УДК 304.444:004

Kabak V., Monich K., Turchenuk M.

Social Engineering

Belarusian National Technical University
Minsk, Belarus

The success of communicating "correctly" for the Social Engineer, depends on acting and the ability to impersonate another person with previously stolen identities. In interpersonal communication the arsenal is replenished by such methods as body language, pathetic or menacing appearance, familiar uniforms, etc. Today let's talk about the importance of appearance, which will not arouse suspicion of the company staff.

Remember the meme about the two pranksters who were able to get into many closed places in the work uniform and ladder in hand? If you don't remember, I recommend you check it out. The bottom line is that the uniform is always credible, and few people wonder, "What is this person doing here?" And in vain, because he can do anything, including leave technical "bookmarks" and study the structure of the infrastructure. Accordingly, electricians, fitters, cleaners - all those who wear uniforms will be above suspicion.

Depending on the specifics of a particular organization, workers taking care of plants, servicing vending machines, etc. may be above suspicion. In general, those who provide/support the functioning of the office. Here we can easily pretend to be a representative of such personnel in order to get into the right part of the building. And if we consider that in a certain situation we can copy the badge of a real employee, then move around the territory of the organization will be easier at times.

In the pandemic, food delivery services, documentation, various goods and services, have reached a new level. An attacker can pretend to wait for a customer at the front desk, and at the same time set up a fake Wi-Fi access point, copy employee passes, etc.

Let me tell you a great example of the above: In front of the visitors, a man in work clothes removed the painting from the wall, took it behind a column, there took it out of its frame, and then leisurely followed the painting to the exit and left with it in a car.

Such examples are many, but it is worth remembering that this method involves a high risk of deanonymization, and the success rate of any attack depends only on the skill, the script and the level of preparation.
The fact that most people leave a huge amount of information about themselves on the Internet plays into the hands of social engineers. By the "digital footprints" of the victim, her pages in social networks the attacker can get an idea of the character, interests, habits of the person and use this data in the attack. The so-called OSINT.

Channels of communication for social engineering attacks can be any: email, messengers, phone calls, SMS messages.

There are various social engineering techniques:

Phishing. Fake website pages are one of the most popular methods of tricking users into obtaining personal or confidential information.

Pretexting. A social engineering technique in which an attacker introduces himself or herself as another person and uses a prepared script to lead the user to commit the action demanded of the fraudster or to reveal sensitive information.

Reverse Social Engineering. A technique in which the attacker forces the victim to seek his or her own "help". This method is used by cybercriminals posing as technical support staff. Such an attack takes place in several stages. For example,

the attacker first creates a reversible problem on the victim's computer. Then he somehow informs the user that he can solve such technical problems (by placing an announcement or his contacts near the user's workplace or where he is most likely to see them). After the user turns to him for help, the attacker solves the problem and at the same time gets the necessary access to the user's computer for his purposes.

There are a few simple rules that all users should follow.

- Never give out usernames and passwords for your accounts to anyone. Even if they try to convince you that an urgent and important task depends on it. Remember that bank employees may not ask you for your card number, CVV/CVC-code or other information that would allow writing off funds.
- Do not download attachments and do not follow suspicious links in the letters received even from the persons known to you. Always check using other available communication channels (phone call, messenger message) that the sender of the email is exactly the one he/she claims to be.
- Before clicking on a link in an email or message, hover your mouse over it to see the real URL of the page.
- Lock your computer when you leave your workplace.
- Use strong and unique passwords for various services. Use password managers.