data.  **Assignment:**  1. What are some examples of what scammers may pose as on the phone?  **Suggested Answers:**  *• Bank security service*  *• Bank employee*  *• Security Major*  *• Police captain*  *• Senior investigator*  *• Daughter, it’s me….*  *• This is your father’s friend….*  **Assignment:**  2. What are some examples of what scammers say on the phone posing as security service, law enforcement officers, family and friends?  **Suggested Answers:**  *“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...”*  *“Your relative has hit a man...”*  *“Using your fake documents, someone is trying to take out a loan for a large amount... We need to clarify its details...”*  *“You became a witness in a criminal case against your classmate...”*  If scammers pose as a relative / friend / acquaintances’ son, they usually say:  *“Our grandmother had an accident, she urgently needs medicine...”*  *“I 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.”* |
| **Slide 6**  **COMMON FRAUD ALGORITHMS**  **Signs it is a scammer who is calling you:**  • 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 you to 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 immediately go to scammers.  **Typical situations:**  BANK CARD IS BLOCKED  You received a call from the bank or received a message about blocking your bank card or unauthorized transactions with your account. Do not answer or call back. THESE ARE SCAMMERS. Contact the bank, the police or relatives.  WINNING THE LOTTERY  You have been informed that you have won a prize, but to receive it you need to pay taxes and transfer the sum of money to an account that is unfamiliar to you. DO NOT rush to follow the instructions! Check the information! It is quite possible that SCAMMERS are communicating with you.  CASES WITH RELATIVES  If they call you and inform you that your relative has been in an accident, behind bars, in hospital, or has had an accident, and now you need to pay bail, a fine, or a bribe for them - this is DECEPTION.  If you receive a call and report that your relative has been kidnapped and a ransom must be paid for him, call the police and this relative URGENTLY.  PAYMENT OF COMPENSATION  You have had a call or received an SMS with an offer to receive compensation for insurance, medical care, utilities and other services, but you need to transfer a certain amount as a commission for this. Be careful, this is most likely SCAM.  MONEY TRANSFER  If you are asked to provide 3 digits from the back of the card (CVV code) to transfer funds to your bank card, you have encountered fraud. Do not tell anyone the three-digit card authentication code, as well as the password for debiting funds.  Изображение выглядит как текст, снимок экрана  Автоматически созданное описание | In schemes with employees of banks and law enforcement agencies, attackers offer to solve the problem in the following way and offer this to their victim:  • Withdraw all money from the bank cards of the victim or their parents 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 office, department and from another number.  In schemes involving relatives and friends, 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 send them the card details, tell them the PIN code, 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. |
| **Slide 7**  **Fraud Algorithms**  **Situation:**  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 it, but he would need boy’s passport and his or his parents’ bank card photos for this.  Изображение выглядит как текст, снимок экрана  Автоматически созданное описание | **Assignment:**   1. Study the situation described on the slide. 2. What was the scammer’s goal? 3. At what point do you think it became clear that the scammer was talking to the boy?   **Suggested Answers:**  Scammers steal bank card details without the participation of couriers or cash. Having received the card data (number, CVV), they can independently carry out small financial transactions without the participation of the victim.  The boy should have stopped the conversation the moment he was asked to send his personal information.  The signs that a scammer called or wrote may include the following:   * You are required to take immediate action. * They rush and intimidate, put pressure on emotions, offer rewards. * They require that you provide confidential information: card details, PIN code or one-time password from the SMS message. * Call late in the evening, at night or early in the morning at weekends. * If you refuse to give your details, they threaten that the money from your card will go to the scammers immediately. |
| **Slide 8**  **Cybercrime and Cyber Fraud**  **Cybercrime** is any illegal act that violates human rights and freedoms through computer systems and networks.  Изображение выглядит как текст, снимок экрана  Автоматически созданное описание | 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, fraudsters) have also intensified their activities on the Internet.  Researchers define cybercrime as any illegal act that violates human rights and freedoms through computer systems and networks.  Cyber fraud is one of the types of cybercrime, whose purpose 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, which we will discuss later. |
| **Side 9**  **Phishing**  ... a type of fraud in which attackers send emails and try to deceive recipients into doing various things.  The final goal is to gain access to the finances or personal data of defrauded users.  Изображение выглядит как текст, обувь, человек, одежда  Автоматически созданное описание | **Phishing**  ... a type of fraud in which attackers send emails and try to deceive recipients into doing various things:   * follow a malicious link; * download an infected attachment; and * provide personal data and other confidential information.   The final goal is most often to gain access to the finances or personal data of defrauded users. |
| **Slide 10**  **A phishing email** is an email that contains a malicious **attachment, a link** to a fraudulent **site**, or malicious software.  **Subjects and authors of letters:**   * Delivery services * Marketplaces * Cryptocurrency * Breaking news * Lotteries * Additional income and investments * Tour operators and holidays * Event tickets * Subscriptions and online services * Photos from the party   Изображение выглядит как текст, снимок экрана, дизайн  Автоматически созданное описание | ***A phishing email*** is an email that 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.  What tricks do scammers use in such letters:   * Delivery services * Marketplaces * Cryptocurrency * Breaking news * Lotteries * Additional income and investments * Tour operators and holidays * Event tickets * Subscriptions and online services   These letters may look like messages from completely respectable sources: online stores, banks, services, etc.  However, these are criminals; they 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 other children to register on special websites 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. |
| **Slide 11**  **Fake Websites and Apps**  **Fraud**  **SIGNS OF A POTENTIALLY DANGEROUS ONLINE STORE**  **LOW PRICE**  The price in a scammers’ store is often significantly lower than in others. You should not succumb to the sales promotion offers, the words “limited quantity”, “hurry to buy”.  **NO COURIER DELIVERY**  In this case, you often have to make an advance payment for the services of the transport company. Malefactors can provide fake receipts for payment for goods.  **NO CONTACT INFORMATION ABOUT THE SELLER**  If the website contains only a feedback form and the seller’s mobile phone number, such a store may pose a danger. Before buying here, you should read reviews on the Internet.  **CONFIRMATION OF THE SELLER’S IDENTITY BY PROVIDING THE BUYER WITH A PASSPORT SCAN**  It is easy to forge a document, especially a scanned one.  **INACCURACIES AND INCONSISTENCES IN THE PRODUCT DESCRIPTION**  It is a good idea to read the description of the same product on other websites.  **NO SELLER OR STORE HISTORY**  Pages registered a couple of days ago are potentially dangerous.  Изображение выглядит как текст, одежда, мультфильм, снимок экрана  Автоматически созданное описание | The method of cyber fraud in various areas of business aimed at appropriating funds is called **fraud[[1]](#footnote-1)**.  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 payment, the credit card details are transferred to the attackers, which the user is not even aware of.  Fraudsters have also learned to fake, for example, bank websites in order to find out customer data from their personal account. |
| **Slide 12**  **EXAMPLE**  **Scam in online games**  Scenario  1/4 you receive an email that you have “won” a prize in a game  2/4 you click on the link to exchange with a special bot  3/4 you enter your account on a fake website  4/4 you give your account details to scammers  Изображение выглядит как текст, снимок экрана, Шрифт, дизайн  Автоматически созданное описание | Recently, online (multiplayer) games, in which 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.  Fraudsters may ask for your account login and password by deceptive means and offer a “good buy” that is difficult to turn down.  Phishing gaming resources are also created to steal accounts from gamers and then extort money in exchange for returning access.  A substantial bonus in the form of a large amount 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. |
| **Slide 13**  **Fraud on Social Networks and Instant Messengers**  o Correspondence with scammers (social engineering)  o Account hacking  o Digital cloning  o Voting  o Quick earnings  o Online pyramids  o Online marketing fraudsters  Изображение выглядит как текст, снимок экрана, Графика, интернет  Автоматически созданное описание | Fraud using instant messengers and social networks has been increasingly gaining momentum recently.  It is implemented in various forms:   * + Correspondence with scammers (social engineering).   + Account hacking   + Digital cloning   + Voting   + Quick earnings   + Online pyramids   + Online marketing fraudsters   Fraud on social networks and instant messengers is often similar to the telephone one, 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 bank card fraud, that is, obtaining card details. |
| **Slide 14**  **Situation**  *An unknown person contacted the teenager on Telegram 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 photo of the screen to receive the reward. Then the teenager acted on the instructions of the fraudulent blogger 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.* | **Assignment:**   1. Study the situation described on the slide. 2. At what point do you think it became clear that a scammer was corresponding with the boy? 3. Why did the scammers ask the boy to take a photo of his parents’ phone screen?   **Suggested Answers:**  It became clear that this was a scammer when the blogger, firstly, wrote on Telegram themselves - this is a suspicious action; and then, when the fraudster asked to take certain actions related to someone else’s property or data.  The scammers needed the screen photo to see what applications were installed on the phone and to find out the application of which bank the boy’s mother was using. Thus, the scammers understood which remote access application could be installed, dictated what to do, and were able to steal the money.  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. “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. |
| **Slide 15**  **Situation**  *Unknown persons created a telegram channel for fans of the online shooter 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.* | Let’s look at an example where scammers came up with a scam based on a popular mobile game.  **Assignment:**   1. Study the situation described on the slide. 2. What are the signs that this scheme is fraudulent?   **Suggested Answers:**  In this case, scammers catch the player in the game by offering in-game currency, graphic designs (skins), items, and placing bets on tournaments. **Communication takes place in the messenger and is not conducted through an official resource (website, game chat, etc.), which is the first suspicious sign.**  Next, 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. |
| **Slide 16**  **Situation**  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 his card, and the girl stops responding to messages and calls and deletes her account.  *Изображение выглядит как текст, снимок экрана, логотип, дизайн  Автоматически созданное описание* | **Assignment:**   1. Study the situation described on the slide. 2. What fraudulent scheme is described here? 3. What are the signs that the described scheme is fraudulent? 4. What is the scammer’s goal?   **Suggested Answers:**  This example examines a deception scheme when dating online - this is another type of cyber fraud with young people.  Fraud should be suspected when strange offers appear. First of all, financial in nature.  The main goal of scammers operating under this scheme is to obtain personal data of a potential victim and access to their accounts.  A simpler example can be given: 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 - a phishing scheme works here. The victim loses all the money from the card. |
| **Slide 17**  **Situation**  *In early October, a 14-year-old girl received a message on a social network from her 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.* | **Assignment:**   1. Study the situation described on the slide. 2. What fraudulent scheme is described here? 3. What actions did the fraudster perform to be believed?   **Suggested Answers:**  This example is **using or taking over a fake social network account.**  Fraudsters hack other people’s accounts and create digital doubles of some familiar faces or other people.  Children and teenagers often 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.” |
| In addition to the situations we have considered, scammers from fake accounts **gain trust and establish contact**, sometimes by faking the pages of adults the child knows.  While communicating on social networks, 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, thereby quietly obtaining the necessary information.  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. |
| **Slide 18**  **PHISHING**   * *Will you vote for me, please, if it’s no bother for you, of course?* * *Of course, I will and what is it?* * *A contest I took part in.* * *The link is suspicious.* * *I won’t follow the link, sorry.* * *You are a bad friend.*   Изображение выглядит как текст, снимок экрана, Бренд, Шрифт  Автоматически созданное описание | Moreover, messages often come from a friend or acquaintance with various requests: to vote, like, lend money, buy a ticket, etc.  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. |
| **Slide 19**  **Fraudulent Schemes to Make Quick Money**   * investments in profitable projects * views of videos from popular bloggers * rating pictures and hotels * voting in rankings * bookmaker bets * online economic games   THERE IS ALWAYS FREE CHEESE IN A MOUSETRAP  **Изображение выглядит как текст, снимок экрана, логотип, Шрифт  Автоматически созданное описание** | People are constantly offered to make quick money or invest money in supposedly profitable projects on the Internet or instant messengers. Popular schemes for children and teenagers include money for watching videos from popular bloggers, rating pictures and hotels, and voting in rankings.  Advertising for quick money, as a rule, promises high income with minimal waste of time.  Criminals advertise to older teenagers how to make quick money using bookmaker bets on their resources.  **Assignment**  Think about what scheme the scammer offers the victim to make the latter lose money or personal data?  **Suggested Answers:**  - Before starting the “work,” **the scammer sends a link and asks to enter the bank card details** (your own or your 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 you need to pay the tax in advance. After entering the data, all funds from the victim’s or their parents’ account are debited.  - Fraudsters convince people **to pay for current expenses (for example, drawing up questionnaires, taxes) or pay for some services**.  - Fraudsters show supposedly successful projects in which you can invest money or place bets. Teenagers are asked **to pay a commission** to withdraw supposed earnings. As a result, the money, along with the card data, ends up in the hands of cybercriminals.  - Fraudsters, showing fictitious profit charts, convince the victim **to transfer as much money as possible** for profitable investment. |
| **Slide 20**  **You Pay, You Win Scam**  Financial Pyramid  **Signs:**   * Lack of gameplay * Paying money for attracting new participants * Complex income calculation scheme * Guarantee of high income without any risk and aggressive advertising on social networks   *Изображение выглядит как текст, снимок экрана, дизайн  Автоматически созданное описание* | Financial pyramids have appeared online under the guise of new business games.  A feature of such projects is the absence of a competitive element.  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 the advertising of a game is very aggressive, promises to earn money without risk, then most likely this is a fraudulent scheme. |
| **Slide 21**  **Cryptocurrency and ICO Fraud Scheme**   * Scam projects (scam) * Dummy projects * Rug n Pull * Pump and dump * Classic phishing   Изображение выглядит как текст, снимок экрана, мультфильм  Автоматически созданное описание | 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 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[[2]](#footnote-2)**. 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[[3]](#footnote-3).  The third scheme of cryptocurrency scammers is **pump and dump)**[[4]](#footnote-4)- 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[[5]](#footnote-5).  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. |
| Slide 22Children are Accomplices of Financial FraudstersИзображение выглядит как текст, снимок экрана, графический дизайн, Шрифт  Автоматически созданное описание | 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 a 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 to act as intermediaries or couriers in the transfer or withdrawal of money earned illegally for a percentage or fee.  In such cases, children and adolescents become accomplices or accomplices in committing a crime.  . |
| Slide 23 **Complicity in Fraud - Providing Courier Services**  **Situation**  *An 81-year-old pensioner contacted the police after a 17-year-old teenager took 100 thousand conventional units from her.*  *The grandmother thought she was helping her granddaughter, who allegedly got into an accident and asked for money over 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 and receiving a percentage of the money transferred. The young man agreed, sent his passport details to the “employer” and became a courier.*  *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.* | Fraudsters offer a child or teenager by phone or on a social network to provide courier services: personally collect money from one person and transfer it to the bank account of another and keep a percentage of the money for the work done for themselves. In the messenger, minors receive clear instructions from scammers on how to behave with the people whom they take money from and how to transfer funds.  **Assignment:**   1. Study the situation described on the slide. 2. What fraudulent scheme was implemented here? 3. When did it become clear that the teenager had become an accomplice in the crime? 4. Do you think there is any punishment for such teenager’s actions?   **Suggested Answers:**  First, scammers fraudulently extort money from citizens by telling stories about the need to help a close relative in trouble. Deceived citizens **transfer money** **to** underage **couriers**.  The courier transfers the remaining amount to the bank card of the criminals for a reward and **becomes an accomplice in committing the crime**.  In addition, he involves his friend in such schemes.  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**.  Scammers who hire minors as couriers entrust them with the dirtiest job - collecting money. |
| Slide 24 **Complicity in Fraud – Money Mules**  **Money mules** are people who help cash out and withdraw money after criminals commit a financial crime.  **Situation:**  *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.”*  **Important!**  People who respond to such advertisements often become participants in fraudulent schemes.  Изображение выглядит как текст, снимок экрана, Шрифт  Автоматически созданное описание | The next fraudulent financial scheme is the one of illegal cash withdrawals and nominee directors.  These schemes use, among other things, **money mules** - people who help cash out and withdraw money after criminals commit a financial crime.  Most often, money mules do not even suspect that they are part of a large criminal puzzle.  **Assignment:**   1. Consider the example of recruiting a money mule on the slide. 2. What are the suspicious signs in this ad which may indicate that the scheme is fraudulent? 3. Who will be the money mules in this case? 4. What work duties do you think a teenager should perform in such a job? 5. What is the scammers’ goal when they hire money mules?   **Suggested Answers:**  What is suspicious in this case? The advertisement contains no requirements for the candidate, only the availability of a bank card. No documents are required for employment. The promise of quick and big earnings.  The teenager who responds will be a money mule. 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**. Money mules are not the initiators of the crime, but they carry out instructions and receive money for it.  Fraudsters transfer the stolen funds to the teenager’s cards, and then the teenagers transfer the funds to another person along the chain. In addition, teenagers are asked to cash out the money received on the card at various ATMs and take a small percentage for themselves.  Thus, criminals make it difficult for law enforcement to find funds and final recipients. |
| Slide 25Money Mules Recruitment SchemesAdvertisements on the Internet, social networks and instant messengers about quick earnings, part-time job related to money transfers, cash withdrawals, and work in the IT field.Calls under the guise of law enforcement agencies about work or to help in catching criminals.Accidentally transferring money to a card with a request to return.Изображение выглядит как текст, снимок экрана, Шрифт, Графика  Автоматически созданное описание | There are different schemes for recruiting money mules by scammers, for example:   1. scammers place advertisements in the streets and on the Internet, including on social networks, offering work related to the money transfer and cashing; 2. scammers post advertisements on telegram channels and social networks about interesting jobs in the IT field with rapid growth in earnings; 3. when posting job advertisements, scammers create (fake) phishing 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, the 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; and 5. under the guise of a mistaken person, scammers “accidentally” transfer money to a bank account, and then ask for it to be returned in cash or transferred to a card. |
| **Slide 26**  **Types of Money Mules**  - *complicit*, aware of the criminal scheme   * act voluntarily and intentionally   - *duped*, unaware of the criminal scheme   * act unconsciously, unintentionally and/or under the influence of fraudsters   Изображение выглядит как текст, снимок экрана, Реклама в Интернете, дизайн  Автоматически созданное описание | 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”.  The first type of dummy includes people who are aware of the criminal component of their activities and act voluntarily and intentionally.  The second type includes 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 law. |
| **Slide 27**  **Consequences of Money Mules’ Actions**   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 for years. 7. Money mules create a negative financial rating for themselves and undermine their reputation.   Изображение выглядит как текст, снимок экрана, Шрифт, число  Автоматически созданное описание | Attackers strive to make it as difficult as possible for law enforcement agencies to identify and track funds passing through cash-out chains.  The 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 it is even very difficult to identify them, **but almost all money mules are caught**.  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. |
| **Slide 28**  **MONEY MULES LIABILITY**  Fine  Confinement  Изображение выглядит как текст, логотип, снимок экрана, Шрифт  Автоматически созданное описание | The money mules’ actions are penal.  **Assignment**:   1. Think about what types of crimes the money mules’ actions are similar to? 2. Think about how severely a money mule can be punished? Can a money mule go to jail?   **Suggested Answers:**  The money mule’s actions may be classified as fraud, legalization (laundering) of funds obtained by criminal means, or illegal circulation of means of payment.  If the actions are classified as such, they will be punished not only with a large fine (from 100 thousand conventional units) but will also be confined for a long term (on average 6-7 years, up to 10 years depending on the severity of the crime committed).  The victim of fraud must be compensated.  And from the age of 14, teenagers must do this: 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, their parents or foster parents are obliged to help them.  Also, the data on the offense will be sent to the Commission on Minors’ Affairs and the Protection of Their Rights. |
| **Slide 29**  **Using Artificial Intelligence for Financial Crimes**   1. false documents 2. fake pictures and illustrations 3. fake news and newsletters 4. phishing, fraudulent websites 5. social bots and social media manipulation 6. conversation (telephone and correspondence) 7. “clone” of a person (deepfake) 8. fake voice messages 9. fake registration in ChatGPT   Изображение выглядит как текст, Человеческое лицо, одежда, снимок экрана  Автоматически созданное описание | 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.  **Assignment:**   1. Consider the main scammers’ strategies using artificial intelligence presented on the slide. 2. Explain how AI is used in each of these strategies.   **Suggested Answers:**  Attackers 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 that are difficult to detect.   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.   1. Attackers can use a fraud scheme related to false registration in ChatGPT through phishing sites or applications disguised as services for selling accounts in the ChatGPT neural network for little money. They take advantage of this chatbot being banned in a number of countries, and many young people trying to gain access to it at any cost. 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. |
| **Slide 30**  **Situation**  *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.* | Criminals often use artificial intelligence to fake voice messages in instant messengers in order to steal money and accounts.  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.  **Assignment:**   1. Think about why such a fraudulent scheme is more dangerous than a traditional one. 2. Think about what simplest action will help you avoid becoming a scammer’s victim.     **Suggested Answers:**  This scheme is dangerous because scammers use **several factors to identify the victim** - account, voice and bank card. The required audio file cutting is generated, and a fake voice message is created with the help of AI. The required document is generated based on stolen personal data using AI.  The easiest way to avoid falling for such a trick is to double-check whether the account owner is really making such a request, for example, by calling them back on the phone. |
| **Slide 31**  **Ways to Protect Yourself from Financial Fraud**  **Изображение выглядит как текст, снимок экрана, компьютер  Автоматически созданное описание** | We’ve looked at 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. |
| **Slide 32**  **General Protection Rules**   1. Critical perception of any situation. 2. A stranger dictates the course of action - this is definitely a deception. 3. Promises of quick profits are always a warning sign. 4. Clicking on unfamiliar and unverified links can lead to fraud and loss of money. 5. You must not tell personal information to strangers. 6. If you have any doubts, you should always ask your family and friends for advice. 7. Call the police.     Изображение выглядит как текст, снимок экрана, Шрифт, логотип  Автоматически созданное описание | Any situation must be approached **with a critical perception**. It is recommended to view with a dose of skepticism all calls and messages 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. |
| **Slide 33**  **Rules for Protecting against Scammers when Making Phone Calls**   * Do not answer or call back unknown or dubious numbers. * It is MANDATORY to call your family or friends/bank/organization/police yourself and ask them for help. * Stop the conversation if it concerns financial issues. * **NEVER** give **ANY** bank card details or confirmation codes from SMS messages to anyone in a conversation**.**   Изображение выглядит как текст, снимок экрана, графический дизайн, дизайн  Автоматически созданное описание | 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 Central Bank and Rosfinmonitoring (Federal Financial Monitoring Service of the Russian Federation) 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. |
| **Slide 34**  **Action Rules with Bank Cards and Payment Transactions**   * NEVER tell anyone or photograph ANY bank card information or confirmation codes from SMS messages. * Block the card if it is lost or you receive a notification about a transaction performed without you. * Do not trust suspicious SMS messages from unknown numbers about the card. * Pay for purchases only through official websites of stores and platforms. You cannot pay for purchases through transfers. * Do not give strangers a mobile phone with installed banking applications. * It is MANDATORY to call your family/bank/organization/police yourself and ask them for help.   Изображение выглядит как текст, снимок экрана, одежда, Человеческое лицо  Автоматически созданное описание | 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. |
| **Slide 35**  **Action Rules on the Internet and** **in Correspondence to Protect against Phishing and Cyber Fraud**   * Do not believe information about winnings and easy money. * Do not install unknown applications, especially at the request of strangers. * Do not follow unknown or strange links. * Check official sources with received information, letters, etc. * Disclose **no** personal information to anyone in correspondence. * Do not enter personal data on suspicious sites and applications. * Always check the information you receive with a real friend and family member (**it’s better to call**).     Изображение выглядит как текст, Человеческое лицо, снимок экрана, мультфильм  Автоматически созданное описание | 1. You should not believe the 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.   1. 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. 2. 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.). 3. Study the subject of the letter or message, the content of the letter and the names of the files. Pay attention to proper writing. If the message encourages you to take immediate action, this is a suspicious sign. 4. 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. 5. Be careful with attachments to letters or messages. Open only the attachments that you have been waiting for. Check the attachment extension. 6. **Never** communicate confirmation codes from SMS messages **to anyone** in correspondence. 7. If a letter or message requires that you enter data (login, password) on suspicious websites or in questionnaire forms, you must delete this letter. 8. 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. 9. You must not share information about the home, school, place of work of parents’ address, what applications family members have on their phones, any passwords and PIN codes with anyone. 10. 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. 11. 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. |
| **Slide 36**  **Protecting Accounts and Hardware**   * Enable two-factor authentication. * Set a complex password. * Block access to your profile for strangers. * Update antivirus software.   **Изображение выглядит как текст, снимок экрана, логотип, Шрифт  Автоматически созданное описание** | 1. You need to protect your accounts – it is necessary to enable two-factor authentication wherever possible. 2. 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, as 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 anywhere. 3. 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. 4. It is important to use antivirus software and update it regularly to protect your computer from malware. |
| **Slide 37**  **Rules for Online Shopping**   1. Check the online store. 2. Do not communicate with the seller in instant messengers. 3. Pay for purchases only through official stores, platforms, etc. 4. Consult with family and friends.   **Изображение выглядит как текст, снимок экрана, еда  Автоматически созданное описание** | 1. 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 seller’s reliability. 2. It is dangerous to purchase virtual money, game improvements, as well as paid game content and other bonuses. This should only be done on the official platform or game by paying through that platform. 3. A sign of a scammer is an offer to communicate in the messenger, and not through the official websites of stores or online trading platforms. 4. It is necessary to check the seller rating 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. |
| **Slide 38**  **Action Rules on the Internet against AI-Related Threats**   * Do not enter financial information in chatbots. * Check the information received with a real person, it’s better to call them. * Check data on official resources. * Ask random questions.   **Изображение выглядит как текст, снимок экрана, человек, графический дизайн  Автоматически созданное описание** | 1. 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. 2. 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 which ask you to enter payment information, and do not install unknown applications on your devices. 3. 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. 4. Use neural networks to recognize fakes. |
| **Slide 39-40**  **INTERNATIONAL OPYMPIAD IN FINANCIAL SECURITY**  **IT IS YOU WE ARE WAITING FOR!**  **Aims of the Olympiad include:**   * increasing general information, financial and legal awareness of the youth, forming a new form of thinking and new format of activities, discovering talented school students and students in financial security; * creating conditions for individual learning trajectory, assisting in carrier guidance for school students and students to form staff resources in financial security system; and * encouraging school students and students’ scientific and educational and research activities, developing scientific knowledge in financial security.     **Изображение выглядит как текст, снимок экрана, Шрифт, дизайн  Автоматически созданное описание** | Bringing to the students’ attention the opportunity to take part in the International Olympiad in Financial Security. |

1. https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov [↑](#footnote-ref-1)
2. Что такое скам в криптовалюте [What is scam in cryptocurrency]// Banki.ru. URL: https://www.banki.ru/news/daytheme/?id=10979400 https://www.banki.ru/news/daytheme/?id=10979400 [↑](#footnote-ref-2)
3. 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-3)
4. 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-4)
5. 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-5)