



Financial Security of the Individual on the Internet

Thematic lesson



RUDN
university



Ministry of Education
of Russia



Ministry of Education
and Science of Russia

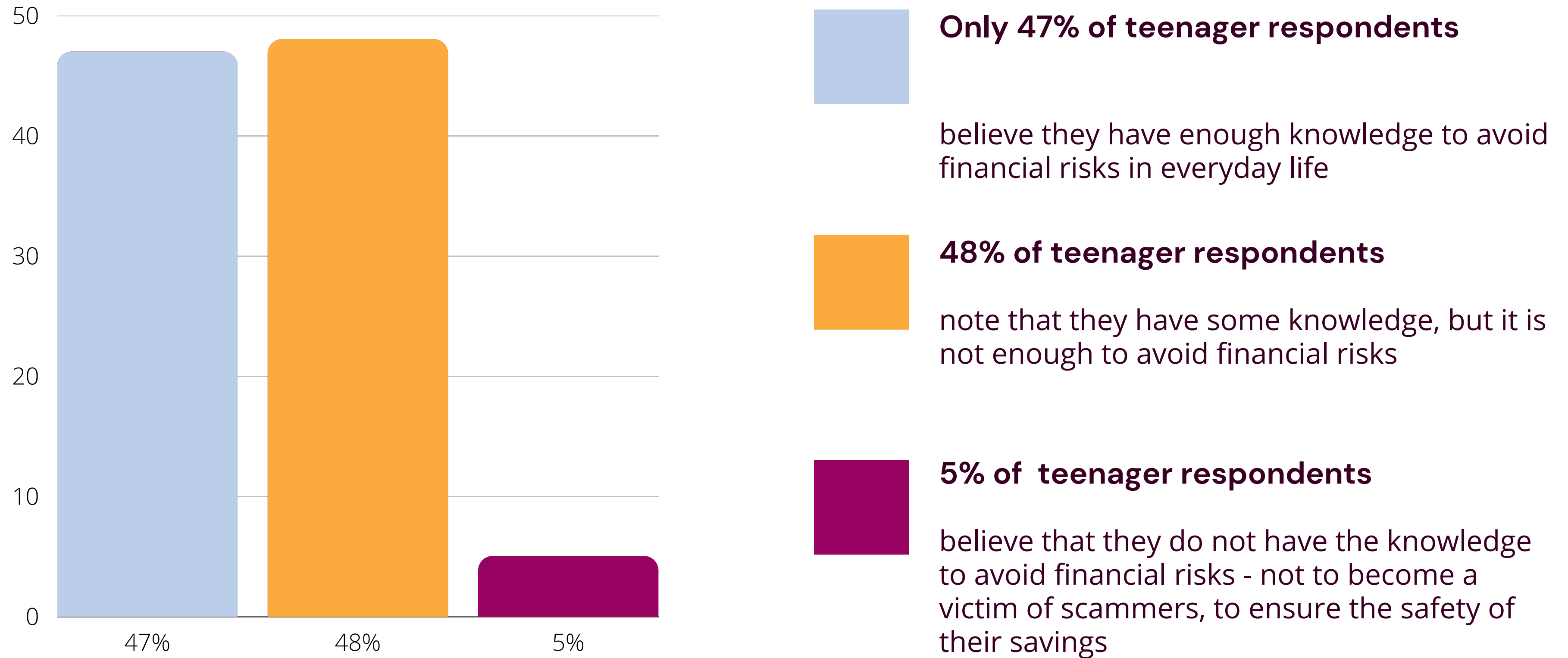


Rosfinmonitoring



Statistics 2022

2



the 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.



National

financial security of the entire state

Regional

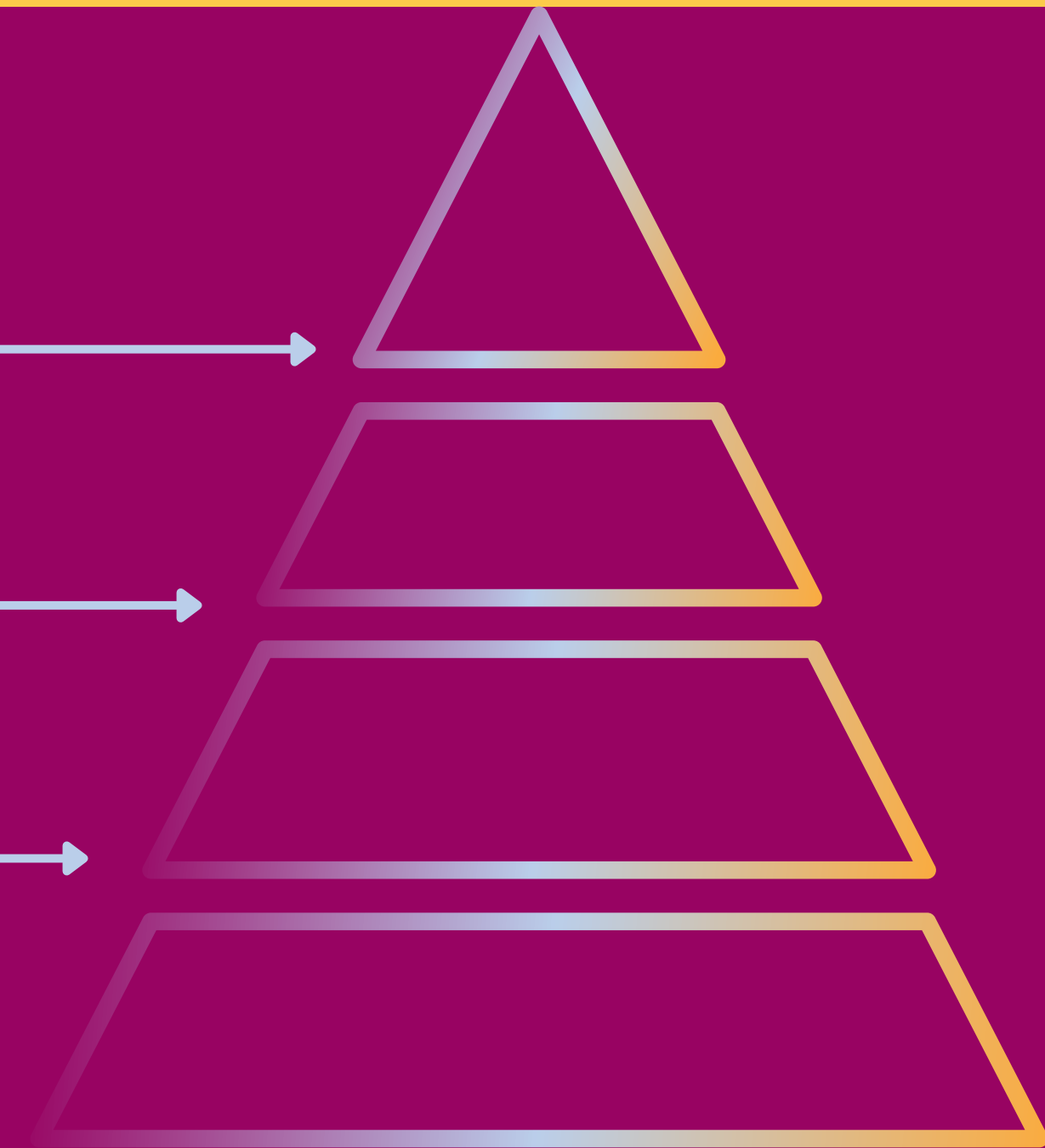
the security of certain parts of the state

Corporate

financial security of organizations

Personal (family)

individual security



Financial Fraud



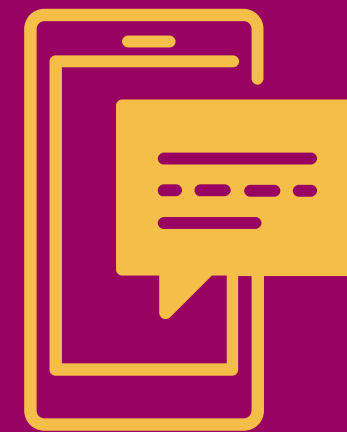
the commission of illegal actions in the field of monetary circulation by deceit, breach of trust and other manipulations for the purpose of illegal enrichment.



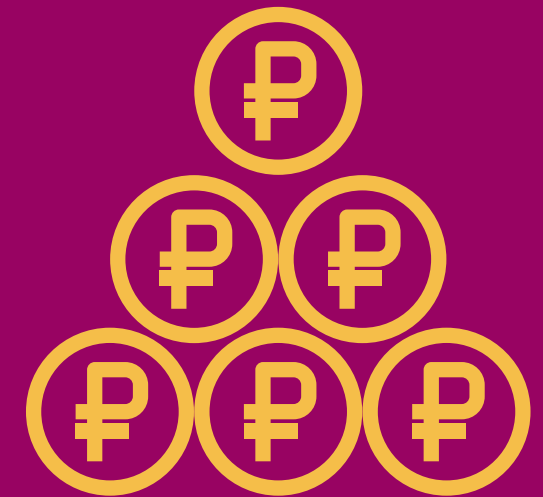
bank cards fraud



Internet fraud

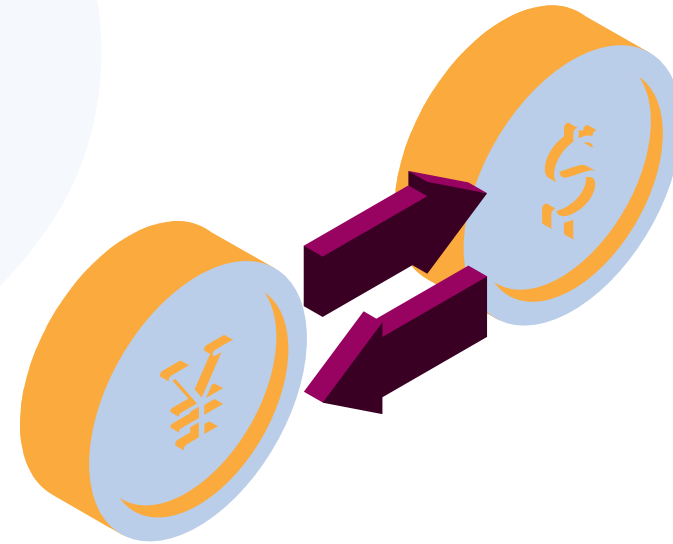


mobile phones fraud



financial pyramids

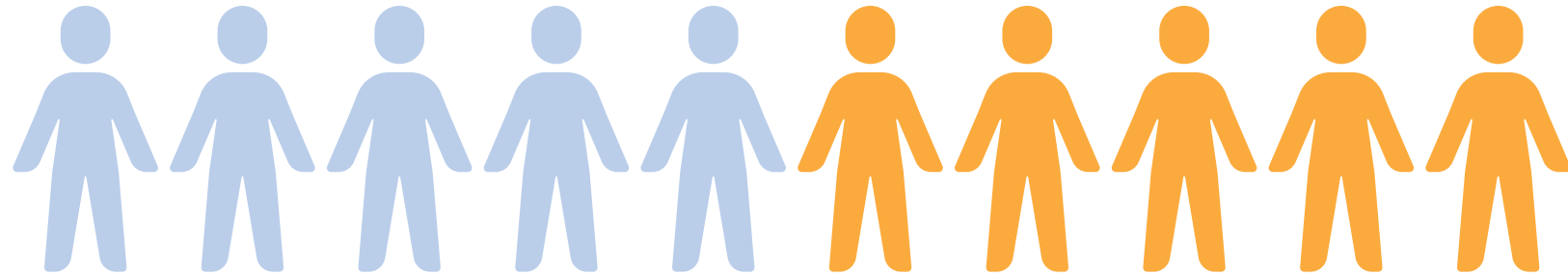




I. Digital Identity Profile and Biometric Personal Data

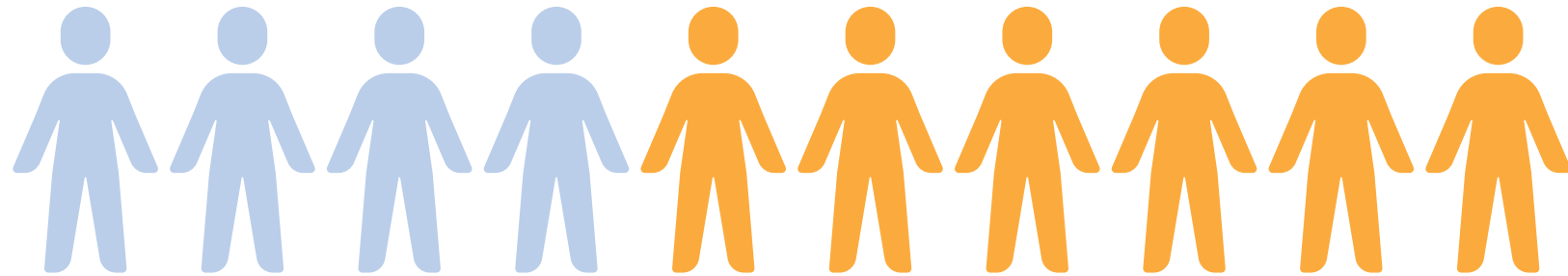
Global Digital Statistics 2023

use of the World Wide Web and the safety of personal data on the Internet



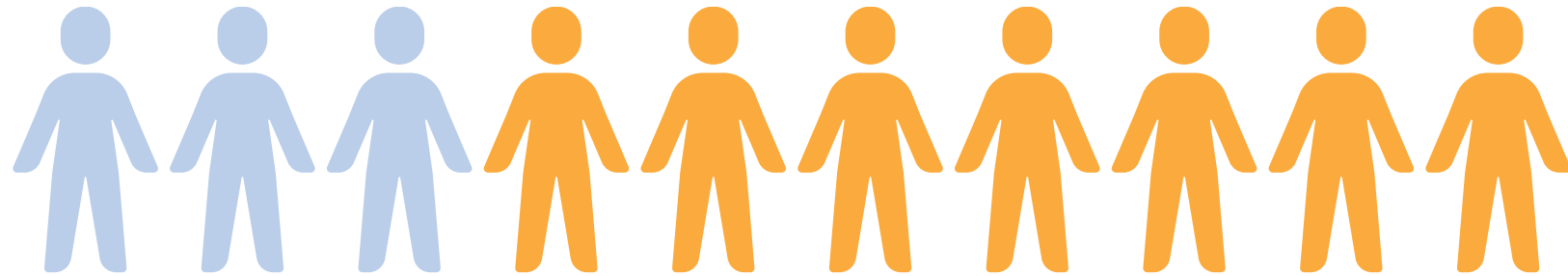
64.4% of the world's population

has internet access as of early 2023



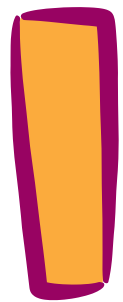
60% of the world population

are users of social networks



59% of young Russians

do not pay due attention to the safety of their personal data when making purchases on the Internet

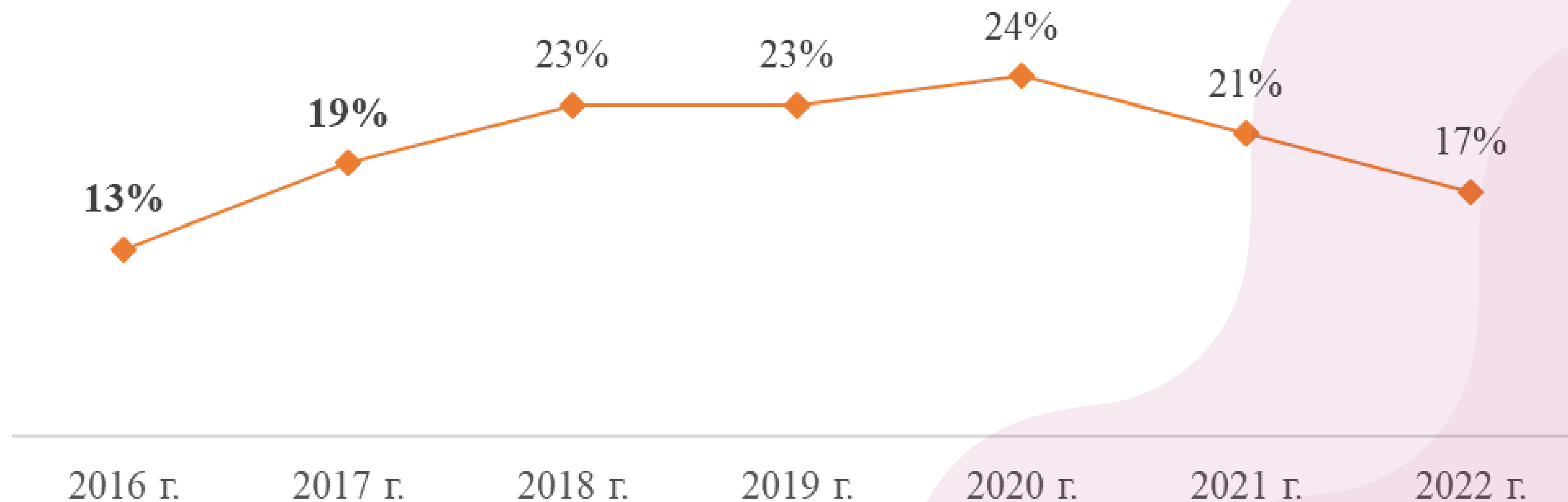


Think and Discuss:

- What conclusions can be drawn from the above data?

Statistics 2022

Percentage of those who agree with the statement: "I have sufficient knowledge and skills to protect my personal information on the Internet", is % of those who use the Internet



Personal Information

any information that directly or indirectly points to you, or is somehow related to you



general personal
data



special
categories of
personal data



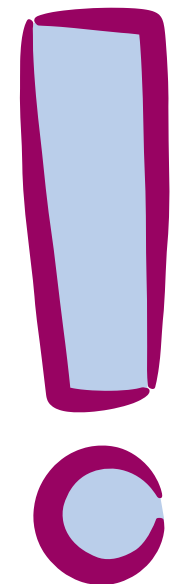
publicly available
personal data
that one allows
to be shared



biometric personal
data

Digital Personality

personal data with which a criminal can impersonate one, for example, to obtain material benefits

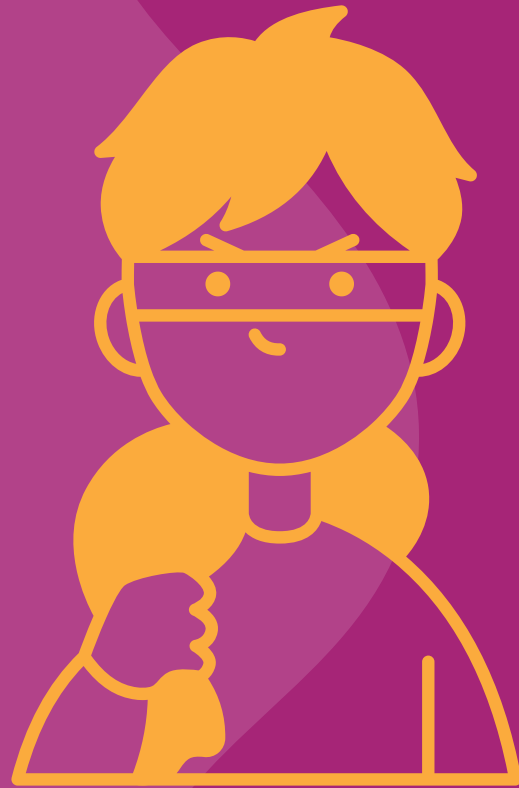


Assignment

Give at least three examples of information, namely elements of your "digital identity" that you publicly release over the Internet. What kinds of your data can be stolen?



Why Do They Steal a Digital Identity?



Fraud and extortion



Registration of fake
accounts



Getting a loan,
bonuses and post-
paid services

Situation

Deputy of N. city Sh.Sh. Sattorov began to find online reviews on his own behalf, published on various resources. Outwardly, these were inconspicuous reviews containing real details of his family life and a description of the product, but rudeness and disrespect for users were always traced in the reviews, they always caused a negative attitude towards the author in the ordinary reader.

As a result, citizen Sh.Sh. Sattorov decided to write to the site owners with a request to remove illegally distributed personal data.

Assignment

11

1. Read the text.
2. Guess what sort of family life details of Deputy Sh.Sh. Sattorov might have been published along with the product reviews.
3. Drawing on the material of the memo on how to eliminate the consequences of data leakage and on the samples of appeals on the next slide, make a hypothetical appeal from citizen Sh. Sh Sattorov. to the site owners.





Please delete!

Sample Request for Deletion of 12 Personal Data

Good afternoon,
Your website (specify the link) has posted my personal data for public access, namely (specify which data). Please help me to remove them.

If there is no response to my appeal, I regret to inform you that I will have to file a corresponding application with the regulatory body, as well as ask for the assistance of the domain name registrar and hosting provider serving your site.
I hope for your help!

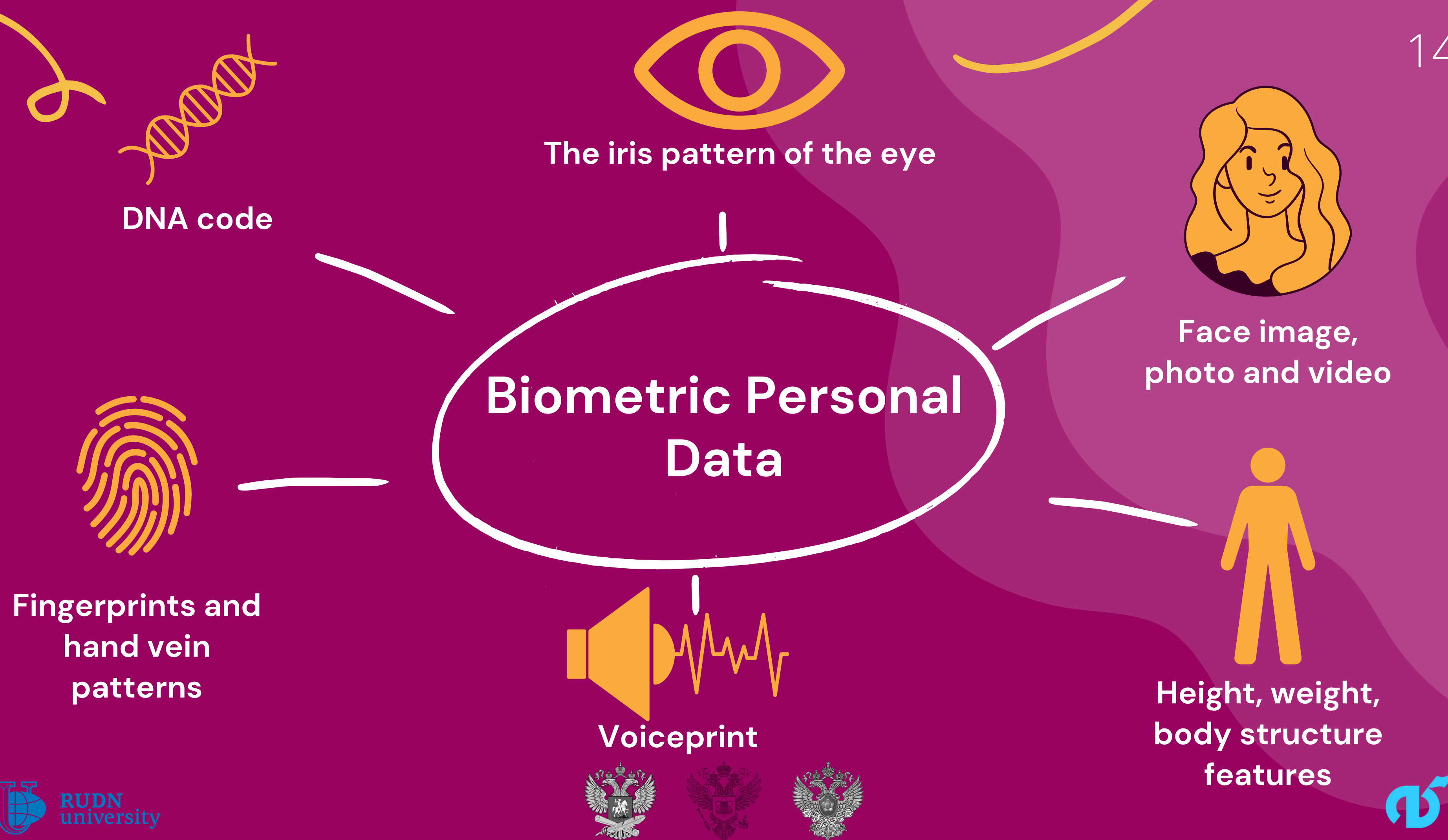
Sincerely,
(applicant's full name).

Digital Hygiene Rules:

- create complex and different passwords, use a password manager to create and store them;
- set up two-factor authentication for logging into your account;
- install applications only from official stores and carefully check what permissions you give to installed applications;
- use mail services for transmission with the ability to delete data from the recipient;
- delete email with personal data from the mailbox and messengers;
- do not use social networks for authorization on sites;
- delete all unused accounts;

It is easier to prevent data leakage than to eliminate its consequences!



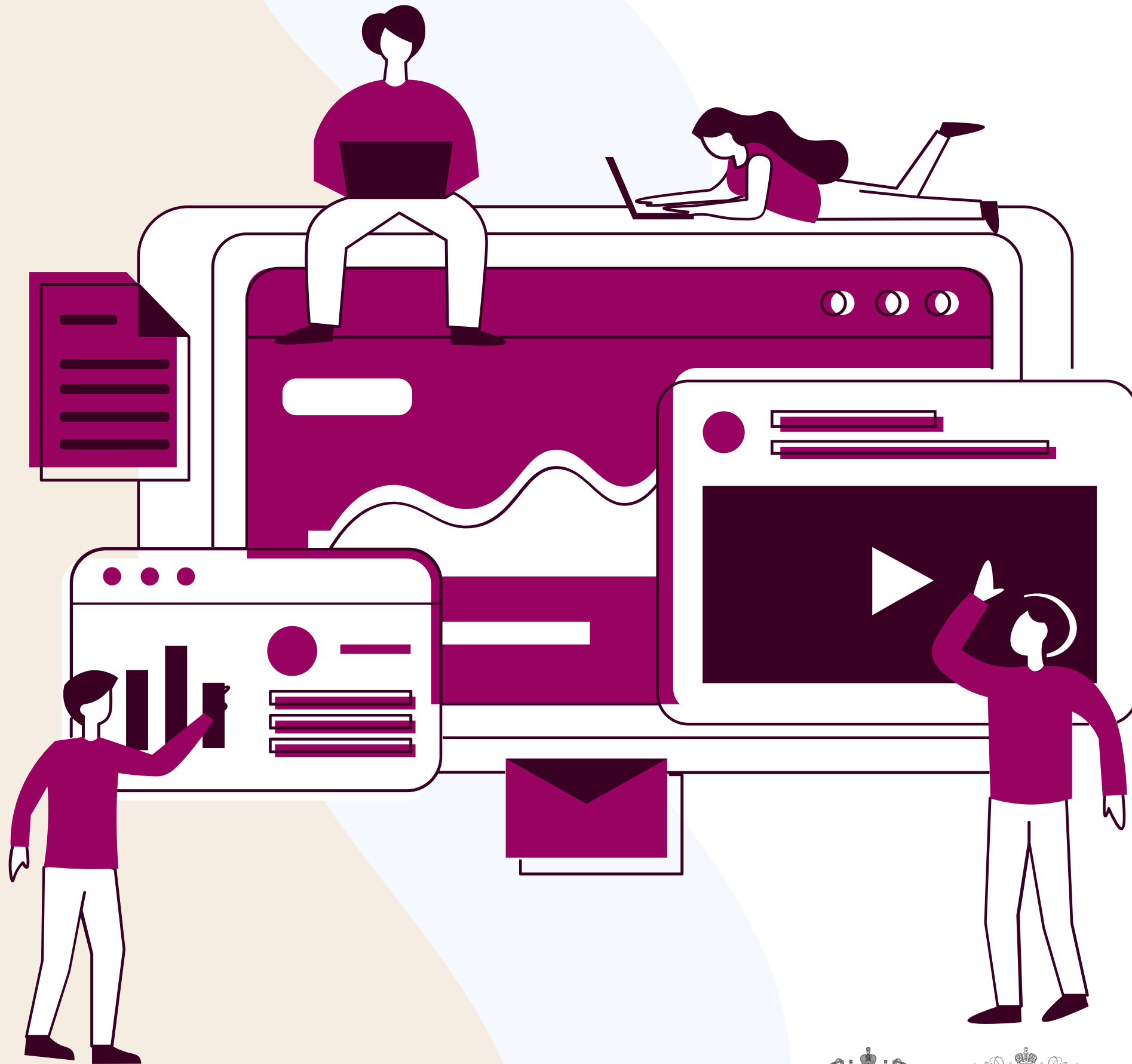


Situation

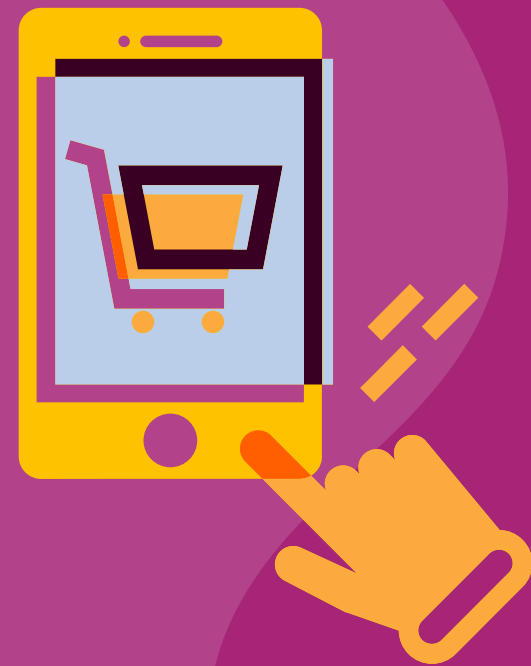
In 2021, a resident of the city, H. Muqaddas, complained that she fell into the trap of scammers who used a special computer program to “clone” a person’s speech, and lost 50,000 conventional monetary units. That was the price to save her friend from revocation of driving license for driving while intoxicated. When a “friend” called from a number unknown to the girl, she had no doubt that she was talking on the phone with a person close to her. Allegedly, he has just changed his phone number and he really needs help, because a police officer is demanding a bribe. Then the phone was handed over to the “employee”, who convinced the girl to hand over the money to “resolve” the situation. The girl followed all the instructions for transferring to an unfamiliar number and only after that she turned to the bank, but the payment to the fraudster had already been made.



II. Financial Security in Social Networks and Online Games



— a type of fraud that involves the use of social networks in order to take over someone else's account, steal the confidential data of victims, or lure them to fake sites in order to gain financial benefit.



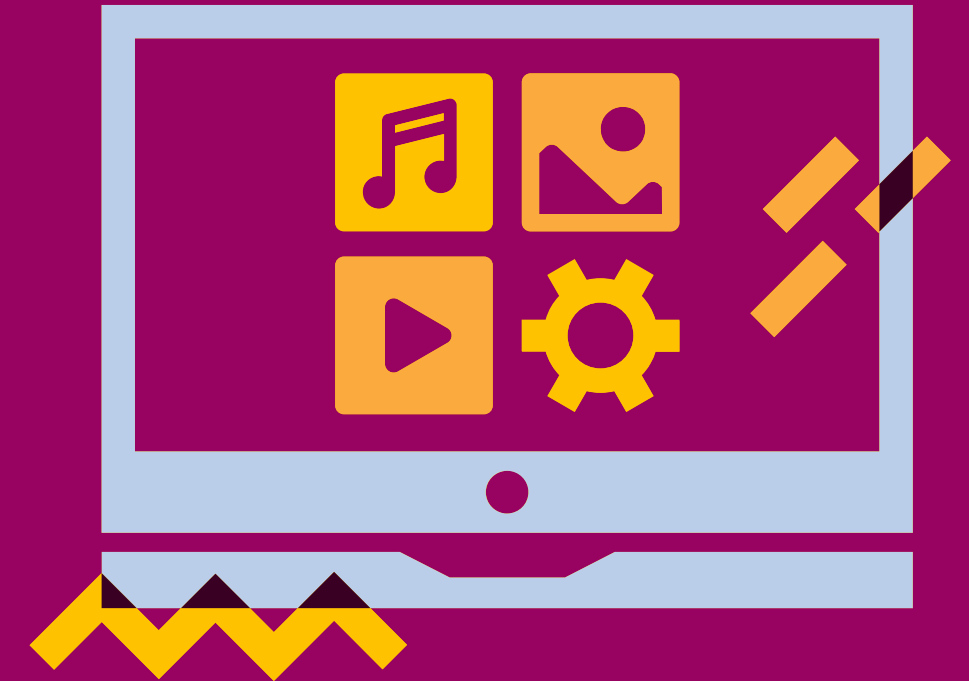
Online stores, cinemas, delivery services and other paid services

Purpose: data that allows access to linked bank cards



Posting emotional stories on social media about children or animals in need of help

Purpose: the maximum number of reposts and money directed to pseudo-charity (which can be used to finance terrorism and extremism)

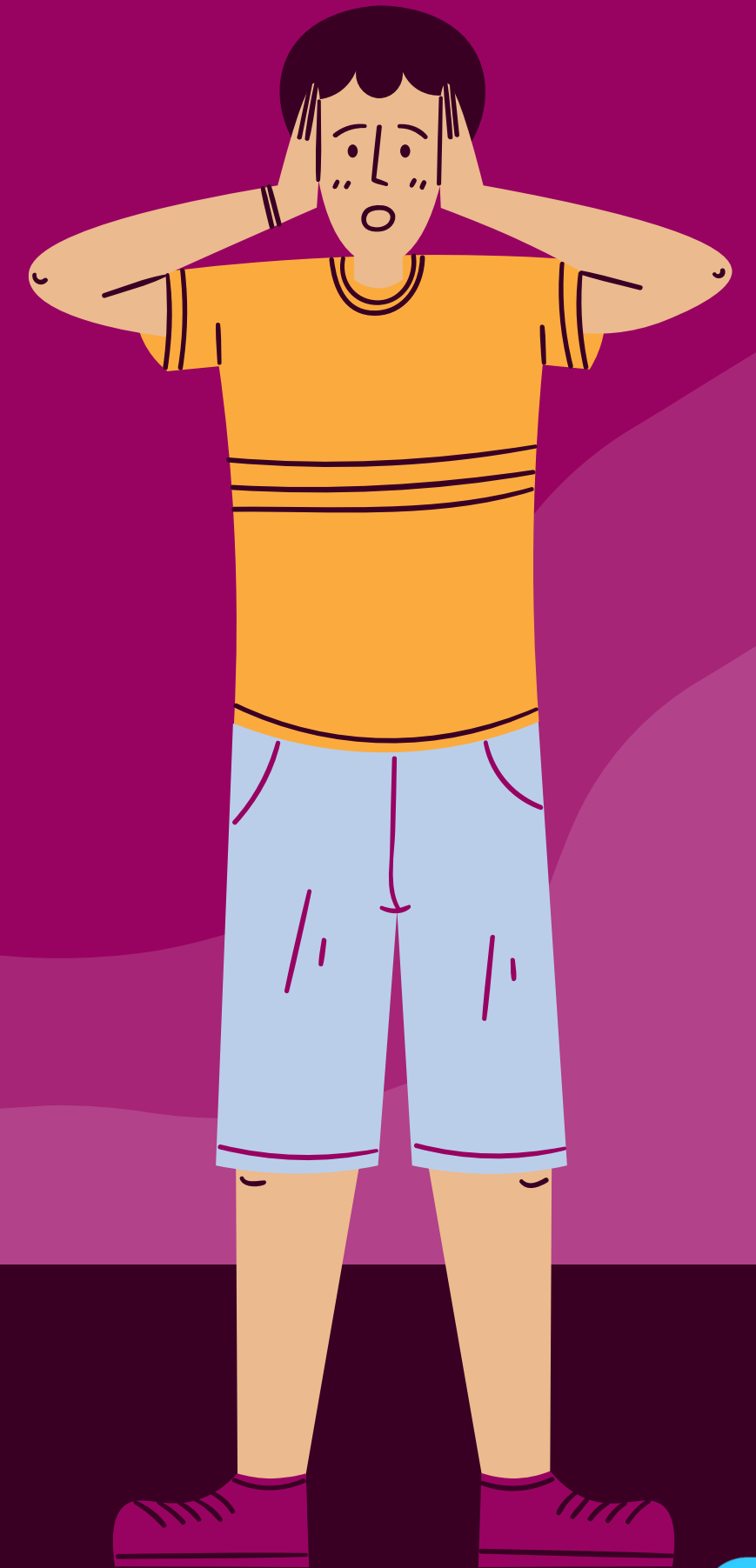


Messages asking for a loan, voting in a contest, a link to a "funny video" from one of your friends, participating in a raffle

Purpose: data from your social network account

Situation

In August 2019, Fstoppers reported on a phishing campaign launched on Instagram, in which scammers sent private messages to Instagram users, warning them of image copyright infringement and requiring them to fill out a special form to avoid getting banned. One of the victims received a private message from a supposedly official North Face account alleging copyright infringement. The victim followed a link in a message to a seemingly legitimate site, Instagram Help Notice.com, where the user was asked to enter their login credentials. The victim, trapped, eventually gave the hackers access to her account information and other personal data associated with her Instagram account.



Checklist: Am I protected from phishing?

Check which of the rules you follow regularly:

- ☒ *Check which of the rules you follow regularly:*
- ☐ *I never use the same passwords on different services*
- ☐ *I carefully check where I enter my login, password and payment information*
- ☐ *I use two-factor authentication*
- ☐ *I do not click on suspicious links*
- ☐ *I do not believe unreasonably good offers*

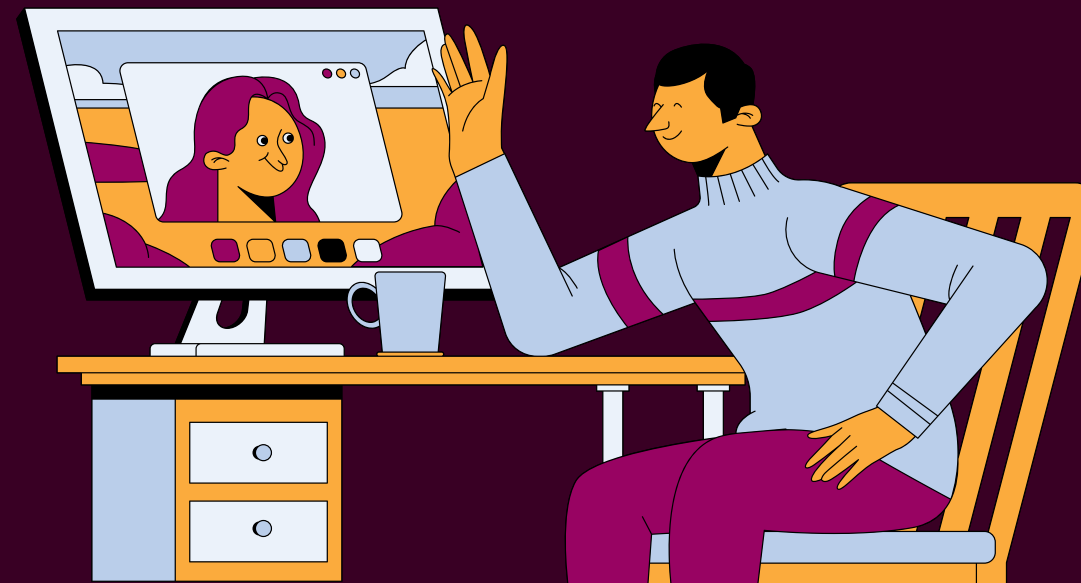


— fake social media profiles that can be used to extort money and personal data from social media users



Online stores and fake charities

- check information about promotions on the official websites of stores and charities
- large stores are unlikely to send news about the draw through social networks



Accounts for extortion and involvement in the financing of terrorism

- check the activity on the page - posts should be published at different intervals (not 10 posts in 1 day), and likes / comments should correspond to the number of subscribers



Celebrity accounts

- check if the celebrity page is verified - trusted profiles are marked with a blue checkmark
- check profile creation date and post originality



Key Threats in Online Games



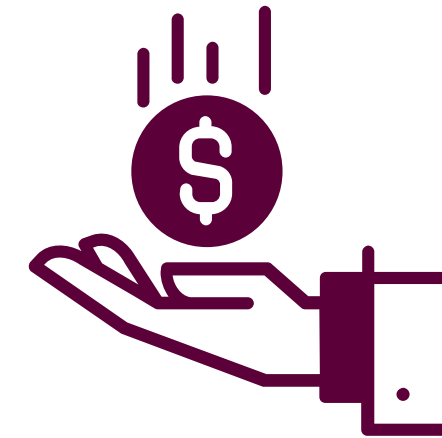
Identity theft

personal data is a direct access
to the wallet



Personal data is a direct access to the wallet

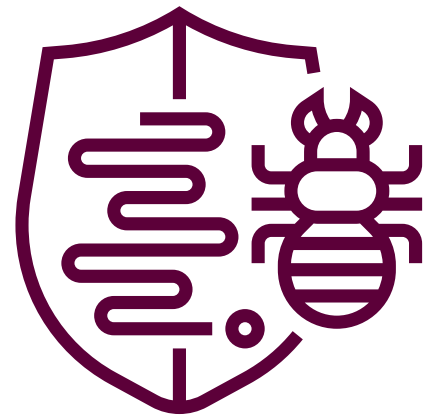
after stealing an account,
scammers begin to blackmail the
user, demand money for a
refund



Cash theft

about half of the fraud cases at
the time of opening an account
to pay for game currency,
purchase add-ons, launch the
game

Key Threats in Online Games



Malware Injection

the user is prompted to download the plug-in for the game by clicking on a link to another site where the malware is running



Breach of privacy

Intruders can gain access your other accounts, register new accounts in your name



Hidden fees

to get access to all the features and functions in the game, you need to pay by linking a bank card to your account, payment is made automatically

Akram, 20 years old



Assignment

1. Read the text on the next slide.
2. **What happened next?**
Assume further developments based on your knowledge of possible fraud in online games.
3. What conclusions can be drawn from the situation?

Situation

"When I was a schoolboy, I found some server in 'Counter-Strike: Source' where there was a dude in the Iron Man skin. When he died, his ragdoll made cool metallic sounds – anyway, I was impressed. I asked at in a general chat how to get such a skin, and the server admin replied that the model is available only for admins, but offered it for nothing. He activated the skin for me on the server, and everything seemed to work fine, but then he wrote that the model, needed to be activated on Steam to keep it from disappearing. At his request, I installed TeamViewer and gave access to the computer. He connected, opened Notepad right on my desktop, and wrote what to do to activate the skin."



**Akram, 13 years
old**



Organizations that protect the rights of citizens in the financial sector

1 Central bank

2 Antimonopoly authorities

3 Internal affairs bodies,
police

4 Prosecutor's Office

Let's summarize:

What should not be indicated on your social network page? Select several options

- a) information about relatives.
- b) geotags .
- c) telephone number.
- d) first and last name.
- e) full address of residence.
- f) all of the above.

What criteria can be used to recognize a fake account? Select several options.

- a) there is no blue tick next to the nickname.
- b) this person is not familiar to you.
- c) a person has a lot of followers, but very little activity on the page.
- d) the profile was created recently and there is only one photo in the feed.
- e) the profile of the page owner is confirmed, but the avatar has flowers, not a photo of the page owner



International Financial Security Olympiad



Ministry of Education
of Russia



Ministry of Education
and Science of Russia



Rosfinmonitoring

29



RUDN
university





Olympiad Goals



- ✓ Improving the general information, financial and legal literacy of young people, shaping a new form of thinking and a new format of activity, identifying talents in the field of financial security
- ✓ creating conditions for an individual educational trajectory, promoting vocational guidance of students to form the human resources of the financial security system;
- ✓ stimulating educational, cognitive and research activities of students, developing scientific knowledge in the field of financial security.

Olympiad Pathway

Thematic lesson on financial security

① INVITATION STAGE OF THE OLYMPIAD

- held on the platform and website of the Olympiad
- Deadline is April 7, 2023.

② PRELIMINARY STAGE OF THE OLYMPIAD (university)

- is held at the sites of the universities participating in the International Network Institute in the field of AML / CFT
- Deadline is May 19, 2023.
- The winners get the right to participate in the next stages of the Olympiad

③ SELECTING STAGE OF THE OLYMPIAD

- sending motivation letters (essays)

④ FINAL STAGE OF THE OLYMPIAD

- held on the federal territory "Sirius" (Sochi, Russia)
- Date: October 2-6 , 2023
- winners and prize-winners are granted additional rights upon admission to higher education programs





We invite you to participate:

Students of educational organizations from Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Armenia, Brazil, India, China, South Africa, Russia, Iran, Pakistan, Namibia



RUDN
university



Ministry of Education and
Russia



Ministry of Education and
Science of Russia



Rosfinmonitoring

More information:

www.fedsfm.ru - Rosfinmonitoring

www.mumcfm.ru - ITMCFM

www.rudn.ru – RUDN University

rosfinolymp.ru - website of the Olympics

E-mail: olimpiada@mumcfm.ru