European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.12.03.92

PERAET 2021
International Scientific Conference «PERISHABLE AND ETERNAL: Mythologies and Social Technologies of Digital Civilization-2021»

METHODOLOGY FOR STUDYING THE INFLUENCE OF SOCIAL ENGINEERING

Daria N. Karpova (a)*
*Corresponding author

(a) Moscow State Institute of International Relations (MGIMO), Moscow, Russian Federation, d.karpova@inno.mgimo.ru

Abstract

The author continues investigating the world problem of cybercrime and social risks as constant companions of that social phenomenon. In the circumstances of a new COVID world order the problem of cybercrime as a challenge to all mankind has only been intensified. Lately the author focused on the problem of understanding the nature of online risks known as risks of continuous online-communication. On the basis of theoretical analysis and empirical research it was systematized probable manifestations of risks taking into account their differential impact on some categories of the population. Now the author makes next step in understanding such a phenomenon like social engineering as a tool for committing a cybercrime. It is stated in the text the relevance of studying that social and psychological case and discussed the need for methodology of its analysis. It is discussed in the article the latest results of a survey conducted by the Russian Opinion Research Center (WCIOM) and proposed the classification of tools used by social engineers while committing such type of crime. According to many experts, the greatest threat to information security, both for large companies and ordinary users, in the next decades will be in roving methods of social engineering used to crack existing security tools. Our biology is inextricably linked with our social essence.

Keywords: Cyber risks, cyber security, online-communication, social engineering

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

It is curious to note that it took almost a hundred and twenty years to spread the spindle (the symbol of the first industrial revolution) outside Europe and less than ten years for spreading the Internet around the world. And only several months were needed to transfer for almost total usage of Internet in our daily lives till these days. The COVID-19 Pandemic has shown us how severely the Internet is affecting us, how much we rely on digital data today and will robotics affect the future of work? (Pichkov & Ulanov, 2021). In connection with the pandemic, millions of people around the world regardless of the level of their computer literacy and digital skills are faced with the need to almost completely transfer their lives to the Internet. Education and work became remote, the purchase of things, groceries, medicines - all the support of a person's life was provided with the help of the Internet and the process of digitalization in general. Schwab (2019) in the annual Global Competitiveness Report stated that more than half of the population in the world have the access to the Internet, and 80.9% of adult population in the Russian Federation respectively. We can observe how not only economics but social sciences get used to this new reality: how people manage social information and how network cognitions are affected by situation and social circumstances (Smith et al., 2020).

Nevertheless, many social scientists are concerned about the bifunctional nature of the digitalization as a whole which appeared under the nonlinear dynamics of rationalization, achievements and side-effects of science and technologies, ambivalences of artificial intelligence. In its turn, digitalization makes a significant contribution to the nonlinear transformation of reality and provides actors with the ability of self-reflection and self-improvement (Kravchenko, 2021). Summing up, the access to Internet resources does not guarantee a careless increase in a person's material and social benefits without risks. One of the most important characteristics of online-communication is still its *riskiness*.

The so-called risk bias effect appears. It has been empirically proven that people on social media make more ill-considered decisions than during direct face-to-face communication with each other. Thus, a person in social networks acts much more recklessly, thereby showing his weakness. Weakness and naivety are a key factor in mistakes. It is a person who is the most vulnerable object in the network, and his similar unsightly and at the same time practically ineradicable human characteristics cause a high susceptibility to the risks of deception in networks. Human vulnerability is the main reason for the effectiveness of cyber criminals who simply exploit the carelessness and carelessness of people within the framework of various social engineering tools.

Lately we have proposed the sociological definition of a cybercrime as an act of social deviation made for the purpose of causing economic, political, moral, ideological, cultural and other types of damage to individual, the organization or state by means of any technical tools and Internet access. The methodology for sociological analysis of cybercrime is formed by object and subject nature of this social action (who commits the crime and who is its victim). In the form of the table below we will designate the main methodological aspects of cybercrime as social action (Karpova, 2017) (See Figure 1).

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Subjects (risk producers)	Cyber criminals		
Objects (risk consumers)	individual	organization	state
Aims (motives)		1. economic	
		2. reputational	
	3.social and psychological		
	4. ideological		
			5. political
Instruments	social engineering		
	virus programming		

Figure 1. Methodological aspects of cybercrime analysis

In this article we focus our attention on acts of cybercrime made by the tools of social engineering. The relevance of this problem is determined by unchanging nature of man. Given all the inherent weaknesses and fears, he can always be deceived. Cybercrime, in particular social engineering, is a global threat to the entire world.

2. Problem Statement

There is still no common sociological definition of a concept of social engineering. Originally it was a technical term only. In times of a complex society, we have proposed a new postdisciplinary approach to understanding new digital reality based on so-called sociotechnical turn, which is a purely integrative approach aimed at solving a tough common issue (Karpova & Proskurina, 2021). For a general understanding of the context, we will offer the following version of the definition of this phenomenon. *Social engineering is a tool for committing a crime both online and offline performed as various techniques of social and psychological manipulation of people in order to obtain any confidential information.*

Taking into consideration interdisciplinarity in defining social engineering we will consider the following methodological approach as a basic in studying that phenomenon. It was proposed by the former hacker and cybercriminal K. Mitnick. Since his release from prison in 2000, Mitnick has changed his life and established himself as one of the most prosperous computer security experts around the world. He co-authored three books on computer security: ‘The art of deception’ (Mitnick, 2003), ‘The art of invisibility.’ (Mitnick, 2017), ‘Social engineering: the science of human hacking’ (Mitnick, 2018). In these books, it is described various real or imagined scenarios of fraud and social engineering attacks, as well as their consequences. Using various examples, Mitnick shows how social engineers use human weaknesses, such as gullibility or the desire to be useful in order to get what they want. The main postulate of Mitnick and all social engineers sounds like this: security is not a technological problem, it is a problem of people and management.

Many different studies by Mitnick have resulted in 6 traits of human nature (human needs) that determine the effectiveness of cybercrime committed by social engineers.

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. *Authority*. A cybercriminal can easily achieve the desired result by convincing the victim that he has more power and rights.

2. *Location.* A victim communicates with a person with similar views, problems or interests, it is easier to make contact and is more disposed towards the attacker.

3. *Reciprocity*. A victim receives something as a gift, advice, promise, or a real physical gift, one tends to automatically respond to the request.

4. *Responsibility*. A victim has a strong desire to be trustworthy to try ones best to satisfy the request.

5. *Social belonging*. A victim does not want to stand out, and if one feels that this behavior complies with the rules of the group, he\she calmly makes contact.

6. *Limitation*. A victim believes in the uniqueness and limitations of the offer.

According to the study by Positive Technologies for the 1st quarter of 2021, in 56% of cases, the targets of attacks are people, and the method of attacks is social engineering (Positive Technologies statistics, 2021). Mitnick proposes the idea that organizations that conduct tests and training of employees and security systems report that they significantly reduce the ability of social engineers to penetrate the company system. Thus, having trained employees who conscientiously apply the knowledge gained in practice is the only chance to create the inviolability of the company's data.

3. Research Questions

This research was conducted under the assumption that various technical methods and programs of protection can be constantly improved, but people remain people with their own prejudices, stereotypes and become the weakest link in the chain of online-communication security. In that case it was relevant to examine 1) the examples of real attacks on a network user. 2) Further classifying them according to human needs. Moreover 3) conduct a series of simulated phishing attacks on different socio-demographic categories of people.

4. Purpose of the Study

The purpose of the study is to prove the significant role of social engineering in understanding crime attacks and suggest a cyber risk research methodology for further development and improvement of countermeasures dealing with cyber criminals.

5. Research Methods

5.1. Social experiment (pilot) with the help of Russian company 'Antiphishing' is aimed at detecting successfully implemented simulating phishing attacks and vulnerable aspects of people's behavior in the face of social engineering. Sample: 204 people aged 17 to 76. 'Antiphishing' is a Russian research company and software developer. The company has been working since 2016 and specialize in solving human factor problems in information security. They have developed a product of the same name

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- *the Antiphishing platform*, which helps to train employees and control their information security skills (Antiphishing platform, n.d.).

5.2. Secondary analysis of data from sociological agencies on cyber fraud.

6. Findings

Over the last 5 years there have been published several scientific articles and reports which reveal the importance of human-centric approach to cybersecurity (Leukfeldt, 2016; Smith & Stamatakis, 2020). But still the most vulnerable piece in that cyber scheme is a man. Now it sounds like fantasy when it comes to predicting cyber attacks as it was a weather forecast (Fang et al., 2019). Situation in this country can't be called optimistic at all. Recently well-known Russia public opinion research center (WCIOM) has published the results of a survey by the method of a telephone interview based on a stratified two-base random sample of stationary and mobile numbers. According to their data over the past six months, more than half of Russians (57%) received calls from telephone scammers, and almost every fifth (19%) received SMS messages; a third (35%) did not face it. Most often, scammers called Muscovites and Petersburgers (70%), residents of cities with a population of over one million (69%). Less often than others, such calls were received by residents of villages (40%) and small towns (55%), as well as young people 18-24 years old (49%). Young people aged 24-35 (26%) and residents of small towns (23%) were more likely to receive SMS messages from fraudsters. Among the most frequently used 'legends' by fraudsters are offers of banking services (38%), bank cards (27%), loans (8%), offers to transfer money (5%), as well as information about winning prizes and medical services (3 %).

As a result of the actions of telephone scammers, 9% of Russians suffered financial damage (of which 6% reported significant damage). More often than others, among the victims of fraudsters were residents of villages (15%), young people 18-24 years old (14%), citizens 35-44 years old (10%), as well as Russians without higher education (13-14%) (Russia public opinion research center, 2021).

The most widespread type of social engineering in Russia is *fraudulent phishing*. This is a non-compensatory tool for cybercriminals, since it is almost impossible to prove that the criminal action was performed by another person and not you. The key thing in such kind of crime is that it is being committed by the hands of the victim. Now there lots of varieties of this kind of scam. One of the most popular and the latest one is the *419 scam* as a reference to the 419 section in the Nigerian penal code. It includes fee fraud, fake lottery, black money scam, etc. 419 scam is a popular form of fraud in which the fraudster tricks the victim into paying a certain amount of money under the promise of a future, larger payoff (Isacenkova et al., 2014).

Of course, the only function of a phishing page is to redirect an unsuspecting user to not a real social networking site (or any other frequently visited Internet resource) after they enter their login information. The phisher can use a well-recognizable interface as follows (see Figure 1):

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

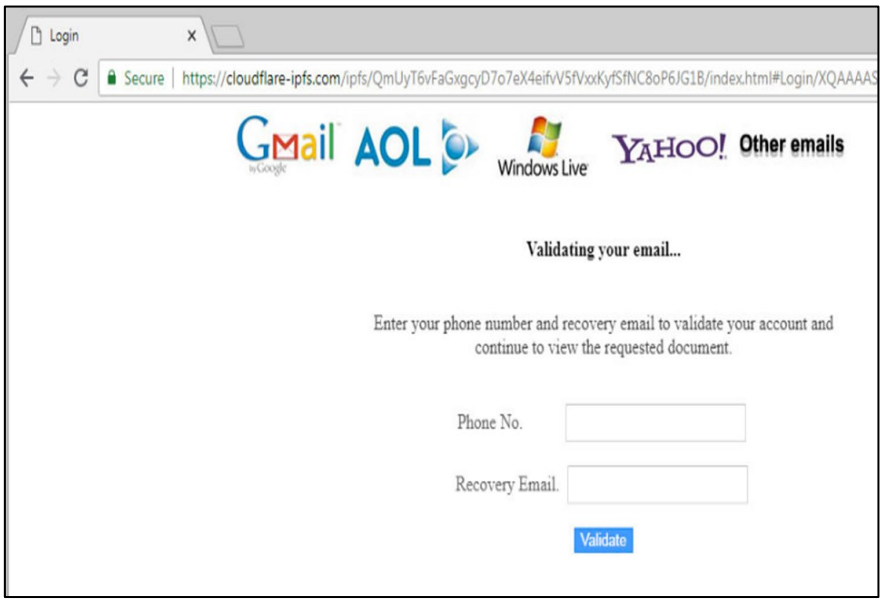

Figure 2. Gmail phishing attack

Recently we have witnessed even the hijacking attacks on smart vehicles and vehicle-to-everything communication attacks (e.g., data theft). These problems are becoming increasingly serious with the development of 4G LTE and 5G communication technologies (Dibaei et al., 2020).

Simulating attacks research

The purpose of our simulating experiment was to find out how effective the attacks will be and which ones will get the maximum user response. This experiment involved 204 people aged 17 to 76 years. Sex ratio: 65% women and 35% men. 58% of respondents were between the ages of 17 and 21, 22% were between 22 and 35.20% were between 36 and 76.

Within a month (March-April 2021), all those who agreed to participate and provide their data received 5 spam messages. These letters were designed in accordance with the style of the brands on behalf of which the letters were sent.

The Coronavirus template was sent first. Of the 204 who received the letter, 111 people survived the attack, 93 people opened the letter, 4 of them followed a potentially dangerous link and 3 opened a potentially malicious attachment. The effectiveness of the attack is estimated at 45.59%.

Similar results for Netflix, Charitable Foundation, and Google Play templates: 93 people opened emails. The effectiveness of attacks is 45.59%. An email with the “Netflix” template was opened by 47% of women and 43% of men, “Google Play” - 50% of women and 39% of men, “Charitable Foundation” - 46% of women, 42% - of men. At the same time, only 1 person followed the link of the Charitable Foundation, 3 - by the link “Google Play”.

The Gosuslugi template turned out to be the most interesting case of the attack. Only 39 people opened the letter, the efficiency was 19.12%. The letter was opened by 15% of women and 26% of men. However, out of 39 who opened the letter, 19 followed the link of the letter. That is, half of the users could have clicked on a potentially dangerous link and suffered from scammers.

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Turning to the analysis, we can say that no significant differences in the behavior of men and women, as well as users of different age groups, were found. Based on the results of 5 templates out of 6, the efficiency of spam attacks is 45%. Almost half of users open spam emails. It is important to note that simply opening an email already carries certain risks. For example, only by opening the letter, the user can subscribe his mailbox for further mailings, since when the mail is opened in the mailing service used by the attacker, it is immediately displayed that this mailing address is assigned to a live and active user. In addition, such letters may contain an image, which is often transparent. Such images are immediately loaded and downloaded from a cybercriminal's website, which in terms of danger can be compared to clicking on a link.

When it comes to links and attachments, a minimal number of people open such potentially malicious attachments or click on links. Thus, we can conclude that half of the users who open all letters are aware of the possible dangers of unknown links and attachments, but do not think about the risks of initially opening the letter.

Although the effectiveness of these templates is estimated at about 45%, almost half of the participants in the experiment who nevertheless opened the letter is already a fairly large number in the context of the risks of social engineering. Half of the users would be affected by spam. This behavior can be explained by human curiosity, which often overshadows barely appeared doubts and warnings. The desire to learn new things, to research is the most important physical and psychological activator of our behavior.

It is worth dwelling in more detail on the results of the attack with the "Gosuslugi" template. Despite the fact that the letter was sent from the portal of public services, where today almost every Russian citizen has a personal account, only 1/5 of the users opened this letter. Taking into account the results of other templates, where the frequency of message opening was consistently slightly less than 50%, it can be assumed that such spam messages that come on behalf of government services are more closely monitored by the internal security systems of postal services, which can explain such a low efficiency. It can be concluded that the letter clearly did not reach the majority of users, however, the damage that it could cause can be assessed as very significant. Half of those who opened the letter followed the link of the letter. And this action, in turn, can lead to a fatal leak of personal data. Thus, although the number of users reached by the letter is not very large, the potential for risk, in this case, is very high.

Analyzing the reasons for this behavior of the recipients of the "Gosuslugi" template, we can say that in this case the individual's desire to maintain safety and the authority of the organization that allegedly sent the letter played the main role. The portal of state and municipal services provides assistance in many areas of life support of citizens. This site is directly related to documents, invoices, receipts, statements, etc. It is difficult to overestimate the importance of maintaining the confidentiality of data posted on this portal. Due to the fear of data leakage and the need to ensure the security of their data on the site and life in general, users tend to open such letters and follow links, not realizing that it is at this moment that data theft may occur.

Summing up, it can be noted that the confident majority of users do not open attachments and do not follow the links that are attached in messages. Consequently, most are aware of the potential risks of

https://doi.org/10.15405/epsbs.2021.12.03.92
Corresponding Author: Daria N. Karpova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

data loss with this behavior. At the same time, about half of users still open spam emails, not suspecting that opening them is already a rather risky step. However, the situation changes when the attack is aimed at the most important human needs in security and hierarchical order when it comes not to a single person but to organization, huge strategic national facility such as hydroelectric power plant.

Experienced information security specialists already use a special toolkit in everyday work, realizing that information security requires taking into account along with the technical factor, the human one meaning careful work with 'risk groups'. Russian scientists from 'Antiphishing' company detect 4 main factors in the formation of such groups: 1) behavior; 2) demographic characteristics; 3) psychological characteristics; 4) specialized criteria determined by the characteristics of the company and business objectives (Limonova & Zharkevich, 2020). The components of the *behavioral factor* can be recorded unsafe actions of employees, repeated violation of established information security rules, information security incidents, the results of training and simulated attacks, as well as a lack of interaction between the employee and the information security department. *Demographic factor* includes: gender, age, place of residence and socioeconomic background, PC experience, Internet and email usage. Research data confirm that women (by gender), people under the age of 25 and older than 50 (by age) can be classified as a higher risk group. Other conclusions (on a territorial basis) were made above in WCIOM research. The *psychological factor* includes personality traits, psychological disorders, urgent needs, the leading type of motivation and emotional state of a person.

7. Conclusion

Why do many researchers believe that social engineering will become one of the main tools for hackers in the XXI century? The answer is simple. Because technical protection systems will be improved but people will remain people with their biological and psychological peculiarities. According to many experts, the greatest threat to information security, both large companies and ordinary users, in the next decades will be in methods of social engineering used to crack existing security tools. Our biology is inextricably linked with our social essence. Social engineering techniques based on our evolutionary needs and the emotions associated with them are tremendously successful among hackers. However, the use of social engineering has a strong impact on the existential safety of members of our society.

In the course of the study, we have considered some sociological theoretical and methodological approaches to the study of risk of social engineering. There was analyzed a database of already committed attacks using a developed list of needs and a further description of their effective exploitation by social engineers. Soon after an experiment was carried out – there were send simulated spam attacks to different socio-demographic categories of citizens. Based on the results of the analysis of the database and the experiment, it can be concluded that our biological and social needs play a significant role in the effectiveness of cybercrime. We see that a fairly significant number of users are aware of the existing risks of online-communication, but our needs, the main of which, in this case, are curiosity, security and hierarchy, increase the riskiness of our online activities.

Of course, the specificity of social engineering requires further active research, since today there is not enough academic knowledge on this phenomenon. However, at the moment, the results obtained can already be used to raise awareness of the risks of social engineering which can be useful for

understanding the effectiveness of attacks and, therefore, for further preventing the possibility of personal data leakage.

Acknowledgments

This article is prepared by the support of the Grant by the President of the Russian Federation for the state support of the leading scientific schools of the Russian Federation (competition 2020), application NSH-2615.2020.6

References

Antiphishing platform (n.d.). Retrieved from https://antiphish.ru/

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, Sh., Zhang, Y., Xiang, Y., & Yu, Sh. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, *4*(6), 399-421. https://doi.org/10.1016/j.dcan.2020.04.007

Fang, X., Xu, M., & Xu, S. (2019). A deep learning framework for predicting cyber attacks rates. *EURASIP Journal on Information Security*, *5*. https://doi.org/10.1186/s13635-019-0090-6

Isacenkova, J., Thonnard, O., & Costin, A. (2014). Inside the scam jungle: a closer look at 419 scam email operations. *EURASIP Journal on Information Security*, *4*, 143-150. https://doi.org/10.1109/SPW.2013.15

Karpova, D. (2017). Manifest and latent risks of continuous online-communication. *The European Proceedings of Social & Behavioural Sciences, 17, 356-362.* https://dx.doi.org/10.15405/epsbs.2017.07.02.45

Karpova, D., & Proskurina, A. (2021). The need for sociotechnical turn in the study of society digitalization. In *XXIII International Conference Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference* (pp. 387-393). University of modern Management technologies. https://doi.org/10.18502/kss.v5i2.8418

Kravchenko, S. (2021). Ot formal′noy k tsifrovoy ratsional′nosti: pobochnyye effekty, ambivalentnosti i uyazvimosti [From formal rationality to the digital one: side-effects, ambivalences, and vulnerabilities]. *RUDN Journal of Sociology*, *21*(1), 7-17. 10.22363/2313-2272-2021-21-1-7-17

Leukfeldt, E. (2016). Applying Routine Activity Theory to Cybercrime: a theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Limonova, O., & Zharkevich, A. (2020). "S kem my imeem delo?" Formirovanie grupp riska sotrudnikov kak instrument dlia ib-spetsialistov] [‘Whom are we dealing with?’ Formation of risk groups of employees as a tool for IS specialists]. *Informatsionnaia bezopasnost' bankov* [Information security of banks], *3*, 84-88.

Mitnick, K. (2003). *The art of deception: controlling the human element of security*. Wiley.

Mitnick, K. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Hachette book group.

Mitnick, K. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.

Pichkov, O., & Ulanov, A. (2021). Will Robotics Affect the Future of Work? *MGIMO Review of International Relations*, *14*, 197-202. https://doi.org/10.24833/2071-8160-2021-1-76-197-202

Positive Technologies (2021, June 11). *Aktual'nyye kiberugrozy: I kvartal 2021 goda* [Current Cyber Threats: Quarter 1 2021]. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/

Russia public opinion research center (2021, June 7). *Telefonnoye moshennichestvo: masshtaby i poteri* [Phone fraud: scale and loss]. https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-masshtaby-i-poteri

Schwab, K. (2019). The Global Competitiveness Report. Retrieved from http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

Smith, E., Brands, R., Brashears, M., & Kleinbaum, K. (2020). Social Networks and Cognition. *Annual Review of Sociology, 46,* 159-174. https://doi.org/10.1146/annurev-soc-121919-054736

Smith, T., & Stamatakis, N. (2020). Defining cybercrime in terms of routine activity and spatial distribution: issues and concerns. *International journal of cyber criminology, 14*(2), 433-459.