Aspects of Social Engineering and Its Modalities to Countercharge and Prevent It

Valerică GREAVU-ŞERBAN, Floredana CONSTANTIN
"Alexandru Ioan Cuza" University of Iaşi
valy.greavu@feaa.uaic.ro, floredanaconstantin@gmail.com

In an Information Age that has been subjected to the phenomenon of forced digitalization, human propensity towards false information and the susceptibility to social engineering attacks have become a major concern in the field of information security. Nowadays, information security is dependent on the recognition and the user's awareness of risks associated with social engineering attacks since, unlike the mainstream information threats, social engineering not only exploits the technological aspect of illicit information gathering, but emphasizes the manipulation of the human factor in order to accomplish the intended result. Therefore, the preconception that the victim of a cyber-attack is without culpability can be seen as a consequence of the mystification of cybersecurity and a lack of informedness on the part of the typical user.

Keywords: *Social Engineering, Susceptibility, Forced Digitalization, Information Security, Cyber Attack, Recognition, Awareness, Manipulation*
DOI: 10.24818/issn14531305/26.3.2022.01

1 The Human Factor in the Area of Information Security

The global spread of the COVID-19 virus and the permanent necessity for humans to adapt to external factors has led to the accelerated uptake of technology and the phenomenon of digitization, hence the majority of information is presently stored in digital format. This accommodation into the emerging state of normalcy has highlighted the importance of training people to recognize potential cyber threats and the significance of training to use technology properly with integrity, confidentiality and availability of information as benchmarks. Lack of such training fosters distrust in the role of the human factor in information security. Furthermore, the human factor is regularly forgotten to be correlated with information security, [1] which is due to the emphasis on technical and procedural measures needed to address common security problems. As a result, most cyber threats are addressed by intrusion detection systems, firewalls or antivirus software, which is why social engineering is a major threat since it cannot be tackled by these conventional means.

Addressing security from social, technical and cognitive viewpoints is required to effectively handle the human factors implicated in information security. By combining human characteristics with technological characteristics, an organizational culture can be created so that the risks associated with social engineering attacks can be minimized. Whether good or bad, the culture of information security is the key factor in avoiding the potential hazards to which information can be exposed. Through an established training program, users benefit from the necessary knowledge that contributes to a good understanding of social engineering attack strategies and the development of the ability to counter and limit potential intents to cause harm. [2] As a result, in order to reach the stage where maintaining information security becomes an activity performed unconsciously and on an ongoing basis, it is necessary to implement an organizational culture established through the agreement and support of users.

2 Defining Social Engineering

Coercion, psychological manipulation and indoctrination methods are just a small part of the ways in which one person's perceptions, thoughts and beliefs are disrupted or even replaced by another person's perceptions,

thoughts and beliefs. Social engineering also falls into this category. Defining the term "social engineering" presents a degree of difficulty because the definitions associated with social engineering vary on the basis of the medium used to derive them. The earliest reference to social engineering dates back to 1894, during the period of Industrialism when, in his writings, the Dutch radical J. C. van Marken stressed the need to develop technical expertise in the "management of human problems". [3] As defined in the Lexico online dictionary, social engineering is explained as "the use of central planning in an attempt to manage social change and regulate the future development and behavior of a society". [4] This definition limits the purpose of social engineering to exploiting the human factor by harnessing communication and the means by which it is achieved. In the context of its applicability to information security, social engineering refers to the act of deceiving a person to disclose sensitive information, gain unauthorized access, or commit fraud by associating with that individual for the purpose of gaining their trust. [5]

The existence of several definitions associated with social engineering underlines its broad applicability in many areas. Used in political, educational, religious or corporate environments, social engineering is used to redesign the behavior of the masses. Lawyers and psychologists resort to the tactics used by a social engineer to gather insights that would not otherwise be divulged. The government uses social engineering through its authority over the people under its rule, the human brain being conditioned to adhere to authority.

Salespeople are social engineers who use their ability to persuade people to appeal to their needs and satisfy them through the goods or services they commercialize. The examples can of course go on, but those given are sufficient to underline the fact that social engineering is used on a daily basis by people and institutions in various social circumstances.

Regardless of the typology into which social engineering instigators fit, the effectiveness of social engineering is explained by the exploitation of human errors such as: making decisions under the influence of emotions, the desire to help, carelessness in familiar situations and disregard for information perceived as irrelevant.

In order to put social engineering into practice, it is mandatory to study individuals and their behavior in order to facilitate the expected result, no matter the reason for which social engineering is utilized.

3 Systematization of Social Engineering Attacks

Theoretically, social engineering attacks can be mainly focused on either technology or individuals. [6] The technological approach to social engineering is to spoof an application system to get the user to provide confidential information through pop-ups, spam emails, malware, spyware, or phishing attacks. The user may receive a pop-up window that indicates that the computer application currently in use has encountered certain problems that restrict its functionality until the computer application can be re-logged in by entering the ID and password. By entering this data, the hacker who created the pop-up window will be able to access the network and computer system using the user's credentials.

Spam emails contain attachments where a Trojan virus or other malicious program affects systems and networks. The consequences of this attack range from slowing down the system to corrupting records and tampering with the entire communications network. [7]

By spreading a legitimate program containing malware or spyware, the victim can be manipulated into downloading it under the belief that the program is a utility that enhances computer performance.

Phishing attacks are the most common attacks carried out by social engineers [8] in which victims are approached through emails or phone calls. These attacks can be classified into five categories: spear phishing, whaling phishing, vishing phishing, interactive phishing with voice response, phishing through compromised business emails. [9]

All these forms of phishing involve fake websites, PayPal websites, scareware, advertisements, antivirus, free offers or prizes through which the attacker can find out the victim's name, physical address, credit card details, et cetera.

Attacks that target human behavioral weaknesses or involve obtaining confidential information without exploiting technological vulnerabilities illustrate the second category of social engineering attacks.

Impersonation or identity theft involves establishing legitimacy with the victim by linking and integrating data known about the victim into a pretext that facilitates obtaining information. This requires that the social engineer initiating this type of attack has a credible story beforehand that does not arouse suspicion on the part of the victim.

Dumpster diving by a social engineer aims to obtain information-generating goods or documents. For example, if an attacker gets hold of a list with employee names or a list of phone numbers, he becomes the beneficiary of many social engineering opportunities: employee names and phone numbers can be used for identity theft or to initiate a phishing attack.

Trickery, as opposed to scamming or fraud that are implemented for financial or material gain, is often used by social engineers to cause embarrassment or snap decisions on the part of the victim.

Spying and eavesdropping depict types of social engineering attacks implemented by the attacker when in proximity to the victim. These attacks can result in obtaining the user's password when it is written down on documents which are accessible to others.

Consequently, despite its many forms, a social engineering attack involves using social skills to obtain sufficient data to compromise or alter an entity's information systems. [10]

4 Social Engineering Attack Frameworks

In any successful attack carried out by social engineers, a series of stages are followed: information gathering, elicitation, pretexting, mind tricks, persuasion, targeting and recognition. [11]

Gathering information is the most meticulous stage of social engineering which is carried out by observing the victim. The duration of this stage can vary from a few hours to several years because the information is not gathered all at once, being later correlated with one another to create a profile of the victim.

Elicitation can be defined as the ability to extract information through logic, which is why it can be difficult to detect. Essentially, the conduct of this stage is achieved by conducting an inquiry. The role of the social engineer at this stage is to maintain obtaining responses to the questions addressed by being natural, avoiding greed and being knowledgeable about the subject of the conversation. Pretexting illustrates the stage of the attack where the social engineer is in a position to adopt a false identity that can influence the victim to take certain decisions.

The role of the social engineer is to identify the victim's way of thinking in order to use their skills effectively. This is carried out through mind tricks and, depending on the mindset of the interlocutor, the social engineer will resort to emotional manipulation, will pay particular attention to the words that could be used in the conversation or will align himself/ herself/ themselves with the victim's perception of certain topics.

Once the appeal to the victim's interests is successful, the social engineer uses persuasion to get the victim to act on its behalf by establishing defined goals, gaining the victim's trust, through reciprocity or through flexibility.

The targeting stage shows that, unlike other attacks on people, social engineering attacks are formulated for a specific person.

The last stage, recognition, is a form of information gathering through which the social engineer has obtained sufficient data to plot and implement the attack on the intended target.

5 The Applicability of Social Engineering in the Sphere of Mass Communication

We live in the Age of Globalization, and most of society is dependent on communication and information to remain connected to the rest of

the world. We need information to develop our personal judgement on a subject, to socialize with other people or to decide in our day-to-day life, information which the media provide us with. Used as a tool, the media influences and stimulates the behaviors and attitudes of individuals or communities, which is why it dominates the mental life of modern societies. [12] Therefore, the major influence the media exude in fulfilling its objectives of informing, educating and entertaining the masses of people suggests the dual nature of the effects it can have on the masses of people. The media was created to allow information to be easily communicated to a wide audience. This is how the most prominent problem of the media makes its presence felt: the interpretation of information varies from one recipient to another. Because of this problem, there are situations where some people resort to deliberately adjusting the information conveyed in order to get the reaction they want to instill in the audience or to obtain their stated goal. In other words, over time, the media has ceased to be a promoter of empowerment and rationality and has become another means of excluding the needs of the audience. [13] In the last few years, fake news have become the most recognizable consequences of media manipulation that have come to constitute a form of manifestation of social engineering aimed at large communities. Under the pretext of relevant or engaging information content delivered via instant messaging, email or websites, social engineers can initiate malware, phishing and Denial of Service (DoS) attacks. Fake news can take many forms: from spam with grammatical errors to spear phishing emails formulated using details about the potential victim. Most of the time, social engineers convert a fake news article into an attachment or link directing victims to a compromised site. The effectiveness of this form of social engineering attack is due to appealing to human curiosity, the need to keep abreast of the latest events, inducing a sense of urgency or exploiting political affiliation. When the social engineering practices that are formulated around fake news do not impact technology, they focus on reprogramming the thinking of the masses. In this case, the role of social engineer is played by internet subcultures, ideologues, partisan news publications and even politicians. Taking advantage of the opportunities for communication and collaboration among many people that the Internet offers, these groups target vulnerabilities in the news media ecosystem to increase their visibility as well as the audience for their messages. [14] People can pass on manipulated content through the media to promote their own perceptions of people, events, religious or political affiliations, economic situations, etc., in order to get a large audience with the same worldview. Regardless of the social classes spreading fake news and disinformation among the masses, they are motivated by four factors: attention, money, ideology, status. Fake news is spread by individuals to earn money from the attention of the audience; internet subcultures create chaos through fake information for entertainment; politicians with a vested interest propagate certain false information to maintain their public image.

People's dependence on social networks, novelty and sensationalism makes the media vulnerable to manipulation by various social classes, contributing to increasing disinformation and encouraging radicalization.

6 The Evolution of Disinformation and Its Propagation in the Contemporaneity

The longevity of disinformation corresponds to that of mankind's existence. When the serpent told Eve that biting the forbidden fruit would not cause her any negative consequences, that was a disinformation. Pharaoh Ramses II of Egypt deceived the masses of people for a long time by tampering with monuments dedicated to others to make it look like they were celebrating his achievements. [15] The Greeks' entry into the city of Troy during the war was made possible by a disinformation: the Trojan Horse was an offering to Athena, the goddess of war, who was going to make Troy impregnable. [16]

Thus, acts of diplomacy, vendettas, feuds,

state wars and civil wars have been influenced over time by misleading the masses of people, spreading propaganda, satirical writing and by the creative output of people's imaginations. Over time, people's growing affinity for sensationalism and entertainment has led to the emergence of modern newspapers and the encouragement of fake and satirical news circulation. However, the advent of the Internet is the crucial factor that has changed the journalistic norms, the extent of the spread of fake news and the technological and/or social impacts that fake news can have. Information distortion is meant to give some nuance to what might be considered "truth" or even, in some cases, take its place. When falsehood is perceived by the audience as truth, the public's mindset is manipulated, opinions are changed, and misgivings are produced and spread widely.

2016 UNITED STATES PRESIDENTIAL ELECTION

In the aftermath of the 2016 United States presidential election, it was claimed that fake news may have played a key role in the successful election of President Donald Trump. [17] Although the outcome of this election campaign cannot be proven to be strictly due to the spread of fake news on this issue, the objective for which the fake news were spread cannot be disputed: changing unwarranted political attitudes, changing voting behavior or even threatening democracy. Social engineers based in Russia used that political context to stimulate panic among American citizens by deploying phishing attacks to publish fake news intended for voters and by sending corrupted files through fake Harvard University email addresses. [18]

THE SPREAD OF COVID-19

The pandemic that followed the global spread of the COVID-19 virus, and subsequently the SARS-CoV-2 forms, has raised awareness that fake news can threaten the overall health of members of a society. [19] Developed in two waves, the first from mid-March 2020 and the second from January 2021, the pandemic introduced a new widespread political, social and economic phenomenon: infodemics. This phenomenon was introduced by the World Health Organization which, in a wordplay, used the term "infodemics" to sum up the spread of misinformation and false or benevolent information among large communities of people in a single word. [20] Social engineers took advantage of the pandemic context to obtain donations on behalf of the Centers for Disease Control and Prevention, to market counterfeit products (such as test kits), to blame racial groups, governments and immigrants for spreading the virus, and to disseminate chaos and social divisiveness that resulted in anti-mask, anti-vaccine and even anti-5G movements. [21]

THE WAR BETWEEN RUSSIA AND UKRAINE

The most recent and far-reaching politically motivated social engineering attack is the Russia-Ukraine war that started back in February 2022. Russian President Vladimir Putin's invasion of Ukraine has brought relations between Moscow and the West to their lowest level since the Cold War as well as bringing war back into the heart of Europe. [22] The Russian military and intelligence entities have targeted Ukraine through disinformation, trying to portray Ukraine and Ukrainian government officials as the aggressor in this conflict. [23] The Russian president's claims are intended to feed an illusion that Ukraine is instigating violence, which is why Russian military action on Ukrainian territory is indispensable if a global conflict is to be avoided. According to Joe Ondrak, head of investigations at Logically, a London-based firm that tracks disinformation, the Russian rhetoric is supported by a multitude of digital activists who have triplicated fake news about Ukraine [24] so that both Russian citizens and potential powers that might intervene in this conflict are convinced that this political move that could have devastating consequences was a necessity, not a whim to occupy territories.

DEEP FAKE TECHNOLOGY

One fear our society will soon have to face is the susceptibility to deep fake manipulation. Animating works of art, generating the voices of famous historical figures, altering the appearance of actors in the film industry or editing videos of famous people for entertainment purposes illustrate some of the current uses of deep fake. Although deep fake is an innovation in the field of computer imaging and digital sound, the technology has not yet reached its remarkable potential. Distortion, unnatural body movements, lack of blinking, abnormal skin coloring, saccadic movements during speech or unrealistic hair appearance are just some of the clues that can be used to identify actual deep fake implementation errors. As time passes, these clues may no longer be relevant because the appearance and the sound of a person might be precisely mimicked, so the likelihood of detecting social engineering frauds may be minimal. In this regard, the use of advanced deep fake technology offers numerous possibilities for creating fake news and implementing social engineering attacks. This technological advancement diminishes the effort of social engineers to impersonate people and represents a breach of security for companies whose biometric systems are based on voice recognition. At the same time, the ability to manipulate public opinion through fake but credible videos targeting public persons, individuals, authorities and politicians could have devastating consequences. For example, in order to objectively reach a verdict in a criminal case, photo and video evidence is a major contribution to our judicial system. Deep fake can hinder the implementation of legislative power if the evidence is falsified or even worse, it can lead to incorrect enforcement of criminal prosecutions. Deep fake is therefore not just an evolution of propaganda, but a revolution in the manner in which disinformation is created and propagated. [25]

7 Human Propensity Towards False Information

Although people are aware of the negative effects of fake news on society, they are also the ones who actively contribute to its spread. Consequently, education, psychology and behavioral sciences play a major role in developing people as individuals to contain the influence of fake news. The arguments that can explain the propensity of the masses towards false information are numerous: people are persuaded by weak arguments, they do not weigh information properly and, most importantly, they fail to eliminate irrelevant information when forming their beliefs. [26]

As evolved cognitive organisms, humans deal with demanding problems by adopting parsimonious strategies that provide sufficiently precise solutions. [27] This highlights the efficiency of the human brain in not over-analyzing every aspect of life in order to carry out challenging daily activities. The interaction between humans and news cannot be considered a challenging activity, which is why the minimal effort that goes into processing information can lead to the decision to believe fake news. Message credibility is seen as the result of an interaction between source characteristics (e.g. expertise, credibility), message characteristics (related to message content, including factors such as plausibility, internal consistency and quality) and receiver characteristics (e.g. cultural background, prior beliefs). [28] Thus, most people are more likely to follow, consume, endorse and prefer information that fits their pre-existing beliefs or that emanates from an ideologically aligned source. [29] This bias in thinking may be the reason why people choose to believe fake news that reports information with which they agree, or it may have the opposite effect of rejecting fake news whose content does not correlate with the individual's affinities.

Fake news appeal to human emotions to impede rational thinking and to increase an individual's propensity for distorted information. Happy people are prone to make cognitive mistakes, sad people are detail-oriented, and angry people approach an EU critical mindset to quickly emit prejudices.

If fake news is spread to a large number of people, the likelihood of an individual coming

into contact with the news repeatedly is high. This induces a sense of familiarity that increases the credibility of fake news. In other words, fake news become credible because they are easier to process.

Based on data collected from a nationally representative survey in Romania, the main results show that people tend to believe that fake news have more influence on others than on themselves. [30] This mentality that fake news can have no influence on individuals may have developed out of a delusion of superiority or a belief that the negative effects of fake news are reflected in isolated cases.

8 Case Study

According to the previous notions on the factors that determine the propensity of human beings to false information, this paper presents a quantitative research conducted to determine the degree of susceptibility of students at "Alexandru Ioan Cuza" University of Iași to disinformation through their interaction with fake news. The elaboration of the case study was made possible by the selection of the questionnaire as the research instrument and the selection of the individual as the survey unit. Therefore, the questionnaire was completed by 100 students who answered 29 questions. The aim of the research was to identify the factors that determine the credibility of fake news among students.

The main objectives of the study were:

- Identifying the role that students are playing in the proliferation of fake news;
- Identifying students' susceptibility to fake news;
- Identify students' views on the impact that the spread of fake news has;
- Identifying the main social networks used to spread fake news;
- Identifying the main social networks used in the informing process;
- Identifying the criterions considered by students to evaluate the veracity of information sources;
- Identifying the main sources of information chosen by students that offer the highest degree of confidence;
- Identifying corrective measures proposed by students to restrain the spread of fake news in the media.

In order to stimulate the completion of the questionnaire formulated for this study, it has been specified that the data obtained is protected by anonymity and has a confidential character in order to obtain the most representative results from the social category under study. Filling in the questions found in the content of the questionnaire was voluntary, after presenting the objectives and the purpose of the research.

The first section of the questionnaire included the question "Are you studying at university?" in order to distinguish the social category under study from the rest of the people who could have accessed the questionnaire after it was distributed through social networks. As a result, the answer to this question was 100% affirmative.

The next section of the questionnaire contained the remaining 28 questions.

The second question was asked to identify the degree of importance students assign to the proliferation of fake news. Out of 100 responses, 61 respondents gave the highest score for the importance of spreading fake news and 20 gave a score of 4. Thus, a majority of students gave 5s and 4s, underlining their concern about the negative effects that can result from the existence and spread of fake news in the Information Age.

The third and fourth questions ("Have you ever consciously played an active role in the proliferation of fake news?", "Do you consider yourself susceptible to fake news as a student?") were asked to identify what role students play in this problem and whether there is a possibility that they may have contributed to the spread of fake news. Thus, 67% say they do not consciously contribute, but when asked the next question, 63% do not deny the possibility of doing so.

The fourth question aimed to identify the sources that spread fake news. The majority voted that social networks such as Facebook, Twitter or Instagram are the main means of spreading fake news.

Questions 5, 6 and 7 sought the contribution

of social networks to the proliferation of fake news and truthful news. 97% of respondents confirmed that they had encountered fake news on social media, with Facebook being considered the biggest emitter of fake news and the most suitable platform for promoting news.

According to the responses, 49% of students do not share articles on social media by title alone because they give limited trust to the content that circulates online, an idea also supported by the fact that only one person gave the highest score to the degree of trust that they have in mass media.

As far as corrective methods are concerned, the students' opinion was similar, with the majority agreeing that monitoring and controlling the news are important factors in preventing the spread of misinformation. Students also specified different methods to remediate low trust in the media:

- *"There should be penalties for spreading false information";*
- *"Increasing media civic spirit";*
- *"Rigorous control of information";*
- *"The sources from which the news were taken should always be specified".*

When asked "Do you think technology and social media have made you a more informed person?", 56 of those surveyed said they had become more informed, but doubted the veracity of the information they had obtained. 8 people stated that they are more informed because of the news they read, 15 stated that they are not able to trust what they read and only 10 people stated that they are more informed because they question everything they read, being selective with the information they choose to believe.

Respondents' academic background demonstrated that the way they evaluated information was positively influenced by the teachers they interacted with during their university studies.

Verification of websites was recognized by 69% as a factor ensuring veracity. Another factor in ensuring the veracity of information is verifying information via a specialized website, but 77% of people indicated that they had not been put in the situation to use it, an idea supported by the 79 responses associated with question 18: "I have never visited a website to verify the veracity of information". Regarding the significance of the characteristics of an information source, adherence to grammatical rules was rated as the most important characteristic, followed by the name of the publication in which the information appears, the relevance of the information according to the respondent's need, the URL from which the information is retrieved, the completeness of the information and the objectivity of the informational content.

The survey shows that students acknowledge trusted sources of information, with the majority agreeing that Forbes is the most trusted source of information.

In terms of the factors used by respondents to identify the accuracy of information, the most respondents said that students always question whether the information they receive on the Internet is correct. Of the other options used to verify the information sources, the name of the publisher or the opinion of a trusted person are the methods used by the vast majority.

When asked about the notion of deep fake, 78 people confirmed that they had encountered deep fake videos, 10 did not know whether some videos they had watched in the past were classified as deep fake and 12 said they had never encountered such content.

In order to identify the effects of fake news on students during the pandemic and post-pandemic period, question 24 was asked. Most respondents attested that the fake news spread during the COVID-19 pandemic affected their emotional state, with cases where fake news hindered their ability to learn about prevention methods, affected their health or simply had no effect on the students who responded to this questionnaire.

To emphasize the physical or emotional damage that can be caused by the proliferation of fake news in a political and social context, question 25 was asked to which the most responses recorded were "It has affected my emotional state because of the fake events that have been reported" and "It has affected my ability to realize the seriousness of the

situation".
The questionnaire intended for the case study was filled in by people attending bachelor's (78%) and master's (22%) degrees, aged between 18-24 years (79%) and 25-34 years (21%), with a predominance of female respondents, (79%) mainly from urban areas (67%).

9 Conclusions

In conclusion, the study conducted on students at the "Alexandru Ioan Cuza" University of Iași revealed the behaviors of searching for truthful information and the ability to determine the reliability and credibility of news. At the same time, it was investigated the students' predisposition to distribute erroneous information through mass media, particularly social networks.

References

[1] E. Kahraman, *Evaluating IT security performance with quantifiable metrics*, DSV SU/KTH Institutionen för Data- och Systemvetenskap, July 8, 2008, https://www.researchgate.net/publication/250839892 [Accessed 12/10/2021].

[2] I.Ghafir, J. Saleem, M. Hammoudeh, *Security threats to critical infrastructure: the human factor*, The Journal of Supercomputing, 2018, Vol. 74 Iss, 10, pp.4986-5002, https://doi.org/10.1007/s11227-018-2337-2 [Accessed 12/12/2021].

[3] R.M. Feener. *Social engineering through sharī'a: Islamic law and state-directed da'wa in Contemporary Aceh*, Islamic Law and Society, 2012, Vol. 19 Iss. 3, p. 300, https://doi.org/10.1163/156851911x612581 [Accessed 12/10/2021].

[4] Lexico Dictionaries, *Social Engineer: Meaning & Definition for UK English*, Lexico Dictionaries | English, (n.d.), https://www.lexico.com/definition/social_engineer [Accessed 12/10/2021].

[5] P. Cichonski. T. Millar, T. Grance, K. Scarfone. *Engineering – Glossary*, CSRC, August, 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2 [Accessed 12/12/2021].

[6] R.E. Indrajit, *Social Engineering Framework: Understanding the Deception Approach to Human Element of Security*, IJCSI International Journal of Computer Science Issues, Jakarta, 2017, Vol. 14, Nr. 2, pp. 1-9, https://doi.org/10.20943/01201702.816 [Accessed 12/13/2021].

[7] T. J. McCue, *Yikes! here is what happens when you respond to spam emails, plus five tips*, Forbes, 2021, https://www.forbes.com/sites/tjmccue/2020/12/31/yikes-here-is-what-happens-when-you-respond-to-spam-emails-plus-five-tips/?sh=7373ed4024fd [Accessed 12/13/2021].

[8] S. Gupta, A. Singhal, A. Kapoor, *A literature survey on social engineering attacks: Phishing attack*, Proceedings of the International Conference on Computing, Communication and Automation, Noida, India, 2016, pp. 537–540

[9] F. Salahdine, N. Kaabouch, *Social Engineering Attacks: A survey*, MDPI, 2019, Vol. 11, Nr. 4, pp. 1-17, https://doi.org/10.3390/fi11040089 [Accessed 12/14/2021].

[10] Ș. V. Greavu, O. Șerban, *Social Engineering A General Approach*, Informatica Economică, Iași, 2014, Vol. 18, Nr. 2, pp. 5-14, https://www.researchgate.net/publication/273708458_Social_Engineering_A_General_Approach [Accessed 12/14/2021].

[11] E. Ozkaya, *Learn Social Engineering Learn the art of human hacking with an internationally renowed expert Dr. Erdal Ozkaya*, Packt Publishing, Birmingham, 2018

[12] G. Marshall, *A Dictionary Of Sociology*, Oxford University Press, Oxford, 2003, p.405

[13] J. Curran, M. Gurevitch, *Mass Media and Society*, E. Arnold, 1991, p.16, https://archive.org/details/massmediasociety00curr_0 [Accessed 02/14/2022].

[14] A. Marwick, R: Lewis, *Media*

Manipulation and Disinformation Online, Data&Society, USA, 2017, pp.10-26

[15] N. Nielsen, *New evidence shows might of pharaoh ramses is fake news*, University of Manchester, 2018, https://www.manchester.ac.uk/discover/news/new-evidence-shows-might-of-pharaoh-ramses-is-fake-news/ [Accessed 02/16/2022].

[16] Britannica, The Editors of Encyclopaedia, *Trojan horse*, Encyclopedia Britannica, 2018, https://www.britannica.com/topic/Trojan-horse [Accessed 02/16/2022].

[17] H. Allcott, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, Journal of Economic Perspectives, 2017, Vol. 31, Nr. 2, pp. 211-236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf [Accessed 02/17/2022].

[18] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, USA, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf [Accessed 02/17/2022].

[19] S. Bangani, *The fake news wave: Academic libraries' battle against misinformation during COVID-19*, The Journal of Academic Librarianship, 2021, Vol. 47, Iss. 5, pp. 1-8, https://doi.org/10.1016/j.acalib.2021.102390 [Accessed 02/18/2022].

[20] O. Trukhachov, *Elements of social engineering methodology used during the COVID-19 pandemic*, Środkowoeuropejskie Studia Polityczne, 2021, Vol. 4, pp. 5–18, https://doi.org/10.14746/ssp.2021.4.1 [Accessed 02/18/2022].

[21] M. Bitaab, H. Cho, A. Oest, P. Zhang, Z. Sun, R. Pourmohamad, *Scam Pandemic: How Attackers Exploit Public Fear through Phishing*, Arizona State University, (n.d), https://www.ftc.gov/system/files/documents/public_events/1582978/scam_pandemic_how_attackers_exploit_public_fear_through_phishing.pdf [Accessed 02/18/2022]

[22] J. Hookway, *Why is Russia invading Ukraine and what is happening on the ground?* The Wall Street Journal, 2022, https://www.wsj.com/articles/why-is-russia-invading-ukraine-11645570205?mod=search_trending_now_article_pos1&tesla=y [Accessed 02/25/2022].

[23] U.S. Department of State, *Fact vs. fiction: Russian disinformation on Ukraine - United States Department of State*, U.S. Department of State, 2022, https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/ [Accessed 02/25/2022].

[24] Los Angeles Times, *Russian disinformation kicks into high gear as Ukraine crisis drags on*, Los Angeles Times,2022, https://www.latimes.com/world-nation/story/2022-02-17/russia-ukraine-disinformation-campaign [Accessed 02/25/2022].

[25] S. Dack, Deep fakes, fake news, and what comes next, The Henry M. Jackson School of International Studies, July 11, 2019, https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/ Accessed 02/20/2022].

[26] J.P. Forgas, R.F. Baumeister, The social Psychology of gullibility, Routledge, Oxfordshire, 2019, pp. 20-24

[27] D. Tarborelli, *How the Web Is Changing the Way We Trust*, Current Issues in Computing and Philosophy, January 2008, Vol. 175, p. 1, https://www.researchgate.net/publication/228938522_[Accessed 02/23/2022].

[28] C.N. Wathen, J. Burkell, *Believe it or not: Factors influencing credibility on the web*, Journal of the American Society for Information Science and Technology, Ontario, 2002, Vol. 53 Iss. 2, pp. 134–144, https://doi.org/10.1002/asi.10016 [Accessed 02/23/2022].

[29] ***, *Fake news: Why people believe, how it spreads, and what you can do about*

it - ischool: Syracuse University, iSchool, 2021, https://ischool.syr.edu/fake-news-why-people-believe-how-it-spreads-and-what-you-can-do-about-it/ [Accessed 02/23/2022].

[30] O. Ștefăniță, N. Corbu, R. Buturoiu, *Fake News and the Third-Person Effect: They are More Influenced than Me and You*, Journal of Media Research, 2018, Vol. 11 Iss. 3, Nr. 32,pp.5-23, https://www.mrjournal.ro/docs/R2/32jmr1.pdf [Accessed 02/23/2022].

Valerică GREAVU-ŞERBAN has graduated the Faculty of Economics and Business Administration in 1998. He holds a PhD diploma in Cybernetics from 1999 and now is assistant professor to Alexandru Ioan Cuza University of Iaşi.

Floredana CONSTANTIN has graduated the Faculty of Economics and Business Administration in 2022 and is actively pursuing a Master's degree in Business Information Systems at the "Alexandru Ioan Cuza" University of Iasi.