# THE PROBLEM OF MODERN METHODS SOCIAL ENGINEERING

***Abdurazaqova Gulginaxon Murodjon qizi***
*Tashkent named after Muhammad al-Khorazmi Student of the Fergana branch of the University of Information Technologies*
***Ibrohimova Nafosatxon Pahlavon qizi***
*Tashkent named after Muhammad al-Khorazmi Student of the Fergana branch of the University of Information Technologies*
***Abduxalilova Sevaraxon Nodirbek qizi***
*Tashkent named after Muhammad al-Khorazmi Student of the Fergana branch of the University of Information Technologies*

**Annotation:** This article discusses the problems of modern methods, social engineering. This study aims to explore the methodology. It contains recommendations to help prevent data leaks in the work of people with social engineering skills.

**Keywords:** Social engineering; VPN; about; the face; good knowledge of social engineering methods.

In the modern world, such a resource as information is of great importance. It has great value for the person or business that owns it. In case of leakage of valuable information, its owner will suffer a great loss and in many cases it will lead to the loss of all the materials they have. Too many losses also change the normal work rhythm of employees. Currently, in order to keep valuable information confidential, various software and hardware protections are being developed that minimize the possibility of data leakage from electronic computing devices. However, regardless of how reliably the system is protected, the main reason for the spread of information is the people themselves. As a result of not carefully using all the devices that a person uses, they create a great opportunity for attackers to easily steal data from them. This is one of the main reasons why all protected information is leaked. This approach to obtaining protected information is called "social engineering". This article discusses social engineering, as well as modern methods and their implementation.

First of all, we need to understand what social engineering is and define this concept. Social engineering is a method of accessing protected information without the use of technical means. The meaning of the key phrase in this definition is "lack of technical means", that is, with the help of a knowledgeable person. For this purpose, it is used for its purpose by influencing a person mentally, gaining his trust. Social engineering is currently affecting many people. People who are easily fooled by the tricks of attackers are mostly suffering from their pity or negligence. Their main weapon is to win the person's trust and easily ask him for the necessary information.

In today's society, almost everyone uses the Internet, so this is where most fraudsters use social engineering techniques. They create such conditions of anonymity for themselves that it is almost impossible to identify them if they are searched. To achieve this, individuals who use social engineering work with virtual private networks (VPNs), the anonymous browser Tor, as well as operating systems created all for anonymity. Identifying the workplace of a social engineering user is as follows:

1. Using the bootloader, an operating system is launched for user anonymity (for example, Tails OS).

2. Connects to a VPN (mainly buys paid access to foreign networks of countries that prioritize user privacy, thereby minimizing the possibility of disclosure. Law enforcement authorities of the connected real IP address are minimized).

3. With VPN, you connect to Tor browser servers. The Tor browser connects to three servers in different countries, and each server has a hierarchy that is structured in such a way that from a lower-level server to a higher-level server, access is not possible. This approach increases anonymity many times.

4. After connecting to Tor servers, connect to another VPN located in another country.

Thus, the workplace of a person who uses social engineering is ready. It should be taken into account that all traffic circulating in this chain must be encrypted, which increases the user's anonymity.

Currently, people who use social engineering work according to the following scheme. A scheme is a described algorithm that includes aspects that allow it to find and deceive a victim. Schemes can be public (held in the public domain) or private (sold by creators for money). There are three types of schemes:

1. White scheme.
2. Grayscale scheme.
3. Black scheme.

Each type of scheme should be considered in more detail.

White scheme. It is characterized by the simplicity of its actions. Anonymity is not required for implementation. As a rule, to implement a white scheme, it is enough to convince the victim that your actions will benefit him. Let's look at an example of a white scheme. You want to spread a remote access virus to the victim's computer. For this, people who use social engineering methods look for people who use computers at the level of ordinary users and cannot understand that the downloaded file of the resolution they need is an executable file. For example, Photoshop users who download additional content every day, a person using social engineering searches for groups in the social network "VKontakte" where such additions are posted, and then uploads a file created there using special software with his permission. It corresponds to a Photoshop file, but in fact it is an executable * .exe file (often it uses cryptography so that antiviruses do not perceive it as a virus). Success in terms of downloads, the main achievement is a well-written and attractive description. This ability is used by social engineers. After installing an additional system, a person using social engineering skills gains access to the victim's computer and uses it for his own needs. In this case, the victim will not be financially harmed.

Gray scheme. Some anonymity is required (a VPN will suffice). The difference between the gray scheme and the black scheme is the minimal, i.e. imperceptible, damage caused to the victim. As a rule, in this scheme, the victim does not understand that he was deceived, so there is no need to wait for punishment. Let's look at an example of this scheme. A group is being created on the VKontakte social network, where photos of clothes are posted, and the price list for them is the same, but much lower than the originals. A person using social engineering techniques advertises the group in such a way that people trust him and make payments. For this, fake screenshots of satisfied customers are created and advertising for this store in other groups is purchased. After attracting the audience, the person using the social engineering technique will sell the existing product and assure the customers that their order has been shipped and will arrive within certain days. Once the amount of money to be collected is reached, the social engineer stops responding to messages and completely forgets about this group. Money is taken, users wait and do not realize that they have been cheated.

Black scheme. Complete anonymity is required. A large amount of money was involved. Applications are written to the authorities and identity searches are carried out using social engineering methods. Let's look at an example of a black circuit. In this case, the topic of "irrevocable" loans is presented. A person really likes to get money without doing anything, so finding a victim is not a problem. Using social engineering methods, the person who finds the victim introduces himself as a bank employee and offers to get an "irrevocable" loan, after receiving the loan, he must delete his information from the database and assures him that it is not necessary to return it. At the same time, a person uses social engineering methods and receives a fee of 50% of the amount. The victim agrees to the money and sends the person all the necessary scanned information to get the loan using social engineering techniques. With the help of credit organizations on the Internet, he issues a credit card in the amount of, for example, 300,000 rubles, while using his fake SIM card to register it. The credit card is delivered to the victim's home by courier, and the person is contacted using social engineering methods. He assures you that you must give him all the information about the card, otherwise it will not be possible to remove the card from the database. The victim transmits all the information about the card, the person using social engineering methods cashes and hides the money through various cryptocurrencies, virtual money. As a result, the victim takes a long time to pay the debt, and the social engineer receives a large amount of money.

In conclusion, it should be said that there are many schemes for the operation of people using social engineering methods, and it is impossible to guarantee the safety of anyone. Learn to be alert without trying to achieve everything easily and get into the habit of earning money with your own efforts instead of hard work, don't install third-party programs. Otherwise, after receiving money easily, you may have to return the amount received many times, or your computer will perform illegal actions in favor of a person using social engineering methods.

## List of used literature:

1. Forum social engineering. URL: https://lolzteam.net/.
2. https://blog.hubspot.com/marketing/internet-marketing
3. Abramov A. V., Panasenko S. P., Petrenko S. A. VPN solution dlya rossiyskikh kompaniy // Confident. 2001. No. 1.