

## **DATA SECURITY ISSUES**

Today we live in the information age. It is a period of history when information is easy to access and it affects many aspects of everyday life. The majority of our personal identifying data is online. In social media accounts any type of personal information can be easily found: a person's education, outlook, location, favorite food, etc. None of us is immune to personal information leaks. This article is an attempt to enlighten the issues of personal data security and to analyze the real situation of security vulnerabilities. To give an idea how serious the problem is, here are some examples of cybercrimes and fraud committed in the last two years.

First of all it is worth mentioning that the COVID-19 pandemic has provoked an unprecedented increase of cybercrimes and fraud. In 2020, only on the territory of the Russian Federation 510.300 episodes of cybercrimes were reported [1]. The detection rate of them was less than 25%. The Heads of such corporations as Facebook, Apple, Google and Amazon were accused of collecting and manipulating personal data for the gain of money. In July 2020, they were interrogated in the US Congress and this process was widely covered by the media [2].

Nowadays the situation is drastically getting worse. The amount of cybercrimes and their variety are constantly increasing. Even if to trace these changes by the latest headlines in mass media it becomes clear that the problem of personal data security is very acute:

*Opera News*: "Personal data of 4.6 million customers of Neiman Marcus department stores were leaked in the U.S." 03.10.2021 [3];

CNews: "A subsidiary of anti-virus software developer Avast received millions of dollars for selling user data." 28.01.2021 [4];

The constituent part of everyday life in the information age is the usage of IDs, passwords, and personal identification numbers (PINs). They are required for such activities as using ATMs and debit cards, logging in to Windows, accessing wireless networks, making an iTunes purchase, instant messaging, etc. And it goes without saying that personal identity data security matters like never before. In fact, the authentication protocols - any method that confirms a person's identity using something the person knows, possesses, or something the person is - are getting more complicated every year. But alongside with this fact, according to the survey conducted by "The Deloitte", 91% of the users accept willingly terms and conditions without even reading them [5].

Nowadays underestimating the importance of information security may lead to serious losses. To protect personal data several important steps should be undertaken. The widely spread and commonly known are: to install security software from a reliable company; to set the operating system and the web browser to update automatically; not to buy security software in response to unexpected calls or messages, especially if it is said that the computer must be scanned; to update and backup the data regularly; to keep safe and protect passwords and user IDs; always read the privacy policy.

Any personal data may become the subject of unauthorized access as hacking techniques change rapidly and their productivity is immense, but by following the basic rules it becomes possible to maintain security as well as to protect privacy against unwanted attempts to access data. Getting started is easy.

## References

1. Article: Number of cybercrimes in Russia [Electronic resource]. — Mode of access:

[https://www.tadviser.ru/index.php/Статья:Число\\_киберпреступлений\\_в\\_России](https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России). Date of access: 12.12.2021.

2. Apple, Google and Facebook were interrogated about "killing competitors.". [Electronic resource]. — Mode of access: [https://www.rbc.ru/technology\\_and\\_media/30/07/2020/5f21f8e59a79470797bd8904](https://www.rbc.ru/technology_and_media/30/07/2020/5f21f8e59a79470797bd8904). Date of access: 12.12.2021.

3. Personal data of 4.6 million customers of Neiman Marcus department stores were leaked in the U.S.. [Electronic resource]. — Mode of access: <https://www.dailyadvent.com/ru/news/3ff04a9604b87b30e41525cb79537480>. Date of access: 12.12.2021.

4. A subsidiary of anti-virus software developer Avast received millions of dollars for selling user data. [Electronic resource]. — Mode of access: [https://www.cnews.ru/news/top/2020-01-28\\_sozdateli\\_znamenitogo\\_besplatnogo](https://www.cnews.ru/news/top/2020-01-28_sozdateli_znamenitogo_besplatnogo). Date of access: 12.12.2021.

5. 2017 Global Mobile Consumer Survey: US edition. [Electronic resource]. — Mode of access: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf>. Date of access: 13.12.2021.