Research of Social Engineering Mechanisms and Analysis of Counteraction Methods

Vyacheslav Yu. Evglevsky[a], Michael M. Putyato[b] and Alexander S. Makaryan[c]
Institute of Computer Systems and Information Security, Kuban State Technological University, Krasnodar, Russian Federation

Keywords: Information Security, Cybersecurity, Social Engineering, Pre-Texting, Phishing, Vulnerability, Human Factor.

Abstract: This article provides an overview of various methods used in social engineering. Also, it examines various threats, their relevance and the harm that may follow after applying a particular method. The relevance of the chosen topic is due to the wide development of science and technology in conjunction with financial, economic and socio-political instability, which is a catalyst for the use of social engineering methods for personal gain.

1 INTRODUCTION

The essence of social engineering methods is the use of the human factor in attacks. Human's fears and weaknesses are manipulated with in such a way that a person produces the necessary action. According to sociology, social engineering is a set of approaches of applied social sciences aimed at changing organization and control over human behavior.

From the point of view of the subject area of information security, it is possible to narrow the definition of social engineering. It is an incentive to disclose confidential information or commit actions by a person using techniques of psychological manipulation.

Five main methods of social engineering are:

- pretexting;
- phishing;
- baiting;
- quid pro quo;
- reverse social engineering.

2 OVERVIEW OF SOCIAL ENGINEERING TECHNIQUES

Consider social engineering methods.

2.1 Pretexting

The pretext method can be described by the phrase "scare-save." After such an impact, victims very often make mistakes and thoughtlessly commit the actions indicated by the attacker. The actions of the attacker are carried out according to a pre-prepared scenario (pretext). The purpose is to provide the victim with specific data and perform the actions necessary for the attacker.

This method requires preparation - for the most successful attack, information about the object of attack must be collected. Information is usually collected from open sources.

Usually, such attacks are carried out using telephone communications, social networks, instant messengers or e-mail.

2.2 Phising

The phishing method consists in sending fraudulent messages, the source of which seems reliable to a

[a] https://orcid.org/0000-0002-5305-1544
[b] https://orcid.org/0000-0001-9974-7144
[c] https://orcid.org/0000-0002-1801-6137

Evglevsky, V., Putyato, M. and Makaryan, A.
Research of Social Engineering Mechanisms and Analysis of Counteraction Methods.
DOI: 10.5220/0010620000003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 140-144
ISBN: 978-989-758-531-9; ISSN: 2184-9862

victim. As a rule, phishing is a massive mailing on behalf of large brands, banks, payment, postal services or from other sources that are trusted by a victim. Usually such letters have the form of real notifications, almost indistinguishable from real ones. They contain a message and a link to a resource that is supposedly an original resource. The message in the letter prompts the victim to follow the link. On the site, under any pretext, the victim is encouraged complete the form by submitting confidential information.

2.3 Baiting

This method involves using various kinds of decoys to attract victims, with by exploiting their character traits, in particular, curiosity and thirst for easy profit.

There are two types of decoys - physical and virtual ones. An attacker lures the victim by affecting the above-mentioned human traits. Physical bait refers to a physical infected drive that the victim uses on his personal or work device and infects it. An entire enterprise network can be infected through a working device if the device is connected to it. In the case of virtual bait, malicious software is also launched, but only downloaded by the user from the Internet under one pretext or another, using messengers, social networks, fake Internet sites, advertisements or mailings directed to a malicious resource.

2.4 Quid Pro Quo

Quid pro quo is a method of social engineering, which consists in contacting the victim in order to obtain information in exchange for "help." As a rule, such appeals are made by phone or by e-mail and are aimed at attacking the enterprise.

2.5 Reverse Social Engineering

When making attacks using reverse social engineering, a sequence of actions is carried out that make a victim herself ask attacker for help.

The set of actions during the attack by reverse social engineering can be divided into three stages: sabotage, advertising and help. Sabotage is the first stage of the attack. The attacker purposefully organizes a problem in the attacked system, while this problem stops the operation of the object and the victim has no choice but to resort to help. For example, software problems are caused by a failure of software settings, malicious software or simulation programs are launched. The problems seem serious, but the attacker's task is to quickly fix them in further stages, so the problems which are created are not critical.

The second stage is advertising - the stage at which the attacker reports to the target of the attack that he can offer a solution to the problem and is ready to provide any help. At the same time, the attacker does not impose his services, he makes sure that the victim herself goes to him, giving information about himself in an open place. So there is an illusion of free choice.

The final stage of the attack is help when the attacker communicates with the object. The object receives a solution to the problem, and the attacker obtains the necessary information.

3 OVERVIEW OF ADDITIONAL TECHNIQUES

The publication Anti-Malware.ru provides techniques of social engineering, which with a high degree of probability, provide a successful outcome for the attacker to obtain unauthorized access to information.

3.1 Theory of Ten Handshakes

It is alleged that between the offender whose purpose is collecting data from a particular object and his victim there may be only ten "handshakes." As a rule, an attacker addresses employees who usually hold an ordinary but knowledgeable position (for example, a secretary). It helps the attacker collect data about employees higher in the job hierarchy. The goal is to convince the victim in that the attacker is either an employee of the organization or an authorized person (law enforcement officer or inspector) calls. The attacker gets the necessary information while communicating with a victim.

3.2 Corporate Language

The attacker can learn the corporate language. The vocabulary of the language consists of commonly used words and vocabulary of limited use - words known to not all speakers of the language. Each industry has its own vocabulary of limited use, there are its own specific definitions. The goal is to speak or write in the usual and familiar language of the victim, which helps to enter the trust and obtain the necessary information. The use of corporate language can be used in both pretexting and phishing, as it can help gain the trust of the victim.

3.3 Social Signals

To conduct an attack, attackers collect so-called "social signals" that help to enter confidence in the target of the attack. This can be a recording of music that the company turns on while waiting for a call. A social engineer records it and then uses it to his advantage. In particular, it is possible to use in pretext, reverse social engineering and in service-for-service attacks.

3.4 Spoofing

When using phone calls in an attack, the attacker uses the means of replacing the phone number (spoofing) - as a result of the substitution, the victim will display a number that she considers trustworthy.

3.5 News Against the Victim

As a bait for phishing, any news against a potential victim, especially topics related to political and economic crises, can be used. Also, certain news can be used in pretext when an attacker tries to gain the trust of the victim.

3.6 Trust In Social Platforms

Targeted phishing uses trust in social platforms. This approach can be used in targeted phishing. Very often, on behalf of well-known social platforms, the statement is used that "technical work" is being carried out and one or another algorithm of action must be carried out that will allow the attacker to compromise the victim's account or obtain other information.

3.7 Typosquatting

The tactics of typosquatting are designed for a simple typo of the user. Having made a mistake even on one symbol, the user can get on a copy of the original resource, which is either a phishing resource or a kind of bait.

3.8 FUD

FUD is a manipulation tactic that involves reporting something to cause uncertainty or even fear of it. "3ump-and-dump" technique (manipulation of the exchange rate on the stock market or on the cryptocurrency market with a subsequent collapse) using e-mail is also widely used. Thus, mass e-mailing is carried out, in which the potential of shares bought up in advance by the organizers of the mailing is signed, which will entail the purchase of these shares and an increase in their price.

4 STATISTICS

Let us consider the use of different techniques in recent years. According to FinCERT, in the period from the III quarter of 2019 to the III quarter of 2020, the number of operations without the consent of the client increased from more than 163 thousand attacks to more than 180 thousand. However, the share of social engineering decreased by 10 percentage units.

According to Positive Technologies, in the second quarter of 2020, the attacks by social engineering methods were more often used against legal entities (Figure 1).

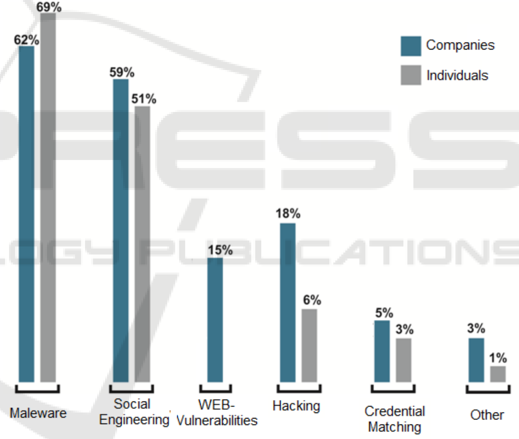

Figure 1: Shares of attacks on individuals and legal entities.

According to Positive Technologies, the topic of COVID-19 in attacks using social engineering methods is affected in 16% of cases. More than a third (36%) of such attacks were not tied to a specific industry, 32% were directed against individuals. The use of the coronavirus theme in conjunction with social engineering was used against state institutions in 13% of cases.

According to the Central Bank of the Russian Federation, social engineering accounts for 83.8% of the total number of attacks on individuals. The share of telephone fraud, as a type of pretext, increased by 30 times compared to 2017, and more than doubled since 2019. The number of fraudulent calls amounted to 15 million, the number of calls per day is more than 100 thousand, they are directed to the field of remote banking of individuals, which, together with FinCERT data, indicates the high development of pretexting.

Thus, it can be concluded that most of the attacks committed using social engineering methods are committed using methods such as phishing and pretexting, their number continues to grow. Other methods of social engineering have a lower proportion than phishing and pretexting, but, nevertheless, are used and pose a danger.

In Table 1, consider criteria such as channel of attack.

Table 1: Analysis of attacks by social engineering methods according to attack channels.

	Phone	Social networks	Messengers	e-mail	SMS	Removable drives
Pretexting	+	+	+	+	+	
Phishing		+	+	+	+	
Baiting	+	+	+	+	+	+
Quid Pro Quo	+					
Reverse Social Engineering						

5 COUNTERMEASURES

In Russian Federation, awareness requirements in the field of information security were first indicated in the Federal Law Of The Russian Federation no. 152-ФЗ "On The Protection Of Personal Data." Training and awareness requirements are described in the FSTEC regulations of Russia, which are based on special NIST publications, as well as in GOST 27th series, based on international ISO/IEC standards.

In the Russian service market, which began to form recently, several security awareness tools developed by companies such as Kaspersky Lab, Antifishing, System Software are presented. We are going to sort them out.

This software provides training in the form of courses and digests, often based on real practice, and training.

Kaspersky Security Awareness and Antifishing systems provide for modularity in positions, i.e. different courses are selected for different positions. In the Syssoft Security Awareness system, the division takes place into focus groups formed by the awareness criterion. Also, this system is aimed only at awareness of phishing issues, when, like the rest, it covers other areas of social engineering. The Antifishing system has a function of correcting for working specifics, when the remaining systems considered do not contain such a function. The Kaspersky Security Awareness system, unlike others, does not have the ability to splice with the client infrastructure and is located exclusively in the cloud, when the rest of the reviewed systems can be located in the cloud and in the client infrastructure.

It can be concluded that most modern remedies are limited to awareness-raising. The above-mentioned means of raising awareness are aimed at working with employees of enterprises, two of the three systems considered cover the development of awareness skills when conducting attacks using several methods of social engineering (Kaspersky Security Awareness and Antifishing), Syssoft Security Awareness system is aimed at countering phishing and does not cover other areas of social engineering.

6 DEVELOPMENT OF NEW METHODS OF COUNTERACTING ATTACKS WITH METHODS OF SOCIAL ENGINEERING

The issue of countering attacks by social engineering methods directed at individuals remains open. According to the statistics given above, most of the attacks are on individuals, so the issue of developing systems and methods to counter attacks by social engineering methods is relevant not only to enterprises, but also to individuals.

The development and modernization of countermeasures can be divided into the development of countermeasures in various channels of attack.

When conducting attacks through social networks, instant messengers, e-mail and SMS, information from the attacker comes in the form of text carrying a particular semantic load. Thus, counteracting attacks through such channels can be reduced to analyzing semantic information by machine learning methods and then outputting the reliability of the source. This technique is applicable to both businesses and individuals.

If we consider telephone communication as a communication channel, then the analysis of the obtained information by machine learning methods is difficult but possible. There are several software products in the mobile application market, for example, the Number Determiner from Yandex or Kaspersky Who Calls. These tools analyze the calling number and display on the smartphone the intended name of the caller or the name of the organization from which the call comes from. However, if the number is hidden, such systems do not work. One of the options for solving this problem is creating a generalized call notification system from large state, financial and other organizations whose names are represented by attackers.

In Russia, there are all prerequisites and opportunities based on practical experience. So, for example, in 2019, the Fast Payment System was launched in the Russian Federation, and from April 1, 2021, requirements for pre-installation on smartphones enter, computers and smart TVs of domestic applications. Thus, using such practical experience, it is possible to create a large association of leading commercial and state companies to create a single system, through which the call from a particular organization will be confirmed and information about the validity of the call from the organization will be displayed on the device screen simultaneously with the incoming call (similar to the work of the applications described above from Yandex and Kaspersky Lab; it is possible to work in conjunction with them by including them and similar software in a single system).

An application that supports the operation of the system, therefore, should be included in the list of mandatory software for pre-installation. However, such measures have not been applied yet. They are only planned, and an analysis of the consequences of the implementation of this bill is needed.

Consideration of such a channel as system drives (in particular, the bait method is considered) boils down to an increase in the culture of cybersecurity for both ordinary users and employees of various companies. The awareness systems described in this work are applicable, but such systems are applied exclusively at the company level and the decision on their application is made only by company management. However, the Ministry of Education approved the proposal of the Public Chamber to introduce a digital literacy course into the educational process.

7 CONCLUSIONS

Various methods of social engineering were researched, examples were considered, protection methods were analyzed and proposals were deduced in this work. The integrated use of the results will help reduce the level of successful attacks on all methods.

REFERENCES

Overview of Information Security Incident Reporting when Transferring Funds (2020). *Central Bank Of Russia.* Circulation Date: 24.01.2021 https://www.cbr.ru/analytics/ib/review_1q_2q_2020/

Current cyber threats (29.08.2020). *Positive Technologies* Circulation Date: 24.01.2021 https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/

Putyato, M.M., Makaryan, A.S.,2020. Cybersecurity as an integral attribute of multilevel protected. In *Caspian Journal: management and high technology*

Putyato, M.M., Makaryan, A.S., Cherkasov, A.N., Gorin, I.G., 2020. Adaptive system of complex security assurance as an element of the infrastructure of the situation center. In *Caspian magazine: management and 2020. № 4 (52).*

Social engineering: 8 highly specialized methods. (2020). *Anti-Malware.* Circulation Date: 24.01.2021 https://www.anti-malware.ru/analytics/Threats_Analysis/8-common-social-engineering-tactics

Security Awareness Market Overview. (2020). *Anti-Malware.* Circulation Date: 24.01.2021 https://www.anti-malware.ru/analytics/Market_Analysis/Security-Awareness

Information security and weak equestrian cyber threat. (2020). *Group-IB.* Circulation Date: 24.01.2021 https://www.group-ib.ru

Kaspersky Who Calls. (2021) *Kaspersky Lab.* Circulation Date: 24.01.2021 https://www.kaspersky.ru/caller-id

Number determiner - Yandex app for Android. Help (2021). *Yandex.* Circulation Date: 24.01.2021 https://yandex.ru/support/yandex-app-android/app/callerid.html

Express Checkout. (2021) Wikipedia*.* Circulation Date: 24.01.2021 https://ru.wikipedia.org/wiki/Система_быстрых_платежей

The Government of the Russian Federation approved a list of domestic applications for pre-installation on new smartphones and gadgets. (06.01.2021) *Habr.* Circulation Date: 10.02.2021 https://habr.com/ru/news/t/536308/

In Russian schools, OBZ lessons will be supplemented with courses on cybersecurity. (2020) *4pda.* Circulation Date: 10.02.2021 https://4pda.ru/2020/01/09/366366/