SOCIAL ENGINEERING

Scherbachenko N.A., Rabkina S.A., Shelkovnikova S.V.
Don State Technical University
Щербаченко Н.А., Рабкина С.А., Шелковникова С.В.
Донской Государственный Технический Университет.

Abstract: Over time began to appear more and more new ways of social engineering. The term is used not only in a virtual network, but also in everyday life. Fraudsters have learned to manipulate people through confidential information from the World Wide Web, extracted by illegal.

Keywords: social engineering, fishing, darknet, Trojans, pretexting, reverse engineering.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Аннотация: С течением времени стали появляться всё новые и новые способы социальной инженерии. Термин используется не только в виртуальной сети, но и в повседневной жизни. Мошенники научились манипулировать людьми, посредством конфиденциальной информации из «всемирной паутины», добытой нелегальным путём.

Ключевые слова: социальная инженерия, фишинг, даркнет, клирнет, трояны, претекстинг, обратная инженерия.

Surely you are familiar with the term "social engineering". Usually underneath it understand human behavior manipulation for the purpose of obtaining benefits- money or sensitive information, certain services. Scammers always used social engineering, but the digital age has presented new opportunities. Cryptographer Bruce Schneier says, that the security situation in mathematics is flawless, computers are vulnerable, but people self-willed and hardly predictable [3]. Indeed, man is the weakest link in any system of protection, it is easy to hack, playing on emotions and weaknesses. And today we'll talk about methods that use social engineers.

Techniques of social engineers are diverse, applied and combined depending on the context. But they are united by one thing: cognitive distortions are at the core. That is human stupidity and inattention.

PHISHING is the most common method of online fraud. Every year it steals 3.5 billion rubles. Observance of elementary rules of cybersecurity rescues, but it happens different. So, in a darknet (a private network whose connections are established only between trusted peers, sometimes referred to as "friends", using non-standard protocols and ports), it's much easier to disguise the phishing site as legitimate because of their similar names. In 2017, the hacker Michael Rico just sowed the forums with links to fake trading platforms and received 365 thousand dollars in bitcoins from inattentive buyers.

A special kind of phishing in a darknet is the enticement of not-so-honest users into the clear (this traditional worldwide network has a relatively low basic anonymity, with most websites regularly identifying users at their IP address) via a special link to find out their IP address, and then blackmail.

Trojans are still used by scammers, but not so daring as in the 90s. Applications for smartphones of a sexual nature and tossed flash drives help to access the financial data of the victim, but not only. Spyware programs separate the list of contacts, the schedule of meetings, mail correspondence and other seemingly insignificant information. All in order for the fraudsters to play a whole play.

PRETEXTING is a method in which a fraudster collects information about a victim and her environment in advance, in order to pretend to be a person who can not be denied. Even small details are important: the name of a dead hamster, the number of the boss's office, the date of birth, and so on. In 2015, scammers on behalf of the top manager of Ubiquiti Networks demanded that their subordinates transfer $ 40 million. And they transferred. Psychologists have proved that under the pressure of authority we will go to anything [1]. According to the results of the experiment, 95% of nurses without questions will introduce a fatal dose to the patient if they are ordered by a doctor.

REVERSE ENGINEERING implies that the victim herself is seeking help from a fraudster. And then the principle qui pro quo (confusion) comes into play - as a reciprocal service the victim is ready to go even to a minor malfeasance. In the Cyber Security Championship, the task was: "What can I do in 2 minutes with the computer of a retired employee to then access the entire network?" The simplest solution is to attach a sticker with a phony phone number of technical support. After all, a sysadmin is the person who is trusted without a doubt, despite the safety technique.

Social engineering is everywhere - everywhere, where there is information, that is, in offline. Interesting tricks are used by the police, traders, journalists and ordinary fans of freebies. Law enforcement authorities are masters in the field of social engineering. They use it to obtain information when the law is being impeded on the way. "We are not accusing you of anything, just tell how it was ..." - the most common circumvention of Article 51 of the Constitution of the Russian Federation, which allows you not to testify against yourself. Another example is the prisoner's dilemma. This is when they tell you that the accomplice, friends, mom and even a dog have already said everything, it remains only to hear your version of events.

Another area of application of social engineering is advertising. And, despite the presence of more modern directions such as neuromarketing, the classic is always in vogue. Repeated pronouncing of information about the product, links to authoritative or expert opinion, exploitation of stereotyped images are the most popular tricks of advertisers. Obsolete, no doubt, but still effective. The media is also a fount of various social engineering techniques. Then you and the imposition of thoughts, and false cause-effect relationships, and manipulation of feelings, and substitution of concepts. In a sense, social engineering is the language spoken by propaganda. But do not be discouraged, social engineering skills can be useful to you personally. If you want a discount in the store, ask her directly and be sure to specify what you need to do for her. And then remind the seller of his right to refuse - this will increase the chances of success. If you want to get somewhere without a queue, just name any reason. Psychologists conducted an experiment: the girl asked to let her to the copier - she lost 60% of the people. When in another group she added "Because I'm in a hurry!" - she was already ceded 94% [3].

Areas of application of social engineering are endless. But to resist psychological pressure is actually easier than it seems. It is important to learn the important rule: when entering any type of communication, pay attention not only to the content, but also to the process itself. More often ask yourself the question: "What does all this mean?" Psychological games are different, but their essence remains unchanged. A critical attitude to incoming information, alertness and common sense will help you not to become a victim of social engineers.

Список использованных источников

1. *Semechkin N.I. Social Psychology. Textbook for high schools. St. Petersburg: Peter, 2004.*
2. *Zimbardo F, Leippe M. Social influence. St. Petersburg: Peter, 2001.*
3. *Schneier B. Secrets and Lies. Digital Security in a Networked World. Wiley Publishing, Inc. 2004.*
4. *Myers D. Social psychology. St. Petersburg: 1996.*