УДК 004.056

THE ROLE OF PERSONAL INFORMATION SECURITY IN SOCIAL NETWORKS NOWDAYS

M. O. Chueva, A. R. Thurmanidze, N. A. Slobozhanina

This article highlights the importance of information security in social networks and the various threats that us-ers may face. A survey of 50 students showed that a significant number of them had experienced hacking of social networks, and only a few knew how to protect themselves online. The article gives tips on how to protect yourself from intruders and improve security and privacy. Tips include using strong passwords, enabling two-factor authentication, being careful when clicking links, updating software, and using antivirus software. Following these tips, social media users can reduce the risk of becoming victims of online threats.

Keywords: Internet; security; privacy; hackers; intruders.

Currently, information security plays a big role in our lives. Due to the development of human information capabilities, the role of information security is increasing. More and more people are facing hacking and theft of their personal data on social networks. Attackers are constantly developing malware so that it is not detected by classic security tools: antiviruses, firewalls, IPS, mail and web gateways [1].

Vkontakte is one of the largest social networks in Russia. A large number of users entails the appearance of a large number of scammers who are ready to steal and sell the accounts or groups of users of this social network. In January 2022, thousands of VK accounts received a phishing newsletter leading to an application that allegedly shows dirt on the account owner. Phishing attack is the issuance of fake websites that mimic the Internet pages of popular companies and are used to steal passwords, card numbers, bank accounts and other confidential information. It is one of the most common ways to steal credentials. When you enter a corresponding query in any search engine, you can find various instructions for creating phishing pages for VKontakte, that is, anyone can, using the instructions in the public domain, become a potential attacker.

But often cases of data theft occur due to inattention and ignorance of Internet users. People themselves can transfer their personal information to intruders who rub themselves into trust for the sake of obtaining it. Many people simply do not know the rules of behavior on the Internet and therefore get into unpleasant and sometimes dangerous situations.

And there are a lot of such cases, so the purpose of our project is to detect the level of competence of users of social networks in the issue of information security.

To achieve this goal, the following tasks were set.

1) To collect and systematize information about the importance of information security: types of threats on the Internet and ways to protect against intruders.

2) To conduct a survey in order to find out the percentage of people who have been exposed to hacking or other harm on the Internet, as well as to understand the level of awareness about Internet security rules.

3) To analyze the data obtained by questioning students and give advice to prevent hacking in the future.

By completing all these tasks, we will help readers understand the security and privacy

Chueva Maria Olegovna (marybelka04@gmail.com), 2nd year student;
Turmanidze Artur Roinievich (Pro100biv@mail.ru), 2nd year student of the Institute of IT and Cybernetics;
Slobozhanina Natalia Aleksandrovna (slobozhanina.na@ssau.ru), associate professor of the Department of Foreign Languages and Russian as a Foreign Language of Samara University,
443086, Russia, Samara, Moskovskoye shosse, 34.

concerns of social media users, as well as provide some steps that will help social media users improve security and privacy.

Theoretical part

To delve into this topic, it is worth understanding what is information security? Information security is a set of organizational and technical measures to prevent unauthorized use, distortion, copying, research, recording and etc. of data arrays. Thus, threats to information security are various events, processes or actions that can lead to violations of the information security status.

There are two types of threats to information security: natural and artificial. Natural can include everything that is not controlled by a person: fires, earthquakes, etc. Artificial ones include those that depend directly on a person. Artificial threats depend directly on the person and can be intentional and unintentional. Unintentional threats arise due to carelessness, inattention and ignorance. An example of such threats may be the installation of programs that are not among the necessary ones for operation and further disrupt the operation of the system, which leads to the loss of information. Deliberate threats, unlike the previous ones, are created on purpose. These include attacks by intruders both from outside and from inside the company. Intentional threats include hacking of social networks, fraud, data leakage and loss, virus programs, spyware, as well as spam, etc. A comparison diagram of the most dangerous threats to information security can be seen in the fig. 1 [2].

The main sources of threats are individual attackers ("hackers"), cybercrime groups and state special services (cyber units). In order to break through the protection and gain access to the necessary information, they use weaknesses and errors in the operation of software and web applications, resort to listening to communication channels and more. The main threats to Internet security are malicious links, hacking of social networks and password theft, as well as viruses [3].

Violation of the information security regime can be caused by both planned operations of intruders and inexperience of users. The user must have at least some idea about information security, malicious software, so that his actions do not harm himself. But unfortunately, sometimes huge number of people does not even know what to do to protect themselves from malicious attacks.

We were interested in the fact that some people do not know the basics of behavior in social networks. Therefore, the question arose: how well do modern young people, in particular students, know the rules of behavior in social networks and on the Internet in general?

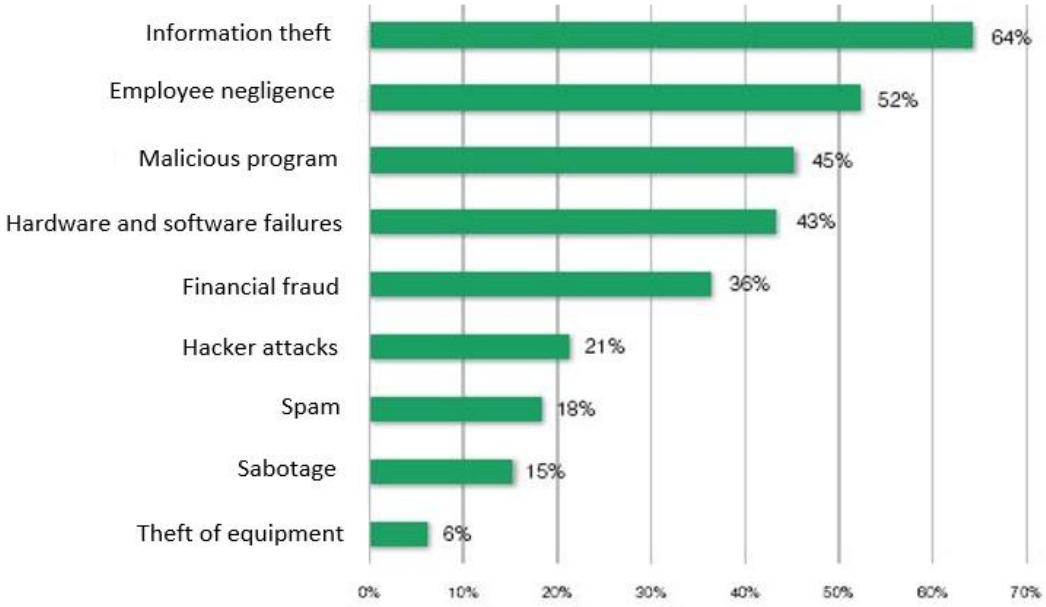

Fig. 1. The most dangerous threats to information security

Practical part

We decided to conduct a survey on the role of information security in our world. We want to understand how people view the importance of information security for themselves and others. With the help of this survey, we will try to clearly understand the importance of information security for various people, compile statistics and identify the main problems that users of social networks are coping with.

The survey was created based on the Google Forms platform and questions were asked in several directions:

• How often have you encountered hacking of pages on social networks?

• What consequences of hacking have you had?

• Do you know how to protect yourself from attacks on the Internet?

• What measures do you take to protect data on social networks?

• What advice can you give on how to stay on the Internet safely?

50 students from different directions and courses of our university took part in the survey. Thanks to their help, we got interesting results, which were recorded in charts, which were subsequently analyzed. The charts below (figures 2, 3) show the percentage of responses of the surveyed people.

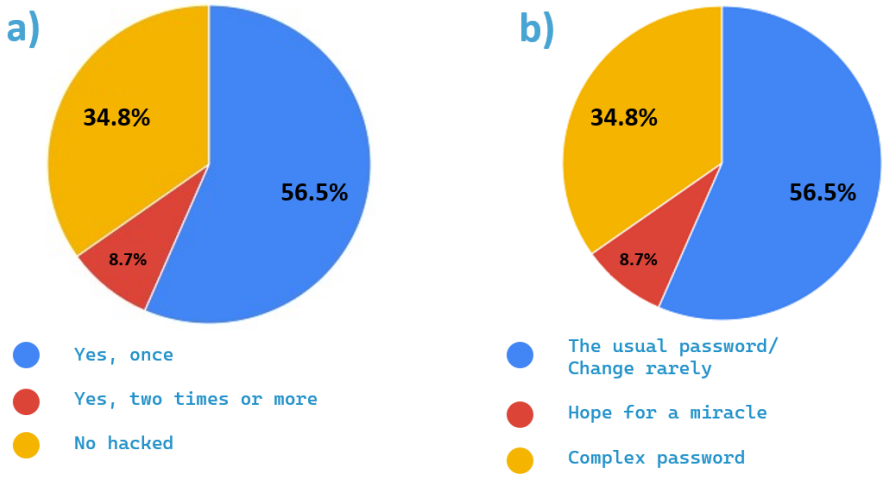

Fig. 2. The results of the survey of students:
a) How often have the surveyed encountered hacking of pages on social networks?
b) What measures do the surveyed students take

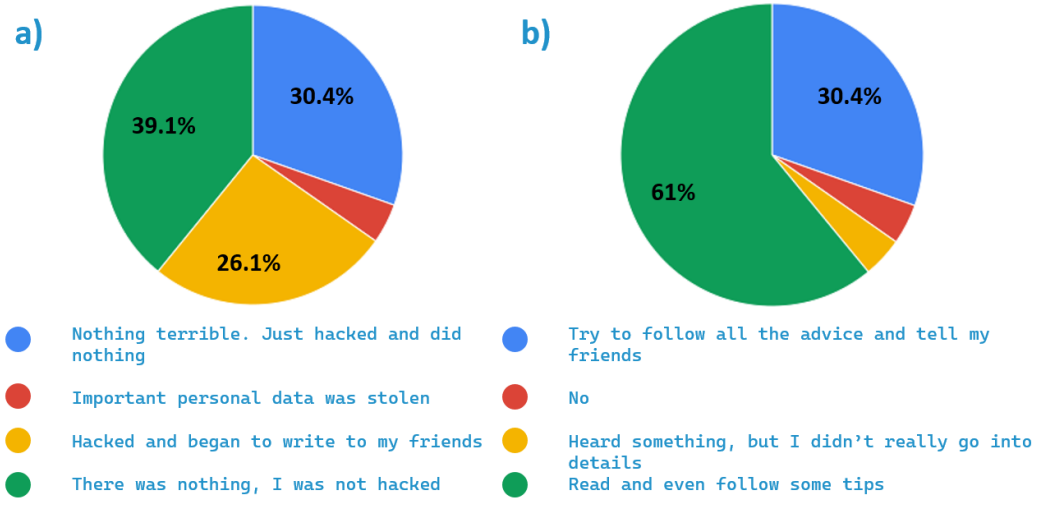

Fig. 3. The results of the survey of students:
a) What consequences of hacking attacks did the surveyed students have?
b) Do the surveyed students know how to protect themselves from attacks on the Internet?

The results of the survey

According to the results of the survey, we have the following:

• 65% of the surveyed students have experienced hacking on social networks, of which about 8% of students have been subjected to another hacking.

• Of all the students who were hacked, about 10% were exposed to identity theft, such as phone numbers or personal passwords. On the accounts of the remaining hacked students, which is 90%, the attackers wrote to friends or sent suspicious links.

• Only 10% students do not know how to protect themselves online – most of them try to follow some tips, but do not use all security measures.

• 34% of respondents set themselves a complex password and often change it, 56% have a cloud password and rarely change it, the remaining 10% treat any protection with disdain.

• Most students are advised to change passwords frequently, not to follow strange or unfamiliar links, use two-factor authentication, be extremely careful with unlicensed programs, and also not to store all passwords in one place and, if it is possible, to use different passwords on different social networks.

Based on our survey, we found out that most of the interviewed students were hacked on social networks and then subjected to some kind of damage. The majority of students know about basic security measures on the Internet but neglect them and hope for good luck. It is worth noting that a small percentage of respondents are responsible for their safety and try to use all methods to avoid unpleasant cases.

Conclusion

Summing up, we can say that often people are just too lazy to follow safety tips, in their opinion it is very tedious and pointless to constantly change the password, but if they are hacked, they do not even think that they need to take stronger security measures. And, unfortunately, there are a lot of such cases, and scammers take advantage of this.

However, there are people who simply do not know safety rules and suffer from attacks due to ignorance, so we decided to take the following elementary precautions.

1) Be vigilant and do not click on unfamiliar or strange links, for this reason there is a greater number of hacks.

2) Set long and complex passwords, and also do not use the same password on all accounts or applications, because if one application is hacked, you risk losing access to all social networks.

3) If the program makes it possible to enable two–factor authentication, then be sure to do it, because in case of a hacking attempt, you will be notified and will not be allowed to log into your account just like that.

4) Buy and download only licensed programs, as there are cases when a free but unlicensed program may contain a virus.

5) Also do not connect to free Wi-Fi in public places, because attackers specifically use your naivety to steal personal data.

6) Keep all your passwords in safe and inaccessible places. Do not send passwords, usernames, passport data, PIN codes and other similar information in messengers, chats or by e-mail.

7) Login in the form of first name, last name and password type 1234 or QWERTY is not the best idea. If someone seriously decides to steal your confidential information, he will split such a "protection" in two accounts.

8) Before accepting another confirmation of "friendship" in social networks, carefully study the account of the person asking to "make friends". If the account of a new "friend" is closed from access to "non–friends" and you cannot form a preliminary opinion about this person - immediately refuse friendship.

By following these tips, you will greatly reduce the risk of being hacked and will be able to safely use your social networks. Do not neglect these tips, because they will help not only to spend time on the Internet calmly and without unpleasant incidents, but also reduce the risks of dangerous situations.

Thanks to all the completed tasks, we were able to achieve the goal of our research, or rather to study the role of information security in social networks and to give some advice to internet users.

References

1) Hiatt D. Role of Security in Social Networking // International Journal of Advanced Computer Science and Applications. 2016. Vol. 7. № 2. P. 12–15. Doi: 10.14569/IJACSA.2016.070202.

2) Угрозы информационной безопасности [Электронный ресурс]. URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 20.06. 2023).

3) Das R., Patel M. Cybersecurity for Social Networking Sites Issues, Challenges, and Solutions // International Journal for Research in Applied Science & Engineering Technology (IJRASET). 2017. Vol. 5 (IV). P. 833–838.

РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛЮДЕЙ В СОЦИАЛЬНЫХ СЕТЯХ В НАШЕ ВРЕМЯ

М. О. Чуева, А. Р. Турманидзе, Н. А. Слобожанина

В этой статье подчеркивается важность информационной безопасности в социальных сетях и различные угрозы, с которыми могут столкнуться пользователи. Опрос 50 студентов показал, что значительное число из них сталкивались со взломом социальных сетей, и лишь немногие знали, как защитить себя в Интернете. В статье даются советы о том, как защититься от злоумышленников и повысить безопасность и конфиденциальность. Советы включают использование надежных паролей, включение двухфакторной аутентификации, осторожность при переходе по ссылкам, обновление программного обеспечения и использование антивирусного программного обеспечения. Следуя этим советам, пользователи социальных сетей могут снизить риск стать жертвами онлайн-угроз.

Key words: интернет, безопасность, конфиденциальность, хакеры, злоумышленники.

Статья поступила в редакцию 30.06.2023 г.

Чуева Мария Олеговна (marybelka04@gmail.com), студент II курса,
Турманидзе Артур Роиниевич (Pro100biv@mail.ru), студент II курса института информатики и кибернетики,
Слобожанина Наталья Александровна (slobozhanina.na@ssau.ru), доцент кафедры иностранных языков и русского как иностранного Самарского университета,
443086, Россия, г. Самара, Московское шоссе, 34.