Information security in social networks/ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Меркулов А.В.

иностранный язык

11 класс МАОУ Академический лицей, г.Магнитогорск Челябинской области

Научный руководитель: Кошелева Т.А., МАОУ Академический лице. г. Магнитогорск Челябинской области

Relevance.

The peculiarity of modern society is in its informatization. It means active development and implementation of information technologies into all spheres of human activity. Information and information resources are the determinants in the development of an individual, society and state. Modern computers and information technology have broad capabilities.

It allows automating the monitoring and management of the state, economic, social, defense and other facilities and systems. We can receive, accumulate, process and transmit information about these processes at almost any required speed, in any quantity.

All this information is significant for different structures. Of course, keeping this information secret is also very important. Information security as science is trying to solve this task.

The problem that prompted me to write this article is that young people underestimate information security while using social networks.

The purpose of my work is to study the problem of information security and find out possible ways to protect social accounts against hacker attacks.

The tasks of the work are:

1. To consider social networks as a means of conveying information.
2. To explore the security of sharing information in social networks.
3. To demonstrate an example of "hacking" an account.
4. To propose ways of protection against hacker attacks.

Hypothesis: these days, even a schoolboy can obtain personal data from other people's social networks.

Research methods: literature analysis, the generalization of the knowledge gained.

Social networks

In the modern world, young people are increasingly communicating through the Internet, most often through social networks.

A social network is a platform, online service or a website designed to build, reflect and organize social relationships on the Internet [1]. These are platforms where people of the same interests come together.

At the moment, people mainly exchange information through social networks, because you can do it without being tied to a specific place and time. Technology makes it possible to exchange information from anywhere in the world.

Social networks security

People transfer gigabytes of information through social networks to each other every day without thinking that the channels of the most social networks are not secure enough to transmit this information.

Let us talk about social networks at the moment in the Russian Federation. We can say that the communication channel reliability is strongly questionable since, at the moment, government services can get the keys to people's correspondence.

When studying the issue of transferring information over the Internet, the question often arises of the protection against hacker attacks on people's pages in social networks. It happens so that the only obstacle to the personal data of users is a

login and password. It is not a reliable method of protection, because more and more often there are cases of "hacking" of user pages by a simple search of all kinds of passwords to the account.

At the moment, there are several ways to gain access to a user account:

- **Fishing**

It is probably, the most common method of hacking social woks pages. For example, a hacker can create a page identical in structure and design, on which the site asks for your username and password. As soon as you enter it, the attacker gets your data. Although many users are already quite literate and can distinguish the address of a phishing site from a real one, do not forget that there are amateurs who, having seen a similar design, begin to trust the fishing site.

Before entering personal data, make sure that the site address matches the original.

- **Keylogger**

This method is probably the easiest of all. And besides, it is the most dangerous one, since even an experienced user can fall into the trap of a hacker. A hacker installs a program on your computer that starts recording absolutely everything that you enter on the keyboard and sends this data to the hacker. The hacker doesn't even need to have access to your computer to install such a program. All he needs is to force you to run the file you receive from him under some pretext.

Of course, an experienced user will not run any unknown programs. But we all have relatives or friends, and they can willingly run a file called "photo.exe" or something like that.

Do not download files from suspicious sites or files that you receive in your social networks, and if you do download them, then always pay attention to the extension.

- **Stealer's**

Many people use the "remember password" feature in the browser. It prevents them from the need to enter a password every time they log into their account. It is quite dangerous if an attacker can install a program that will take data from your browser and send it to the attacker.

- **Hacking a mobile phone**

With so many people using their phones to access their social networks, it becomes easier to hack them. If a hacker gains access to your phone in any way, he will be able to gain access to your page on social networks. There are many different tools and apps for tracking someone's smartphone. For example, Spy Phone Gold and Mobile Spy.

- **Fake DNS method**

The method will only work when the victim and the hacker are on the same network. This method allows the hacker to create a fake login page, and as a result, the hacker will receive the data entered by the user and, therefore, access his page.

- **Gaining access to an account via access_token**

For a demo example of "hacking" a social network page, we chose to scan information from a user's account using access_token.

Token, also known as access_token, is an especial access key. It is a combination of Latin letters and numbers. Having a questionnaire token, you can use it to access the corresponding sections of the page. There are many services for obtaining an access_token, the most popular of which is github.io
With the help of a token and a program that uses ready-made API libraries provided by the social network, you can use some of the functions of the user page:

1. "Catching" messages arriving at a given time
2. Sending messages to users
3. Receiving and saving the histories of all user correspondence

4. Gaining access to all albums and audio recordings of the user (including hidden ones)
5. Receiving all attachments of the user's correspondence (including voice messages)
6. Management of groups in which the user has administrator rights

We should understand that when the attacker receives an account token, he cannot go through the usual authorization with a username and password. The access_token allows using the program code to send requests to the social network server to execute the given commands.

This method has an advantage. When the attacker uses the software, no authorization in the social network occurs. It means that it is almost impossible to catch the attacker. But at the same time, it is also a disadvantage of the method because software control does not give full access to the page, which you get through the usual way of logging into your account.

Ways of protection against hacker attacks

To avoid an attack on your page by hackers, you should follow several rules:

1. Do not transfer your data to anyone on the Internet.
2. Do not follow suspicious links and do not download suspicious files from the unknown sources.
3. If you suspect malicious activity on your page, change your account password and end all the sessions associated with it.
4. Regularly check your device for malware or viruses.
5. Periodically check the devices connected to your account. Complete all work sessions, if required.

Conclusion

In this article, we studied the following concepts:

social networks,

social network security,
hacking,
access_token.

In the course of studying these materials, we came to the following conclusions:

1. It is impossible to imagine the modern world without communication through social networks. People exchange information every day, not always realizing that transmission channels have got low protection.
2. At the moment, the sphere of hackers is flourishing. Many of them are hacking users' pages on social networks to obtain personal information.
3. There are many ways to access and control the victim's page.
4. To save your page, you should follow several rules: set only secure passwords on pages, monitor your activities on a social network (do not click on suspicious links, do not download unfamiliar files).

The main conclusion of all our work done is that the current systems for protecting personal information on social networks are highly unreliable. It is necessary to monitor the integrity of the user's data very carefully monitoring Also, we realized that our work is relevant and modern, because IT technologies today are not a fashion trend, but a necessity.

Список литературы

1. Филимонова Е.В. Информационные технологии в профессиональной деятельности: Учебник. – Ростов н/Д: Феникс, 2004. – 352 с. (серия «СПО»).
2. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.
3. Башлы П.Н. Информационная безопасность / П.Н. Башлы. —Ростов н/Д: Феникс, 2006. — 253 с
4. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006.