**Federal State Autonomous Institution of Higher Education**
**Peoples' Friendship University of Russia**
**(RUDN University)**

# Guidelines
## for preparation and conduct of a thematic lesson on the topic
## *Financial Security of the Individual on the Internet*

Moscow, 2023

**Abstract**

The Guidelines have been designed to provide the teachers of basic general, secondary (complete) general and additional education with methodological assistance in organizing and conducting a thematic lesson on the Basics of Financial Security on the Internet. The guidelines offer conceptual, substantive, methodological and technological recommendations for conducting a lesson.

The Guidelines cover a set of issues related to the lesson. The proposed materials are advisory in nature. Thus, while conducting a lesson the teacher can also rely on their own experience, take into account age characteristics of the students, their training level, as well as traditions of the region.

**Explanatory note**

Financial education of young people contributes to making competent decisions, minimizes risks and, thus, can strengthen the financial security of the population. A low level of financial literacy can not only lead to bankruptcy, but also to poor retirement planning, vulnerability to financial fraud, excessive debt, and social problems, including depression and other personal problems.

*The goal* of the lesson is to develop the students' financial literacy and acquaint them with basic rules of financial security on the Internet.

*Tasks* **:**

- ✓ to convince the students that financial literacy and financial security both personal (family) and state are the basis of financial well-being;
- ✓ to get the students acquainted with the patterns of competent financial behavior on the Internet, to form the basic financial concepts, to work out an algorithm for solving difficult life situations fraught with the danger of falling victim of leakage of personal, and specifically biometric, data;
- ✓ to give the students a general idea of financial risks in the current economic situation; to enhance awareness of the systemic correlation between personal financial security and financial security of the state; to make the students aware of the danger of financial crimes for the state and citizens.

Against the background of digitalization of all the spheres of our life, young people are becoming active users of financial services on the Internet. Thus, every third teenager uses a non-cash payment method, and every second makes purchases via a smartphone.

A relatively high level of digital literacy [1] and smartphones allow teenagers to use mobile and Internet banking (56% and 38%, respectively).

Despite the fact that cash remains the most common payment method for teenagers (42%), a large proportion of them make purchases non- cash (32%). Nearly half of teenagers (43%) make contactless payments via their smartphones.

According to statistics from the National Financial Research Agency (NAFI) [2], only 10% of the population in Russia demonstrate a consistently high level of financial literacy. Notably, the most financially literate people in Russia are men and women aged 40-49 with higher education, as well as major cities residents.

Every second young person (53%) believes that they lack knowledge of financial security: 48% of respondents admit they have some knowledge in this area, but it is not enough to protect them from fraud, and 5% say that they have no knowledge about the safe dealing with finances at all. Teenagers aged 14 to 17 are more often unsure of their knowledge (53%).

---

[1] The level of digital literacy of teenagers is 73% out of 100, for comparison, the adult index is 52%.

[2] Data from the portal My Finances. https://xn--80apaohbc3aw9e.xn--p1ai/article/finansovaya-gramotnost-rossiyan-vyrosla-za-poslednie-4-goda/ (date of access: 01/19/2023 ).

A number of misbelieves in terms of financial security are common among the Russian youth [3].

First of all, it is an erroneous perception of the reliability of cryptocurrency as an investment tool: 65% of young people are not aware of the high risks of digital currency and believe that investing in it is a reliable way to protect money from inflation. This position is more characteristic of young residents of major cities (49%) and respondents aged 18 to 24 (46%).

Almost two-thirds of young people (60% of respondents) are mistakenly convinced that there are many simple ways to increase capital. Thus, the lack of understanding of the ratio of risk and profitability of financial instruments creates the prerequisites for the massive involvement of young people in highly profitable and often illegal investment schemes fraught with high risks.

Young people also neglect personal data protection when making online payments. More than half of young citizens (59%) do not pay due attention to their personal data safety when making purchases on the Internet. Mature young people (aged 25 to 35) state it more often than others (57% among the respondents).

In the modern world, biometric data are becoming the main means of identifying a person when making financial transactions on the Internet. According to the results of the Visa payment system study, the Russians tend to trust the banks and payment systems more than social networks, mobile phone manufacturers and mobile operators (48% of respondents have trust in them to store their biometric data).

Respondents give the greatest preference for biometrics to a fingerprint (92% of respondents), 17% of respondents use the face in identification, 12% use the voice. At the same time, the Russians are less tolerant to passwords and pin codes. However, 51% of respondents have multiple passwords for their accounts. At the same time, one in ten respondents uses only one password to log into all accounts. According to Visa, it is the difficulty in remembering that pushes Russians to use the same password for different accounts, thereby increasing the risk of being hacked by fraudsters. Identification by biometrics eliminates the need to remember many passwords and pin codes. According to 47% of respondents, it is its main advantage.

Everyone can face fraud when consuming financial services and personal data leakage when making online purchases. Most of these incidents can be avoided by applying the rules and precautions in this area, grouped under the heading "financial security".

Recently, financial losses have often occurred at all levels, affecting both the macroeconomy (nationwide, national) and individual citizens. The financial security of an individual depends both on the level of financial and, more broadly, economic security of the state, and on the financial decisions made by a citizen himself/herself, that is, the level of one's awareness of financial literacy in general, and financial security in particular.

The lesson is aimed at developing the financial culture of students, educating them to understand the importance of acquiring basic knowledge and skills to ensure personal financial security and its relationship with the financial security of the state.

The lesson's goal is to answer a number of questions:

- how to protect the rights of a financial services consumer
- how to protect personal data from leakage
- how to protect oneself from intruders in social networks and online games.

Designing the lesson, the teacher is recommended to use information videos, comics, and brochures on financial security.

Students can be invited to study cases, analyze statistical data and theoretical materials on the topic of personal financial security on the Internet, discuss the topics proposed by the teacher, share their opinion and experience concerning situations which require knowledge of financial security rules.

While preparing for the lesson, teachers can use the materials from the media library of the International Educational and Methodological Center for Financial Monitoring (

[3] A representative youth survey was conducted in June 2022 using the Tet - o- Tvet -M online panel. 1,000 people aged 14 to 35 were interviewed. https://nafi.ru/analytics/kazhdyy-vtoroy-predstavitel-molodezhi-schitaet-chto-emu-nedostatochno-znaniy-o-finansovoy-bezopasnos/ (date of access: 01/19/2023).

https://mumcfm.ru/mediateka ), the educational service of the Research Financial Institute of the Ministry of Finance of the Russian Federation ( moifinansy.rf ).

**Specifics of educational activities organisation**

To achieve the pedagogical goals of the lesson it is important to ensure that frontal, group and individual work should complement each other. In organizing the educational activities, the teacher should also take into account the age and educational capabilities of students.

**Main points of the lesson**

Modern society has been rapidly developing in all areas, including finance, which today incorporates all the latest achievements of scientific progress. In this situation, the main thing is not just to teach students to act according to an algorithm (which is also very important when addressing certain financial problems), but to form their competence to navigate the financial space, evaluate various alternatives for solving financial problems and make the best decision in specific life circumstances.

The results of a study by the International Training and Methodological Center for Financial Monitoring (ITMCFM) [4] showed that young people are most interested in the aspects of financial security related to their personal rights protection in the financial sector (78%), information security of an individual in the financial sector (67%) and security of biometric personal data (73%).

In our society at the modern "information" stage of its development, information is the most significant resource and the information field is the main habitat of modern man.

Various types of *data* are at the heart of all available services, which help us, among other things, manage our financial assets and carry out financial transactions. *Personal data* are directly related to us.

The Internet stores countless numbers of our personal data, which form the so-called "digital profile" of a person. It is a set of all the traces of existence that we leave in the digital world. Over time, such traces get increased: new gadgets are being introduced (for example, smart watches for health monitoring), technologies for tracking location and communication, digital identification of a person.

By adding new data to the already familiar photos, passwords, search history in the Internet browser, areas of interest, we get a digitalized profile of a person. The analysis of a large amount of data about a person (or digital personality analysis) makes it possible to judge their intellectual level, competencies, capabilities, and prospects.

Despite the fact that digital technologies simplify our lives in many ways, they also create many threats. Uncontrolled collection of information about a person creates a number of dangers from harmless but annoying spam calls to manipulation of opinion, consciousness, theft of their "digital identity" and money.

*What is "personal data"?*

*Personal data* is any information relating directly or indirectly to a specific or identifiable person (personal data subject), that is any information that directly or indirectly points to or is somehow related to a person.

There are several *types of personal data:*

a) general: first name, last name, patronymic, passport details, date and place of birth, registration addresses and places of residence;

b) special categories of personal data, which include nationality, political, religious or philosophical views and believes, information about the state of health, intimate life, criminal record;

c) publicly available personal data authorized by a person for distribution (e.g. information that one provides to an unlimited number of people through social networks);

d) biometric personal data: fingerprints, iris pattern, palm vein pattern, DNA code, voice cast;

e) depersonalized: data by which it is impossible to identify a person without additional data (Table with identifier values).

**SECTION I. Digital identity profile and biometric personal data**

[4] A representative youth survey was conducted in partnership with ITMCFM in September 2022. 1,000 people aged 14 to 35 were interviewed. https://nafi.ru/analytics/finansovaya-bezopasnost-chemu-i-kak-obuchat-molodezh-/ (date of access: 01/09/2023).

Today algorithms know much more about a person than their own parents. They have at their disposal not just information about something specific, but a whole layer of data that opens the possibility of creating a specific personality in the digital world, an analogue of a living person.

The concept of a digital identity has been firmly established in everyday life, and we distinguish it from the concept "profile" in social networks. If the first definition is mostly used in the scientific world, in development, the second one is familiar to everyone. In this vein, the issues of financial security of a digital person should be considered.

*How does digital identity theft occur?*

After the transition of many areas of human activity to the Internet, the digital identity has also acquired a price. It has become a commodity with its own characteristics, value and cost. It does not only refer to taking possession of a password or access rights.

Digital personality analysis is at the heart of all modern marketing. They are willing to pay for information about a person's preferences, lifestyle and needs. Moreover, the more companies are willing to invest, the more data they get at their disposal. This is what makes "smart feeds" work. Targeted ad impressions, tracking the flow of people during advertising do not surprise anyone, but one also does not fully know how far this analysis extends.

Even an adult, not to mention a teenager, is not able to give their informed consent to something that they do not fully understand, while a digital person can easily become the object of illegal actions. Such phenomena as the abduction of a digital identity are already not uncommon in modern reality. If a company works with the financial management of individuals and businesses, a large number of people are concerned about what it does with the information about their financial assets, investment goals, risk appetite, etc.

Another example. At the beginning of 2019, it was found out that the Genesis marketplace sold more than 60 thousand stolen digital identities, and there was a special browser with a built-in human digital trace generator.

*What information is stolen?*

Digital identity theft: *photos, videos from one's pages on social networks, accounts and profiles, passport data and copies of documents, selfies with documents, photos of bank cards* – can be committed for various purposes, i.e. from the banal sale of information to blackmail and use in fraudulent schemes. The simplest example is the use of phone numbers, names, personal information and voices to deceive and scam.

*Why do they steal a digital identity?*

Access to someone's account opens up a wide range of opportunities. One can read correspondence and hold it on behalf of the owner, one can follow them, look for confidential information, publish content on their behalf, ask for money transfers, distribute spam, use it to promote advertising groups. All these things are the threats posed by the loss of personal data that make up the digital identity of a particular person.

1.*Fraud*. By creating fake accounts and under the guise of people we know, scammers force and convince people to go to unfamiliar sites that allow them to access their money.

2. *Receiving bonuses and postpaid services*. Some of us have come across ads of betting companies, forex sites, online poker rooms and other sites that offer new customers money into an account that they can use to employ the services. The stolen data will be used by the attacker to create an account in order to receive bonuses. This is usually harmless enough for the victims, the only thing is they will not be able to take advantage of the promotional offer in future. The consequences of acquiring postpaid services with stolen data can be much less rosy, when an attacker registers an account for your data, uses the services, and in the end, instead of paying for them, simply disappears. In this case, a full-fledged fraud is committed on your behalf.

3.*Account registration*. Photos of people are used to create social media spam accounts, which increases the frequency of successful attacks. Attackers often do not bother to change the data and take the real data of the victim, including the name and surname. On the network you can find offers for the sale of accounts in various social networks and other sites. To register such accounts, attackers also use stolen data, less often such accounts are collected as a result of phishing or data leakage.

4.*Getting a loan*. Today, in a highly competitive environment, online loan companies are everywhere lowering the requirements for borrowers, simplifying the procedure for obtaining a small amount. Such risks pay off high interest on loans, which sometimes reach thousands of percent per year, and heavy penalties for any delay. Minimization of checks and data provided has turned online loans into a tasty morsel for scammers who take loans on other people's data. In some cases, scammers will only need electronic copies of two documents of the victim, for example, a passport and driving license. To get them one can create a job ad and ask potential job seekers for a copy of the documents after "recruiting". Fraudsters know many ways to get copies of documents and to borrow by using them. There are also more sophisticated fraud schemes to obtain loans without the owner. On a Russian-speaking underground forum, there was an offer to sell air tickets for 50% of their real cost. The service owner assured that there was no fraud, air tickets were not bought with stolen funds. At first, forum visitors were distrustful of a tempting offer, then positive reviews began to attract more and more customers. Clients sent all their data to the attacker, including photocopies of documents. None of the clients had any problems with the flight. Problems arose later, when the bank in which these tickets were issued on credit began to demand a refund of the amount for air tickets, interest and appreciable sums for default on a payment. As a result, the victims paid 200-300 percent of the real cost of the purchased tickets.

5.*Revenge and damage to reputation*. On the net, one can find many stories about how ill-wishers, wanting to take revenge on someone, exhibited their photo and profile on various dubious sites. The main problem is that even if the site has deleted the victim's photo and profile by that time, other sites that copy data may host the profile, and thus, the photo will end up in the search results for images. Removing data from all sites and search engines often becomes almost an impossible task, especially if the victim does not have sufficient funds for this. If you are a reputation addict, detractors may try to ruin your reputation, e.g., to post reviews on products for adults on your behalf. Everyone who will look for information about you in future, whether they are employers or potential partners, will stumble upon similar reviews that do not color you. Any user can become a victim of a data breach when accounts are exposed online due to technical vulnerabilities or malicious actions. One can check if this data has been included in an open database by using a *special site* that accumulates information about account leakage.

Skeptics say that attackers will be able to get personal information in any case, if necessary, but it is better to make it as difficult as possible for them to get to one's data.

*What should be done in case of a leakage?*

In the event that your personal data got into the network and was posted on one or more sites, the following measures may be effective.

1.*Contacting the site owner*. It is the simplest and often the most effective method if your personal data are leaked and posted on one or more sites. You could ask politely and without any threats the site owner to help you. If your courtesy does not help, you may warn that you will be forced to take legal action and to apply to the regulator for the sole purpose of protecting your personal data.

2. *Appeal to the regulatory body*. You may write an appeal to the communication authority, in which you inform that the specified site distributes personal data without your permission, violating national laws. Make sure to include a link to the posted data. The maximum that the regulatory body is capable of is to fine the owner if it is found and is in the same legal jurisdiction as the body itself, or to block it in the territory of the country where the regulatory body is located. For many site owners, blocking in the territory of a particular country is a serious loss of audience, and they immediately remove the content that caused the block.

3.*Complaint to hosting provider and registrar.* A hosting provider is an organization that provides a site with a server for hosting, a registrar is an organization where the site owner has registered a domain name. You could go to the websites of the registrar and the hosting provider and find contacts for complaints there, they usually contain the word " abuse ". Even if such a contact is not found, you may refer to any available contacts.

4. *Appeal to fighters against fraudsters*. If the site is fraudulent (for example, it sells documents, or your personal data are posted there for the purpose of extortion), you should warn the organizations involved in the fight against such sites or compiling the databases of dangerous sites.

5.*Legal action.* If the appeal to the site owner, hosting provider and registrar has not brought a positive result, you may find a lawyer and think about going to court. The court may decide that a page with your personal data will be blocked in your country, as well as oblige search engines to remove your personal data. However, the possibilities of the court are highly dependent on the legislation of your country, it is worth consulting a lawyer on this issue. In order to break free from restrictions site owners often remove the content blocked by a court decision.

6.*Appeal to law enforcement agencies.* In many countries, the distribution or sale of personal data is a criminal offence. It is worth notifying law enforcement agencies about a site that violates the law. Fortunately, today it is not necessary to go to the nearest police station, stand in line and file an application as all this can be done online.

7.*Changing document data.* If you are afraid that a posted photocopy of your document can be used for fraudulent purposes, for example, to get a loan, it would be reasonable to contact law enforcement agencies and change your document number. This option is not available in all countries, you'd better turn to a lawyer to clarify the details.

*How to prevent digital identity theft*

To protect your data, you must follow the basic *rules of digital hygiene:*

✓ do not share a lot of information about yourself on the network;

✓ create complex and different passwords, even better – use a password manager to create and store them;

✓ wherever possible, set up two-factor authentication for logging into your account;

✓ do not store confidential documents and private photos for easy access on devices - smartphones, tablets, PCs;

✓ put a security solution on all devices and update it regularly; it is important that it is not just an antivirus, but a comprehensive solution to protect against phishing, online fraud, web surveillance, with a secure payment function;

✓ install applications only from official stores and carefully check what permissions you give to installed applications;

✓ do not follow dubious links, do not perceive a tempting offer as a call to action;

✓ be wary of calls from unknown numbers, messages from unknown senders, and any requests to transfer money;

✓ se for transmission the mail services with the ability to delete data from the recipient: Gmail has similar functionality;

✓ be sure to delete letters containing personal data from your email inbox and messengers in case your mailbox is hacked, especially if you sent scans of your documents somewhere;

✓ ask the recipient to treat your personal data with respect: when sending a letter with documents by mail or in a messenger, accompany it with a request to treat your personal data with respect

✓ do not name photocopies of documents with keywords: in some social networks, documents uploaded by users are made public, therefore, it is better to give any valuable documents, no matter how they are transmitted and stored, with neutral titles, for example, “pic15” or “image1988”;

✓ do not use social networks for authorization on sites: in exchange for this, you provide the site with access to your personal data, which it collects, sometimes sells, and sometimes is stolen by attackers;

✓ delete all unused accounts: website leaks are one of the most common ways of identity theft;

✓ when sending copies of your documents, indicate on them the date and the addressee (or the site where you send the data) using a watermark or a piece of paper attached to the photo of the documents with the addressee's data written on it: even if the copy falls into the hands of intruders, they will not be able to use it on other sites and most likely it will be removed as a defective product.

Compliance with these rules will at least make it more difficult for fraudsters to access an important part of the information about you as a person, and will help reduce the risk of losing money, reputation, and time. If the user himself pays more attention to the data that he provides about himself consciously or automatically, a digital identity theft will not be so elementary.

***Protection of biometric personal data***

In early 2018 the IBM Security division released a global survey on consumer opinion concerning digital identity and authentication. About 4,000 adults in the United States, the Asia-Pacific region (APR) and Europe took part in the IBM Security study "The Future of Identification Systems". According to its results, when logging into applications and devices, users are more concerned about security than usability. Moreover, according to the study, young people place less value on the security of traditional password identification. They prefer to use biometrics, multi-factor authentication, and a password manager to log in to increase their personal level of information security. Biometrics is going mainstream with 67% of respondents successfully using biometric authentication, while 87% of those surveyed said they would continue to use the technology in the future.

Survey results showed that teenagers and young people are leaving passwords in the past: 75% of those surveyed use biometric identification. At the same time, less than half of them use complex passwords to log in, and 41% reuse their passwords. Older people pay more attention to creating a strong password but are less likely to use biometrics and multi-factor authentication.

Against the background of the rapid spread of biometrics as a way of recognizing (identifying) a person for various purposes, for example, for identification in the access control systems of offices, in computer systems, smartphones, payment services and/or identification of users of financial services, the issue of ensuring protection of this type of personal data becomes especially relevant.

Biometric data are unique for each person, it is not repeated and does not change during life.

Biometric personal data include fingerprints, palm vein pattern, iris patten of the eyes, DNA code, face image, voiceprint, height, weight, features of the body structure, images of a person (photos, videos), other physiological and biological characteristics of a person (for example, gait).

*Threats of misuse of biometric personal data and ways to protect against them*

1) Deepfakes are realistic substitution of photos, audio and video materials created with the help of neural networks. Using computer algorithms, you can "revive" photos, replace faces with videos, and even synthesize a person's voice.

Almost anyone can create deepfakes due to the availability of training and numerous programs for working with this technology. Such a low entry threshold moves the technology forward, but also increases the number of tools for fraudsters to deceive users and steal their personal data.

Deepfakes can be used to manipulate our minds: for example, this technology can be used to create provocative videos with harsh statements by politicians or a video message from a well-known blogger, which either cause great resonance in society or call for registration on a website to participate in a raffle prizes. It is especially dangerous if a link to a phishing site is distributed along with such videos. But the most common way to use deepfakes is extortion; pretending to be friends, relatives or superiors, scammers can obtain personal data of a person using voice or video messages as confirmation of their identity.

2)Face recognition programs are neural networks that analyze the unique features of a human face and compare them with other photographs in various databases.

Most certainly each of us at least once used the image search in the browser. Using algorithms that collect key information about a person from his photo, you can find his social media accounts and use his personal data. For such a search, it is enough to upload a photo of a person, and the program will display information about him from open sources. Thanks to such a "portfolio" on the victim, scammers can easily draw up a suitable scheme of deception in order to extract even more personal data, and then money.

*How to protect yourself from fraudsters who use someone else's biometric data?*

✓ You should not use facial recognition programs, because in this way your data will fall into their database, and you will become a much more vulnerable target for scammers.

✓ Close your profiles on social networks - this way the programs will not be able to find your photos during the analysis.

✓ On social networks, add only trusted people whom you know personally as “friends”

✓ Fraudsters most often use open resources to create deepfakes. If you restrict access to your accounts in social networks and instant messengers (set up privacy), then they will be less likely to create something believable with your personality.

✓ Post only the information you need and make sure that the pages of your friends and acquaintances have a minimum of your personal data, or none at all.

✓ Check the details of the prize draws, contests or events on the official website of the company or in the actual account of the celebrity on whose behalf the promotion is being held. You should not follow unknown links, even if the photo accompanying the publication is a real image of a famous person.

✓ Be vigilant; always find the source or analyze the material before taking any action. Fraudsters will try to create stressful conditions to force you to make a decision immediately. Do not fall for such tricks, even if at first glance everything looks true.

**SECTION II. Financial security in social networks and online games**

According to the study published in 2019, almost 90% of Russian teenagers use social networks every day or "almost daily". We post a lot of information about ourselves on our social media pages; this is perhaps the largest information repository in the public domain and the easiest for scammers to get to.

It does not mean that in order to protect yourself and not fall victim to scams, you should stop using social networks. It is simply important to be aware of threats and rules that will help to protect yourself.

The most dangerous threat of fraud in social networks is involving users in financing terrorist and extremist activities through deception. *Financing of terrorism* is the provision or collection of funds or provision of financial services with the knowledge that they are intended to finance the organization, preparation or commission of any of the crimes of a terrorist nature, or to finance or otherwise materially support an organized group, illegal armed group, criminal community created or being created to commit such crimes.

Terrorist groups actively use the Internet, including social networks, to replenish their financial resources. The global money-raising networks of major terrorist organizations are built in the same way as those of non-governmental organizations, charitable foundations and other financial institutions. On websites, forums and chats, there are direct requests to help the "Jihad cause" by transferring funds or deceptive calls to transfer funds to fake charitable foundations to help those in trouble.

*Phishing on social networks*

This type of scam comes in many forms and involves the use of popular social media to take over someone else's account, steal sensitive data from victims, or lure them to fake websites for the purpose of gaining financial benefit. Fraudsters may create fake accounts by impersonating someone a potential victim knows in order to lure them into a trap, or they may even impersonate a customer service account of a well-known company in order to prey on victims who apply to this support company.

Also, through social networks, scammers can offer to buy various goods with big discounts, and when you follow the offered links, you fall into the trap: you do not receive the goods and you lose your money.

*How dangerous is phishing on social networks?*

By hacking your account and gaining access to your correspondence, sent and received files, subscriber base, fraudsters will have ample opportunities for various types of blackmail, publishing provocative information and social engineering; hiding behind your identity, a fraudster can contact each person in the contact list – that is how a chain reaction of fraudulent activities can be launched. Often, such mailings occur at night, as scammers often work from other countries (this complicates the process of tracing a scammer by law enforcement agencies).

*The most dangerous types of phishing:*

1) Messages asking for a cash loan, voting in a contest, a link to a "funny video" from one of your friends. When you go to the voting page or to watch a "funny video", you are prompted to enter your login and password on a page similar to the main page of the social network, after which the account is hacked.

2) Online stores, cinemas, delivery services and others. Here, the goal is data that allows access to linked bank cards. According to a study by Group-IB, in 2020 such services were the target in 30.7% of

fraudulent attacks[5]. Those who enter payment data in online stores are also at risk: if you make a mistake with the input window, without checking the address in the browser line, you risk sending money to a scammer. Moreover, there are services that simulate a transaction error in order to repeat it, for example, to conduct a transaction twice in a row.

3) Playing on feelings and emotions through publication on social networking pages of very emotional stories about children or animals in need of help, backing up the post with photographs, documents and the message "maximum repost". The main thing is to create a post conversion and its distribution from one person along the chain of his friends and contacts. Of course, the money from such "pseudo-charity " goes to scammers!

4) Curiosity game. You can receive tempting offers in private messages or in the news feed. In any case, you will be asked to follow a link and enter personal data or bank card details.

*Basic rules for protecting against phishing in social networks:*

✓ As soon as you find out that the data have been leaked or could potentially be stolen by scammers, change passwords from social networks, mail, and payment services as soon as possible. And it is better to change passwords every three months!

✓ Never use the same passwords. The rule "one password, one service" will help to interrupt the running phishing chain to check if your login and password match other popular services. Today, scammers use automatic services that allow to quickly check where else your data can go.

✓ Be cautious. Avoid rushing when entering your login, password and payment information. Check the address bar, look at the design elements. If something confuses you, do not enter your data!

✓ Use two-factor authentication. If your login and password are in the hands of hackers, you will have to enter the code received on your phone to enter or use an additional application.

✓ Do not trust dubious offers and links. A link hidden by a short URL service like *bit.ly* can lead to scammers. If the style of messages or the way your friend communicates in the chat has changed it is the reason to call him and make sure that he is the one who is writing to you.

*Fake accounts: why are they dangerous and how to recognize them?*

A fake profile on a social network is one of the ways to swindle users' personal data and money.

Fake pages can be created for various reasons.

1. The most harmless of them is when a person, for some personal reason, does not want to advertise his presence on a social network. Last name and first name are usually fictitious. Instead of an avatar, there are flowers or cats and few or no friends.

2. *Store sites* that offer popular or scarce items at very low prices and usually ask for a full refund before the item is shipped. And even if at the last moment you changed your mind about paying in advance, you have probably sent personal data to the scammers of to whom to deliver and where. They will be happy about this too and they will certainly figure out how to use your personal information.

*What to do:*

check information about promotions on the official websites of stores;

✓ remember that large stores are unlikely to send news about the prize draw through social networks; for this end they will rather use SMS or email,

you should be wary if you are asked to tell a large number of acquaintances about the promotion; this is a typical way for scammers to spread their links.

3. *Hacked account of a real person*. From such profiles, messages with spam (most often prohibited information or malicious links) or aggressive and offensive letters may come; they are designed to provoke you to inquire about the identity of the "hater" and, possibly, follow the link (often the only one) posted in his profile. But more often, scammers send letters to all friends asking for financial assistance or simply to help out with money until tomorrow. If you suddenly receive letters from friends with such pleas, be sure that this is most likely a hoax. In order not to be deceived, it is better to ask a friend personally by calling him.

*What to do:*

✓ do not react to negative comments: just block the user and delete the message;

[5]Group - IB official website. https://www.group-ib.ru/resources/threat-research.html

✓ do not use the links from the pages of users you do not know, especially if the only available option on them is to click on the proposed link;

✓ carefully check all pages where you are asked to enter personal data: look at the domain name, the https protocol and the lock icon;

✓ set up two-factor authentication on all social networks where possible (see the memo);

✓ in your privacy settings, block strangers from leaving comments and hide your posts from them to avoid spam and insults.

*4. Creating a celebrity profile* - a favorite performer suddenly announced a collection, for example, to help some person, or for a prize draw.

*What to do:*

✓ check if the page of the famous person you would like to chat with on social networks has been verified - reliable profiles are marked with a blue checkmark;

✓ check the creation date of the profile and all posts if the photos were uploaded two days ago, its author is probably a scammer; you can determine the originality of the photo using the "image search" function in Internet search engines;

✓ view the content of the account: malicious links or obscene expressions are a reason for *not to make friends* with such a public page.

✓ analyze the activity: read the comments and study the news feed and the speed of its filling - fake profiles fill up quickly, and they are filled with the same type of comments and subscribe to everyone in a row.

*Tests and polls in social networks*

Each of us, one way or another, met funny tests in the social network feed, offering to find out your psychological age, which of the film character you look like, or which zodiac sign you are most compatible with. The answers to these questions are unlikely to help in life, but such tests can allow attackers to steal your personal data or money from electronic accounts.

Tests operate on basic data from a social network profile, such as name, number of photos, connections with friends, for which they ask you to give permission to synchronize with your profile (access to photos, profile data, posts on the wall, list of friends and other personal information). This seemingly harmless and meaningless data will end up in the developer's database and subsequently be used for illegal purposes.

It should be remembered that tests published on social networks are hosted on third-party resources, the owners of which earn money by placing ads and monetizing the tests themselves; the user may be required to pay to get test results or take the test or offer to install some application. Tests are deliberately done with a huge number of questions in expectation that the user will feel sorry for the time spent and will send an “inexpensive” SMS, the cost of which may be much higher than previously declared, or several SMS may be needed.

In addition to following a link, there may be a risk of an attack called " *clickjacking* " - a fraudulent scheme in which an attacker can gain access to confidential information or even to a user's computer by luring him to an apparently harmless page or injecting malicious code into a safe page. The principle is based on the fact that an invisible layer is located on top of the visible page, into which the attacker loads the needed page, while the control element (button, link) necessary to perform the required action is combined with the visible link or button that the user is expected to click on. There are various ways to use the technology - from subscribing to a resource on a social network to stealing confidential information and making purchases in online stores at someone else's expense.

*What to do:*

✓ When allowing a test to access a profile on a social network, always read carefully what information is being requested.

✓ Regularly check your profile settings on the social network: what applications are linked to it and what rights they have.

✓ Do not give your bank card details, phone numbers, passwords and other personal data in tests and when clicking on links.

✓ Using and regularly updating an antivirus will prevent penetration of a malicious element if it is injected into the test.

✓ Tests can be taken on the Internet without installing separate applications (you can often see an installation prompt).

***Online games: to have fun and become a victim of scammers?***

Computer games have long ceased to be something unusual and mysterious and a huge number of people around the world enjoy them. According to Microsoft, the total audience of video games is more than three billion people[6].

With the development of the Internet, a separate class of computer games has appeared; one can play them not only locally on a personal computer or with a partner on the same keyboard, but with thousands and tens of thousands of players from all over the planet.

The growing number of players in online games entails an increase in threats, as scammers try to make the most of the current situation. Online games store not only game currency and purchased game items, but real money which is of particular interest to attackers.

*The main dangers of online gaming*

*1) Identity theft* is perhaps the most common type of online fraud.

*2) Theft of money*: game currency, game items and real money in a virtual wallet are the main interest of scammers. Experts warn that the risk of being scammed for a gamer is highest when he opens an account for payment; in fact, that is the purpose to launch a game. 48% of fraud cases occur just at the time of payment.

*3) Account theft*: after stealing an account, scammers begin to blackmail the user, demand money for its recovery.

*4) Malicious software*. For example, the user is prompted to download a plugin for a game. Unaware of the trick, he follows a link to another site running malicious software. The purpose of such software is to harm the security and privacy of the user's device. Moreover, viruses can be embedded in the game files, and unknowingly, the user can let them into his system during installation.

*5)Privacy violation*. By matching the data obtained from games and other sources, attackers can gain access to your other accounts, such as social networks, as well as register new accounts under your name or even create digital identities.

*6)Hidden fees* . Some online games are released in a shareware version: some of the content is provided for free, but you need to pay to get access to all the features and functions. To do this, you need to link a bank card to your account, and payment will be automatically debited from the card when the user purchases new items or services.

The most common *fraudulent schemes:*

*1.Redirecting players to fake sites* that usually look like real sites for buying add-ons (equipment, powers, new abilities, etc.) and in-game currency. In fact, the main goal of these sites, like any phishing sites, is to trick the user into transferring money for a product that he will never receive .

*2.Attacks on players' IP addresses (* unique user addresses on the Internet), having learned which, scammers can figure out your actual address, first name, last name and other private personal information. With this data, they can steal your financial information or game credentials.

*3.Phishing mailings, the purpose of which* is to deceive the user's account information. Fraudsters may send emails to players asking them to verify their login details. By clicking on a link in such an email, players are taken to a fake login page, where they are asked to enter their current password and username. As a result, the credentials end up in the hands of scammers.

And links to malware can also be sent, and in the most diverse ways:

on the players' forum (links to a malicious program are published under the guise of a link to a game patch);

in the game itself (links to a malicious program are sent under the guise of a “new patch”);

by e-mail (spam is sent with the malware itself or with links to it);

malware is distributed through file-sharing networks;

---

[6] Source: https :// news . microsoft . com /2020/09/21/ microsoft - to - acquire - zenimax - media - and - its - game - publisher - bethesda - softworks /

uses web browser vulnerabilities (to download malware when visiting gaming sites.)

most often, attackers post links to a malicious program with tempting comments on a game forum or in a game.

*4. Fake mobile versions of popular online games.* Once downloaded, these applications install malware on victims' smartphones or computers. Fraudsters use such software to intercept account information used to make purchases on popular gaming platforms and consoles. This data is then used to steal sensitive user information, including bank card details, home address, and phone number.

*Basic safety rules in online games*

✓ To make any in-game purchases, use only official sites , while carefully checking the domain name of the site, as scammers often use domain names that are consonant with the brand.

✓ When learning about a new feature in a game or app from a source other than the official source, look for more information on the topic. Most often, there are already people who have encountered this and shared their positive or negative experience.

✓ Look for and check information about promotions and great offers from official sources or from official representatives.

✓ Never follow links that lead to third party sites .

✓ Do not respond to emails or correspondence requests **that** ask you for banking, financial or personal information , even if you think the message was sent from the gaming platform. A real company will not ask you for information via messages.

✓ Do not share personal information , do not transfer account information over the Internet. Do not forward your credentials even to friends.

✓ Use a strong password to enter the game and never use the same password for multiple accounts

✓ Don't forget about two-factor authentication . It protects you more reliably and complicates the task for attackers.

✓ Remember to update your antivirus software regularly.

✓ VPN can be one way to protect (Virtual Private Network, virtual private network). It makes your internet connection private. VPN applications are easy to install, do not require complex configuration, and offer a number of advantages:

-protect against attacks, such as DDoS , which can be launched against rivals in online games, especially in the case of competitive struggle;

-provide additional security when transferring data and performing banking transactions, since the VPN connection cannot be traced.

Some VPN apps are free, but they may restrict your data transfer and may not provide complete security. Before choosing a VPN, you need to clearly understand what its protection will cover. To do this, please read the terms of service, including the privacy policy. While some VPNs promise to protect you from malware and phishing sites, they don't offer the same level of protection as a standalone antivirus, so it's best to have both .

**SECTION III . Protection of human rights in the financial sector**

It is impossible to consider the issues of protecting human rights in the financial sector without defining the concept of “human rights” proper. Among them it is customary to include the right to life and liberty, freedom from slavery and torture, freedom of opinion and their free expression, the right to work, education, etc. These rights should be enjoyed by all people without exception, regardless of their gender, age, race and ethnicity, religion, etc.[7]

The list of key human rights and freedoms is fixed in the Universal Declaration of Human Rights, adopted in 1948, later other documents were created that expand and clarify the list of human rights in various fields[8].

---

[7] Human Rights / United Nations Organization. URL : https :// www . un . org / ru / global - issues / human - rights (date of access: 07/04/2022)

[8] Universal Declaration of Human Rights, 1948. /
URL : https :// www . un . org / ru / documents / decl _ conv / declarations / declhr . shtml (date of access: 07/04/2022)

Many of the human rights mentioned above are not directly related to the financial sector, but it would be a mistake to think that human rights cannot be violated in the financial sector. Factors that directly threaten human rights in the financial sector include[9]:

1.Discrimination in lending practices: lending can affect human rights, regardless of the size and term of the loan. So, a person may be denied a loan because of his race, religion or creed. And the development of automatic credit checks allows such practices to be disguised.

2.Lack of an objective view of the client: all financial institutions must conduct a full range of checks before issuing a loan, including when working with people. Failure to comply with this principle and issuing credit without verification can lead to serious human rights violations later.

3.Lack of an objective view of the sector in which they plan to invest: financial institutions must ensure that their investments in various types of projects do not lead to violations of human rights.

4.Confidentiality of customer and employee data: weak protection of this kind of information can lead to a violation of human rights, especially if information about important aspects of a person's financial situation has become available to third parties. It is important for financial institutions to ensure data protection so that this does not happen, as well as to increase the competence of employees in terms of information protection.

Equity in pay: Organizations in the financial sector (as in any other field) must provide fair pay based on an assessment of the performance of an employee, his professional, and not any other qualities. Otherwise, one of the basic premises of the concept of human rights is violated - the idea of universal equality.

The opportunities for human rights violations in the financial sector listed above demonstrate how this area fits into the broader concept of human rights. However, many of the aspects that have been discussed relate more to employees in the field of finance or interorganizational interaction.

With regard to specific human rights in the area of finance, it is worth noting that those who speak of these kinds of rights are referring to Article 25(1) of the Declaration of Human Rights, which states that “Everyone has the right to a standard of living which includes food, clothing, housing, medical care and necessary social services necessary for the health and well-being of himself and his family, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other loss of livelihood in the event of circumstances from him. They draw attention to the fact that it is the availability of finance and access to financial instruments (for example, credit) that allows a person to gain access to all the basic goods that everyone should be entitled to. Moreover, it is precisely the ability to use financial instruments that can contribute to the exit from poverty (which is interpreted as the lack of access to the benefits listed above). Based on this, scientists conclude that the right to access finance and credit should be considered as a human right.[10]

In everyday life, the concept of human rights in the financial sector can be interpreted more broadly, and speaking of human rights violations, experts often understand situations where citizens are faced with financial fraud, problems with credit institutions, etc., and are forced to fight for the safety of their funds. Despite the fact that much in terms of financial security depends on the person himself, organizations that ensure the protection of human rights in the financial sector play an important role in ensuring it[11].

Measures to protect human rights in the financial sector can be divided into reactive (working on the fact of an already committed fraud, for example, based on complaints from victims) and preventive (when potential human rights violations are identified before someone is harmed by them. Activities in both directions leads *the Central Bank* ... You can contact him and report that a financial organization violates human rights in the financial sector... The Central Bank does not interfere in the contractual

---

[9] 10 Human Rights Priorities for the Financial Sector // BSR. URL : https :// www . bsr . org / en / our - insights / primers /10- human - rights - priorities - for - the - financial - sector (Accessed: 04.07.2022)

[10] Pradeep KB Access to Finance and Human Rights / MPRA Paper No. 80336. 08/03/2017. URL : https :// mpra . ub . uni - muenchen . de /80336/1/ MPRA _ paper _80336. pdf (date of access: 04.07.2022)

[11] The list of organizations and description of their powers is prepared on the basis of: Protection of the rights and interests of consumers of financial services. Federal Fund for the Protection of the Rights of Depositors and Shareholders. URL : https :// fedfond . ru / bitrix / docs / zaschita _ prav . pdf ? ysclid = l 4 orjbx 4 qj 889467271 (date of access: 06/22/2022)

relationship between the organization and the client, however, it can initiate an audit of the organization's activities and take measures if violations are detected. The Central Bank keeps statistics on filing complaints against various types of organizations.More than half of all complaints about violations of human rights in the financial sector are accounted for by credit organizations.

*Antimonopoly authorities* can also be attributed to organizations that guard human rights in the financial sector. One of its key tasks is to ensure competition in the financial services market. Along with this, she monitors compliance with legislation in the field of advertising. Among the areas of activity:

prevention and suppression of advertising that can mislead the user or harm his health;

protection from unfair competition;

bringing subjects of advertising activity to responsibility for violation of the law;

– Liaising with advertising regulators.

Speaking about organizations that protect the rights of consumers of financial services, one cannot fail to note the work *of the internal affairs bodies, the police* . They are engaged in the investigation of crimes and are obliged to accept citizens' appeals at any time, regardless of the place of the crime and the completeness of the data about it. The statement must indicate the essence of what happened, the date, time and place. It is also important to provide information on the amount of damage caused. After submitting an application, you must receive a coupon notification of its acceptance. The decision on the further fate of the application must be made within seven days from the date of application. If the answer is not received, you need to contact the head of the police department, and if you can’t get an answer from him, you need to contact the prosecutor’s office.

*The bodies of the prosecutor's office* play a special human rights role, since its bodies have the relative autonomy of the functional branches of state power and sufficient branching, providing almost universal access to them for the population. The Prosecutor's Office has the authority to protect the rights and freedoms of man and citizen, both in supervisory and non-supervisory activities.

## *Appendix*

***Appendix No. 1***

**Glossary**

*Authentication* is a procedure for verifying the identity of a person gaining access to an automated system by comparing the identifier reported by him and the presented confirming factor.

*Blockchain* is a distributed database that contains information about all transactions carried out by system participants.

*Income* is the totality of all monetary receipts of a person or household (such as wages, business income, social benefits, income from property, etc.).

*Proceeds of crime* is money or other property obtained as a result of a crime.

*Inflation* is the change in the price level in the current period compared to the selected period.

*Compliance control* is an internal system for ensuring compliance of the company's activities with the requirements of financial legislation.

*Lending* is the provision of money to a borrower by a bank or other financial institution at a certain percentage.

*Cryptocurrency* is a digital payment system that does not involve banks during operations.

*Legalization (laundering) of proceeds from crime* - giving a legal form to the possession, use or disposal of funds or other property obtained as a result of a crime.

*Personal financial security* is a socio-economic opportunity for a person to have financial independence to meet their material and spiritual needs, both individually and within society, as well as maintaining this independence in the future and its further multiplication.

*Fraud* is theft by deceit or breach of trust.

*National financial security* is the state of the financial and credit sphere, which is characterized by balance, resistance to internal and external negative influences, the ability of this sphere to ensure the effective functioning of the national economic system and economic growth; the level of protection of financial interests at the macro and micro levels of financial relations.

*Personal data* is any information relating to a directly or indirectly identified or identifiable natural person (subject of personal data).

*Savings* is the difference between income and expenditure of the population.

*Counterfeiting* is the production of counterfeit bank notes, securities for the purpose of selling, as well as their storage and transportation.

*Financial security is* a concept that includes a set of measures, methods and means to protect the economic interests of the state at the macro level, corporate structures, financial activities of business entities at the micro level.

*Phishing* is sending e-mails about alleged changes in the bank's security system.

*Forex* is a market where the buying and selling of banknotes takes place.

## Resources

***Appendix No 2***

Online anonymity and security course. URL: https://book.cyberyozh.com/ru/?fl=ru .

Portal "Financial culture": https://fincult.info/ .

Fingramota portal : http :// www . fingramota . org / .

Internet and social media statistics for 2023 - figures and trends in the world and in Russia [website]. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-iv-rossii/ .

Internet portal of the National Financial Research Agency. URL: https://nafi.ru/analytics/27-derzhateley-bankovskikh-kart-mogut-stat-zhertvami-moshennikov/ .

Portal of the Non-Commercial Partnership "Institute of Education and Science" (NP "ION"). URL : https://profin.top/literacy/lichnye-finansy/base.html .

Video lessons of financial literacy for schoolchildren. URL: https://www.youtube.com/watch?v=kK5vp_uzY6Q .

Scientific and educational portal " IQ " of the National Research University "Higher School of Economics". URL: https://iq.hse.ru/more/finance/neobhodimost-povishenia-finansovoj-gramotnosti .

## Test tasks for knowledge control

*Appendix No 3*

**1. A stranger is added to your "friends". Your actions (1 correct answer).**

a) I will reject his application.

b) I'll add if we have mutual friends.

c) I'll add you as a friend! The main thing is more friends!

I'll look at his page and add him as a friend if I don't see anything suspicious.

**2. Your close friend sent you an email with the following content: "Hi. This month they did not pay my salary, but I have a loan. Lend me a thousand. Throw it on the map. Your actions (1 correct answer).**

a) I have no money myself, I will not transfer.

b) I won't lend until I talk to a friend in person.

c) Asking for a loan for the first time. The amount is small, why not help a friend out. I will translate!

d) I don't remember a friend telling me about a loan. I will clarify in the correspondence what kind of loan and when he issued it. After the answer I will transfer the necessary amount.

I won't give you a loan, I know that I definitely won't return it!

**3. You are following the official account of a well-known blogger who has just published a post: "In honor of my birthday, I decided to raffle off an iPhone. To participate in the draw, follow the link and fill in your details. Your actions. (1 correct answer).**

a) I will not follow the link and open it.

b) I will participate, I just need a new phone.

First, I will check if this account is fake: if there is a "blue tick" next to the nickname, then I will take part. Everything is safe!

**4. You saw a repost on your friend's page asking for financial assistance for an operation on a seriously ill child. The child's profile contains all the documents confirming the diagnosis and the need for urgent surgery. You will help? (1 correct answer).**

a) I will transfer the money and make a repost on my page. The child must be helped!

b) They are most likely scammers, I will not help. I'd rather help someone through a trusted charitable foundation.

c) I will look carefully at all the documents confirming the diagnosis. If the situation is really difficult, I will send a small amount.

My friend helped and I will help! This will improve my karma.

**5. Fraudsters often hide under the guise of online stores on a social network, so before making a purchase, you need to carefully study the store page. Which store do you choose not to buy from? (1 correct answer).**

a) If the store does not have its own website.

b) If the store is not able to pay for the goods upon receipt.

c) If the store has few subscribers and no customer reviews.

If the store does not have the possibility of self-delivery.

**6. You actively communicate in different social networks, but you haven't used one for a long time. How will you deal with your account? 1 correct answer.**

a) I will not delete, suddenly, it will still come in handy!

b) I don't know what to do with it.

c) I'll delete it, why do I need it, I still don't use it.

I want to delete it, but I keep forgetting about it.

**7. You received a message on a social network with an offer to buy attributes for an online game at very attractive prices and a link to a resource where you can buy them. Your actions (1 correct answer).**

a) Saving is always good! I will definitely go through the link and, if the prices suit me, I will make a purchase.

b) These are all tricks of scammers, I will not follow the link.

I'll follow the link, I'm afraid to miss a good opportunity!

**8. What contributes to a decrease in the personal financial security of a person? (select all that apply)**

a) Fraudulent activities by intruders

b) Low level of financial literacy

c) Deteriorating economic situation

Long-term employment in one workplace

**9. Which of the following examples characterize the situation of risk diversification? (select all that apply)**

a) Distribution of all available savings between accounts in different banks and in different currencies

b) Ignoring information about the risks of revoking a license from a large bank

c) Increased risk of car theft by storing it at home rather than in a paid parking lot

Use of various investment instruments: stocks, bonds and real estate investments

**Answers** : ***1*** *- a ) /* ***2*** *-b /* ***3*** *- c /* ***4*** *-b /* ***5*** *-b /* ***6*** *- c /* ***7*** *-b /* ***8*** *-abc /* ***9*** *-a d*