UDC 344

CRIMINAL LEGAL CHARACTERISTIC OF SOCIAL ENGINEERING AS A WAY OF COMMITTING FRAUD

Vladimir PAKHOMOV,
Doctor of Law Sciences, Associate Professor,
Head at the Department of Criminal Disciplines and Legal Proceedings
of Sumy State University

Olga BONDARENKO,
Candidate of Law Sciences, Senior Lecturer at the Department
of Criminal Disciplines and Legal Proceedings
of Sumy State University

Mikhail DUMCHIKOV,
Candidate of Law Sciences, Assistant at the Department
of Criminal Disciplines and Legal Proceedings
of Sumy State University

SUMMARY

Today, the phenomenon of social engineering becomes an integral part of cybercrime. It is a certain manipulative method of influencing the emotional and natural behavior of a person who helps to force the victim to give the scammers all the necessary information. There are many different methods of using social engineering, but the main ones are the manipulation of human fears, interest or abuse of trust. The victim of social engineering can be, as during personal communication or use of digital gadgets and on the Internet. One of the most popular tools of social engineering is phishing – a kind of internet fraud that aims to capture information of a private nature fraudulently.

Key words: social engineering, fraud, cybercrime, phishing, whisking, internet fraud.

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК СПОСОБА СОВЕРШЕНИЯ МОШЕННИЧЕСТВА

Владимир ПАХОМОВ,
доктор юридических наук, доцент,
заведующий кафедрой уголовно-правовых дисциплин и судопроизводства
Сумского национального университета

Ольга БОНДАРЕНКО,
кандидат юридических наук, старший преподаватель
кафедры уголовно-правовых дисциплин и судопроизводства
Сумского национального университета

Михаил ДУМЧИКОВ,
кандидат юридических наук, ассистент кафедры
уголовно-правовых дисциплин и судопроизводства
Сумского национального университета

АННОТАЦИЯ

Сегодня феномен социальной инженерии становится неотъемлемой частью кибермошенников. Речь идет об определенной методике манипуляции, при которой идет воздействияе на эмоциональную сторону поведения человека, которая помогает заставить потерпевшее лицо отдать мошенникам все необходимые данные. Существует немало различных методов использования социальной инженерии, но основными из них следует считать манипуляцию человеческими страхами, заинтересованностью или злоупотребления доверием. Жертвой социальной инженерии можно стать, как во время личного общения или использования цифровых гаджетов, так и в сети Интернет. Одним из самых популярных инструментов социальной инженерии следует считать фишинг − вид интернет-мошенничества, целью которого является завладение информацией частного характера обманным путем.

Ключевые слова: социальная инженерия, мошенничество, киберпреступность, фишинг, вишинг, интернет мошенничество.

Problem setting. Accelerated scientific and technological progress and the global computerization of society have led to significant changes that manifest themselves in both positive and negative consequences for any sphere of public life. The negative effects of computerization are expressed in the emergence of not only new types of cybercrime, but also new methods of committing fraudulent actions characterized by high social danger. This is due to the value of the sub-

ject of a criminal offense and, of course, the vulnerability of both computer information and person's consciousness.

With the popularization of the scale of the use of various types of cashless settlements, all the latest ways of committing fraud, first of all, social engineering, constitute a threat to the economic life of the country and its population. We believe that today this issue is very important in the solution and relevant for discussion.

In modern science, this issue was also addressed by such scholars as Karchevskaya, Bulgar, Dzundzyuk, Shulyakovskaya, Shcherbakov, Trofimchuk.

The purpose of the work is to study the phenomenon of social engineering, its significance, analysis and justification as one of the methods of committing fraud, which is dangerous for everyone, and to prove the necessity to implement urgent measures for the prevention and counteraction of such a criminal phenomenon.

Research methods.

• Methodological basis for writing of this work was used different methods of scientific knowledge.

• In particular, the method of observation for direct familiarization with the essence of the phenomenon of social engineering and the challenges that he calls.

• The method of generalization was used to define the general concept of social engineering and its importance for the economic security of the state and society.

• The statistical method made it possible to investigate and assess the extent of the development of a social engineering fenomon.

Basic material. Today, in the era of information technology development, more and more people are suffering from various manifestations of fraud. Intruders try to capture the property of a person in various ways, and in this case, as a rule, in a contactless manner using psychological influence and using the trusting state of the victim.

One way of doing this kind of fraud is the phenomenon of social engineering, that is, the art of manipulating people through action, or the disclosure of confidential information in a way other than through the means of technical destruction of databases.

It should be noted that the phenomenon of social engineering developed not only in Ukraine and CIS countries, but also in Europe, each third person in one way or another faced with this. The most common and at the same time the simplest types of social engineering are telephone calls and sms messages of a diverse nature. The nature of such messages is also different, and I can be as joyful, such as winning a lottery or winning a car, and the sad nature where the problem of loved ones is with the law. Unfortunately, there are people who believe in these messages and transfer money to accounts of intruders, we are talking about certain age qualifications, namely about people who have not reached the age of majority and the elderly.

According to world statistics, the number of hacker attacks using social engineering methods has steadily increased, in 2015, such attacks hit 37% of financial institutions in the world. In order to increase the effectiveness of protection from typical attacks, it is necessary to constantly investigate the most common types of fraud, analyze the actions of intruders, as well as to build the appropriate security system [6].

It is with the help of such simple and easy actions that affect the psychological characteristics of the human person. The fraudsters are trying to seize our personal data (other confidential information) with a clearly more negative purpose than filling out a questionnaire for getting a bonus card in a popular store.

Social engineering is based on the psychological features of a person, such as:

– the principle of reciprocity;

– the principle of social verification (you evaluate your behavior in the context of the behavior of the majority);

– Respect for authorities (you will be more confident with a doctor and a policeman than an average person). All these principles apply to "offline" fraud, but they have their own specifics when committed online [1].

The most popular scheme of influence on a person used in social engineering is the Schein's scheme, which consists in the following steps:

1) the formation of the purpose of impact on the object;

2) search for information about the object;

3) identification of the most convenient targets of influence;

4) creation of the most favorable conditions for influence on the object;

5) coercion for the desired action;

6) the result.

To analyze the effectiveness of combating social engineering as one of the manifestations of cybercrime, you need to get acquainted with the main methods of its application in practice. Yes, they include the following.

Phishing an Internet fraud view whose main purpose is to access the victim's confidential information, built on sending letters from financial institutions or Internet portals, followed by the introduction of a password or downloading a virus program. This method of Internet fraud is achieved through the distribution of emails on behalf of popular dreams, financial institutions [7].

Whisking the name of this type of Internet fraud went from the previous one and consists in imitating calls to the mobile phone, as if from a banking institution (with a pre-recorded voice) and receiving a request for communication with the bank to confirm this or that information. In this case, the victim is required to say his password or other confidential information required for access to bank accounts [5].

Spear Phishing. If regular phishing involves sending millions of generated e-mail messages mail to different users, then the purpose of spam phishing is only specific users. Emails used for spam phishing are configured for specific recipients, with their names and personal information in order to make the messages more legitimate and plausible.

Since the number of emails used in spam phishing is much lower than that of regular phishing scams, this method of fraud is harder to detect.

Whaling is one of the types of phishing phishing. Instead of seeking "small fish", "whale hunting" focuses on "big fish", that is, on rich people, on bank accounts that an attacker wants to access. By concentrating on this small group, the attacker can take more time to attack and provide a clear message formation, to be more successful with greater probability.

Farming The procedure is to redirect the victim to a false IP address. The scammer installs a malicious program on com-

puters, which, once launched on the computer, provides redirection of the victim instead of the sites they seek to fake sites that are then "robbed" of people.

Virus warning on your computer. In this case, the malware developer warns the victim about infecting her computer with a virus and reports that to clear the operating system, you need to go through the link and install the required program. This program is harmful and provides access to the necessary information.

Quid pro quo The specified type of online fraud is based on the ability of a person to telephone a conversation or e-mail to trust the victim (usually an office worker) and, having presented himself as a co-worker of the technical support service, to offer him a solution to the problem, in which he will receive all the necessary confidential information.

Reverse social engineering. Realization of this method can be carried out only in the case when the swindler pre-acquaintes with the victim and deserves its trust. In this case, the victim himself turns to the rogue (for example, the system administrator), asking to help restore the lost file (which has been hidden by the crook). At the same time she is notified that such an action can be done as soon as possible only by going to her account. Thus, the victim at his own discretion tells all the information a scammer.

Fraud related to purchases via the Internet. The low price of a product, much lower than its competitors, requires a full or partial prepayment, must immediately alert the buyer. Such a fraud scheme is the most widespread one. The seller places a low price, but always requires a prepayment, full or partial, to refuse to pay to the department of delivery. In such cases, the buyer pays the goods, its part or the cost of delivery quite often remains with nothing. The main rule of shopping on the Internet − make a prepayment only to proven vendors, with others pay for goods after receipt.

Fraud related to sales through the Internet. Selling goods online, with the help of stock exchanges, may also be a victim of a fraudsters. Under the pretext of paying for your goods, the crook will try to find out all the data of your payment card, which will allow you to withdraw money from your account. In order to protect yourself from losses, it is necessary to remember the following simple rules:

1) To pay for your card is sufficient to know the number of 16 digits; in no case do you disclose the validity of the card and the CVV code on the back of the card;

2) to pay for your card, you do not need to receive any SMS messages or to approach an ATM, do not inform the fraudsters on SMS messages that arrive on your card and do not carry out any operations at the ATM at their request.

The specified types of online fraud are the most popular manifestations of the use of Internet engineering. At the moment, it's worth considering the Internet crime prevention measures that are being applied in Ukraine.

Classifying tips for preventing the manifestations of social engineering can be according to the source of information requests.

So, in case of an attack by using the phone, the following advice would be advisable: verification of the person calling; use the service of determining the number; ignore unknown phone messages.

In case of encroachment by using e-mail: do not open incomprehensible attachments in documents; do not click on untested hyperlinks in the body of the message; check requests for personal information sent in such messages.

In order to prevent an attack by using instant messaging services, you need to choose one platform for such exchanges, define the principles for setting up new contacts, and use high-quality passwords to access your account.

However, in the field of legal science, more interesting for the study is not advice how to protect themselves from negative manifestations of social engineering, and legal problems of protection against this phenomenon [1].

In order to understand the essence and meaning of the concept of "social engineering", it is necessary to consider the concept of "fraud". The Criminal Code of our state gives a clear notion to this word − it is a punishable act involving the possession of someone else's property or the acquisition of the right to property by deceit or abuse of trust (Article 190 of the Criminal Code of Ukraine). Social engineering in this case serves as a way of committing fraud, which usually combines two methods of committing a crime, namely deception and abuse of trust. The peculiarity of this article is that the victim is a volunteer, at his own will, and does not transfer property to the detriment of his own interests, or the right to it to another deceitful person. This fraud differs from other criminal acts, such as: abduction (when a person takes possession of the property or rights to it without the consent of the person) or extortion (when the property or rights are transferred to him compulsorily). But voluntariness with mischance is imaginary, because there is still a lot of mischief here. The law sees two methods of fraud: fraudulent abuse of trust. The first is a message to the person of inaccurate data, through which she is deceived, the second one − more cynical, because a potential fraudster for his actions uses a confidential relationship with the victim. Also the constituent parts of this crime are: direct intent of the performer; selfish motive. That is, the person who carries out this punishable act deliberately goes to this crime, with the aim of seizing the property or the victim's right to it.

In particular, the Criminal Code of Ukraine defines the term ""fraud with the use of electronic computers" (Part 3, Article 190), "Illegal collection for the purpose of using or using information constituting commercial or banking secrets" (Article 231) and a whole list in the section of the XVI-like crimes [2].

In 2016, significant progress was made in the fight against cybercrime as a whole. The President of Ukraine signed the Decree, which entered into force the decision of the National Security and Defense Council of Ukraine of January 27 "On the Strategy of Cybersecurity of Ukraine".

This document states that, together with the benefits of the modern digital world and the development of information technology, cases of illicit collection, storage, use, destruction, distribution, personal data, illegal financial transactions, theft and fraud in the Internet are now actively spreading. Modern information and communication technologies can be used to carry out terrorist acts, in particular by breaking the standard modes of work of automated control systems of technological processes at infrastructure objects. Politically motivated activity in cyberspace is becoming more widespread in the form of attacks on government and private websites on the Internet.

Analysis of this document allows us to identify the following key provisions:

1. The main threats to the cyber security of Ukraine are identified and the Russian Federation is mentioned as a potential source of such threats, as well as their factors are described;

2. The main tasks of the national system of cyber security are fixed and the relevant bodies and their sphere of responsibility are specified;

3. The main priorities and directions of ensuring the cyber security of Ukraine (one of which is carrying out exercises on emergencies and incidents in cyberspace) is determined;

As a matter of fact, this document is filled with really relevant provisions and programs that require the development of appropriate regulations, which will include a system of measures for their implementation. At this stage, it will be interesting to observe that the National Coordination Center for Cyber Security, which is the working body of the National Security and Defense Council of Ukraine, was created by the Decree of the President of Ukraine №. 242/2016 of June 7, 2016. However, information on the site of the National Security and Defense Council on the activities of this body and among other available resources has not been revealed [6].

In addition, by the Decree of the President of Ukraine №. 32/2017 On Decision of the National Security and Defense Council of Ukraine dated December 29, 2016, "On threats to cybersecurity of the state and urgent measures for their neutralization", the mentioned decision of the National Security and Defense Council was put into effect. This decision draws attention to the most important steps to protect critical infrastructure objects from cyber-attacks, as well as requirements to the Cabinet of Ministers of Ukraine to develop legislative proposals for the implementation of the provisions of the Convention on Cybercrime [4].

These acts are mainly aimed at establishing the foundations for building a powerful cybersecurity system in Ukraine, but only a small number of their provisions can very closely relate to the cybersecurity of individuals. On the one hand, this is due to the political situation in the country, however, in my opinion, it is impossible to forget about the interests of citizens of Ukraine and other persons, even due to the unstable situation in Ukraine.

Thus, despite the prevailing public opinion about phishing and social engineering as methods of criminal activity, they can and should be used, first of all, for the prevention and fight against crime on the Internet. Undoubtedly, their application, as well as the use of any operational-search activities, requires the prior agreement of all legal aspects. It should be noted that today the main way of protecting from social engineering methods is to carry out preventive measures consisting in training of citizens and employees of enterprises, institutions and organizations. Custom credentials are the property of the company (enterprises, institutions, organizations). All employees on the day of recruitment need to explain that the logos and passwords they received cannot be used for other purposes (on third-party web sites, for personal mail, etc.), to be transferred to third parties or other employees of companies who do not have on their rights. For example, very often, the employee, on leave, passes his authorization data to his colleague in order to be able to do some work or look at certain data in his absence.

Based on the foregoing, one can conclude that countering cybercrime is an important component of protecting the national interests of the state. Cybercrime has already become a big issue for the world, which needs immediate resolution. Law enforcement agencies are trying to be at the forefront of combating these crimes: special units are created to fight cybercrime, legislators adopt new laws, banking and financial institutions, within their competence, carry out preventive work with the population, providing appropriate recommendations for the safe use of the Internet. However, the loss of citizens and the damage to the state and the private sector from the illegal actions of Internet fraudsters is constantly increasing. Cybercrime, like any other crime, is not only a legal and a social issue. It is necessary to create a unified classification and a formal model of cybercrime that will facilitate and counteract cybercrime, and investigate cybercrime. The organization of the information security system should be comprehensive and based on a thorough analysis of possible negative consequences. The main way of protecting from social engineering methods is to train employees. All company employees should be warned about the risk of disclosure of personal information and company confidential information, as well as ways to prevent data leakage.

References:

1. Соціальна інженерія. *Вікі-знання* ; Тернопіл. нац. техн. ун-т ім. Івана Пулюя. URL: http://wiki.tstu.edu.ua/Соціальна_інженерія (дата звернення: 27.02.2019).

2. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III / Верховна Рада України. URL: http://zakon4.rada.gov.ua/laws/show/2341-14. (дата звернення 27.02.2019).

3. Про основні засади забезпечення кібербезпеки України № 2163-VIII от 05.10.2017 р. / Верховна Рада України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html (дата звернення 27.02.2019)

4. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» : Указ Президента України № 32/2017. / Верховна Рада України. URL: https://www.president.gov.ua/documents/322017-21282.

5. The Social Engineering Infographic. *Security trough Education: a free learning resourse.* Social-Engineer, Inc. Apr. 28, 2014. URL: http://www.social-engineer.org/social-engineering/social-engineering-infographic/ (дата звернення: 27.02.2019).

6. Gunn J. Social Engineering and How to Win the Battle for Trust. VASCO: blog. Nov. 5, 2015. URL: http://blog.vasco.com/electronic-signature/social-engineering-win-battle-trust-infographic/ (дата звернення: 31.10.2016).

7. Що таке фішинг? *GoDaddy: сайт*. URL: https://ua.godaddy.com/help/sho-take-fishing-346 (дата звернення: 10.11.2016).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Пахомов Владимир Васильевич – доктор юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин и судопроизводства Сумского национального университета;

Бондаренко Ольга Сергеевна – кандидат юридических наук, старший преподаватель кафедры уголовно-правовых дисциплин и судопроизводства Сумского национального университета;

Думчиков Михаил Александрович – кандидат юридических наук, ассистент кафедры уголовно-правовых дисциплин и судопроизводства Сумского национального университета

INFORMATION ABOUT THE AUTHORS

Pakhomov Vladimir Vasilyevich – Doctor of Law Sciences, Associate Professor, Head at the Department of Criminal Disciplines and Legal Proceedings of Sumy State University;

Bondarenko Olga Sergeyevna – Candidate of Law Sciences, Senior Lecturer at the Department of Criminal Disciplines and Legal Proceedings of Sumy State University;

Dumchikov Mikhail Aleksandrovich – Candidate of Law Sciences, Assistant at the Department of Criminal Disciplines and Legal Proceedings of Sumy State University

olya.tereschenko34@gmail.ru
kafedrapravasumdu@ukr.net
misha.dumchikov23@gmail.com

УДК 342.9

РАЗВИТИЕ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРАНСПЛАНТАЦИИ В ПЕРИОД СССР

Вадим ПИШТА,
аспирант кафедры административного,
финансового и информационного права
Ужгородского национального университета

АННОТАЦИЯ

Статья посвящена исследованию развития административно-правового регулирования оказания медицинской помощи с применением трансплантации в период СССР. Определены нормативные первоисточники трансплантации. Анализируется становление таких правовых категорий, как донор, реципиент, донор-труп, врачи и обслуживающий персонал, которые были задействованы во время проведения соответствующего вмешательства, согласие донора на извлечение органов, предварительное согласие родственников умершего на изъятие органов, заготовка анатомических материалов, констатация биологической смерти, международное сотрудничество в сфере трансплантации. Детально освещено постепенное развитие условий, которые были необходимы для извлечения органов у донора и донора-трупа.

Ключевые слова: трансплантация, административно-правовое регулирование, донор, реципиент, согласие на извлечение органов.

DEVELOPMENT OF ADMINISTRATIVE AND LEGAL REGULATION ON TRANSPLANTATION IN THE USSR PERIOD

Vadym PISHTA,
Postgraduate Student at the Department of Administrative,
Financial and Information Law
of Uzhhorod National University

SUMMARY

The article highlights the question about the development of administrative and legal regulation of medical care with the use of transplantation in the USSR period. Defined normative primary sources of transplantation. Analyzed the formation of such legal categories as: donor, recipient, deceased donor, doctors and attendants, who were involved during the relevant intervention, consent for organ donation, prior consent for organ donation of the deceased's relatives, preparation of anatomical materials, statement of biological death, international cooperation in the field of transplantation. Details covered the gradual development of the conditions that were necessary for the extraction of organs from the donor and the deceased donor.

Key words: transplantation, administrative and legal regulation, donor, recipient, consent for organ donation.

Актуальность темы исследования. Трансплантация – это метод лечения тяжелых заболеваний человека, который применяется в тех случаях, когда устранение опасности для жизни или восстановления здоровья больного другими методами лечения невозможно.

С самого начала своего существования трансплантация поставила много вопросов правового характера, которые еще не приходилось решать в процессе развития человечества. Необходимость в совершенной правовой базе трансплантации связана, прежде всего, с особыми отношениями между донором и реципиентом, специфика которых заключается в равном для каждого из них праве на жизнь. Именно поэтому с принятием 17 мая 2018 года Закона Украины «О применении трансплантации анатомических материалов человеку» [1] возродилась волна научного интереса к вопросам правового регулирования трансплантации.

Вместе с тем нельзя оставлять без внимания генезис административно-правовых норм, регламентирующих вопросы оказания медицинской помощи с применением трансплантации. Исследования в историческом разрезе