Volume XXIII 2020
ISSUE no.1
MBNA Publishing House Constanta 2020

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Study of social engineering attacks in Romania 2019

To cite this article: Radu Moinescu, Ciprian Răcuciu, Sergiu Eftimie and Dragoș Glăvan, Scientific Bulletin of Naval Academy, Vol. XXIII 2020, pg.263-270.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-20-I1-037
SBNA© 2020. This work is licensed under the CC BY-NC-SA 4.0 License

Study of social engineering attacks in Romania 2019

Radu MOINESCU, Ciprian RĂCUCIU, Sergiu EFTIMIE, Dragoș GLĂVAN

Military Technical Academy "Ferdinand I" – Systems Engineering for Defense and Security Doctoral School
radu.moinescu@gmail.com

Abstract. Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust. In recent years, cybercriminals have done everything in their power to be innovative. They are taking advantage of every aspect of our lives to develop new social engineering schemes. This paper provides an in-depth survey about the social engineering attacks that took place in Romania in 2019, their classifications, detection strategies, and prevention procedures.

1. Introduction

In recent years, cybercriminals have done everything in their power to be innovative. As robust as firewall systems, cryptographic methods, intrusion detection systems and antivirus applications are, social engineering is still a real challenge to cyber security.

Cybercriminals use social engineering techniques, because it is usually easier to exploit the natural inclination of man to trust than to find vulnerabilities or ways to bypass the systems that provide cyber security.

Usually, social engineering techniques are used to distribute malicious content, but in some cases, they are part of an attack, as a factor that allows obtaining additional information, committing fraud or gaining access to secure systems. Social engineering techniques range from random, large-scale attacks that are crude and easily identifiable, to sophisticated, multi-stage attacks, which can be almost imperceptible to legitimate actions.

The present paper presents some of the most frequent and efficient forms of social engineering that were used by cybercriminals in 2019, in Romania, as well as methods of counteracting them.

2. Exploiting the sense of urgency

Vishing is a phishing method that is accomplished through telephone calls (*voice + phishing = vishing*). Perhaps the most popular method of social engineering in Romania is the "accident method", which continued in 2019. The offenders call by accident (or not), either send SMS messages and notify the victims that the son / daughter / brother / sister or one from the parents was involved in an accident and a large amount of money is needed quickly to solve the problem.

In order to convince the victim of the veracity of the information transmitted by telephone, the offenders usually use information available online. Not surprisingly, most of the time, when the victim answers the phone the caller will greet her name.

In order not to become suspicious about the conversation and its need, as a rule, offenders attribute the story to an aura of urgency, because they are aware that this is a weakness of the people who appear when they feel pressured and have to fulfill a task in a given period of time, they may react irrationally.

This social engineering scheme has subsequently moved to socialization platforms as well, being targeted by parents or grandmothers who use them more to keep in touch with relatives in other cities or abroad.[1]

3. Exploiting gullibility

Credulity is the tendency to believe everything easily, without inquiring closely. In the busiest time of the year in terms of online shopping and promotions, cybercriminals test users' vigilance every time, trying to take advantage of their naivety in the face of immediate gains.

In December 2019, a series of social engineering-based attacks were propagated through messages received on social platforms. Users received messages with embedded links, which once accessed gave the impression that they were participating in a contest that could win an iPhone X Max. It should be noted that, this variant of the terminal does not exist, the closest model as name being iPhone XS Max. The web page was designed for mobile devices (featuring JavaScript functions for vibrating user notification, and the page is portrayed). The data originally displayed were: device type, date of access, city and internet provider used. In order to make the message displayed to the victim more credible, the cyber criminals included in the message the idea that other people in the city received such awards. Depending on the device, its settings and internet provider displayed a confirmation page of the chance of winning an iPhone X Max mobile device. Later, the user was transferred to another page where he had 3 attempts to find the prize out of 9 existing variants (boxes). Of course, each time the last box chosen was the winner (Img. 1).

Img. 1. Win an iPhone X Max - viral message luring users to a scam

Also, in order to provide legitimacy to the initiative, cybercriminals have inserted in themselves a series of comments that appeared to be taken from certain Facebook users. In reality, these messages were encoded in the source of the web page.

After choosing the third box, the victim was informed that he had won an iPhone X Max device that is reserved for 5 minutes, a period of time meant to create a sense of urgency, thus diminishing the judgment of the moment.

Subsequently, he is asked to follow "3 simple steps", making a series of redirects to similar pages, which requires sending an SMS with a surcharge to the number displayed, in exchange for services, movies, music or games. Of course, subscribing to such services had nothing to do with the fake competition, being only a social engineering scheme.

It is recommended that you carefully handle phone calls or incoming messages announcing that you have earned certain items or sums of money. Each contest that takes place has, each time, a regulation specifying the method of contacting the winners. Also, before participating in such contests on the Internet, or accessing pop-up messages that encourage you to earn certain items or money, be sure to carefully check the website URL and that the alleged campaign is run by the company mentioned in the message.

4. Exploiting authority and obedience to authority

Obedience is the situation in which the individual changes his behavior following an order coming from a source of influence endowed with legitimate authority. Obedience was studied with interest by Stanley Milgram. He explained obedience by the concept of "agentic state", which represents a psychological state in which the individual accepts "definitions of reality provided by authority", obeys its indications and is considered an instrument in its hands. Thus, the individual does not bear responsibility for the actions carried out under the authority's authority, the responsibility being transferred to the latter.

In view of the high degree of compliance resulting from the incarnation of an authoritarian figure, many roles played by social engineers fall into this category. Being convincing and credible in the role of a person endowed with authority and aiming to believe that he will be responsible for all the consequences of the requested actions, the social engineer will be able to very easily obtain the subjection of the subjects without them being able to question the quality under which they are. is recommended.

The "chief message" social engineering method generally refers to the employees of companies that are authorized to make payments (accounting or financial department). The offenders call or send emails from altered addresses (but there have also been cases in which actual compromised email addresses have been used) to the targeted employees, under the pretext that they are high level managers, and give urgent and confidential to employees to perform financial transactions in a manner that does not comply with the company's internal procedures. The offenders are trying to build their victims' trust by using publicly available information online, which makes any discussion seem credible. A persuasive language is used, such as: "We trust you, stay with us, I am busy now", and the discussion usually refers to a sensitive situation such as control of authorities, procurement, etc. Often, it requires payment to be made to an account outside the country and even Europe.

Business-oriented social media platforms, such as LinkedIn, are a goldmine for cybercriminals when they want to get information about companies, because profiles contain information about business relationships or employee identity and function. Business registers or even company websites can also provide useful information. If the necessary information is not available online, cybercriminals will contact you to obtain this information.

Blocking phone calls or fraudulent emails is virtually impossible. Cybercriminals are able to hide their identity well and can quickly change their approach strategy at any time. The most important recommendation for preventing these attacks based on social engineering is to increase the awareness of the employees, especially from the accounting and finance departments that are targeted by this type of fraud. The following basic rules should be strictly followed:

- do not give information to suspicious contacts and do not follow the instructions in such cases, even if you are under pressure;
- all organizations should check what information is available online;

- procedures must be defined which all employees are obliged to abide by at all times. For money transfers it is recommended to request collective signatures.

5. Exploiting sexual attraction

Sexual attraction is a powerful weapon, and when used effectively the chances of successfully manipulating a target are high. It is most often exploited through the websites of dating ads, online dating or social media. Victims, regardless of sex and sexual orientation, are attracted to cybercriminals, who project a caring image, show seriousness, have high social status and are desirous of serious relationships, but after a while, for various reasons or pretexts, they they ask for different amounts of money or valuables and after they get them disappear in the fog. If the victim does not comply, they resort to blackmail. The victim is threatened with being filmed with the webcam in intimate situations, and the video is to be sent to all contacts in the agenda corresponding to the email address. Thus, cyber criminals demand an amount of about 1000 euros, payable in cryptocurrencies, within 48 hours.

Caution is advised when posting personal data on social media platforms or on dating websites and online dating websites. Check the profiles and photos of the people you correspond with because they can be illegally copied and used. Pay attention to grammatical errors, inconsistencies in information, and excuses such as "my camera / webcam doesn't work." Do not send any compromising material that could be used for blackmail. Check people's profiles and photos, because they can be copied and used illegitimately. If you would like to meet in person, let your family / friends know the place and time. Never send money, avoid prepayments and don't mediate money transfers, because money laundering is a crime.

6. Playing a role

In order to achieve its goals, a cybercriminal will never reveal his true identity. He will always claim to be someone else, inventing a scenario that will increase his chances of believing in the target and achieving its fulfillment. A cybercriminal is able to interpret a variety of roles, depending on the difficulty of entering the target system, the personality of the subjects he will interact with, but also his own abilities. Although it is recommended that the role played by complex, to withstand the checks and to try to cover the unforeseen situations, these things take a long time, especially in the information gathering phase. Sometimes, the simpler the role played, the easier it is to sustain, and it is also more cost effective over time.

Img. 2. Phishing scam that uses the name FAN Courier

On July 23, 2019, cybercriminals used the image of the fast courier company Fan Courier to send malicious e-mail. Users were informed about the status of a parcel shipment. The text of the message received did not contain many details, being apparently automatically generated, but to give a note of authenticity, cybercriminals were used including the name of a company employee. Not having enough information about the alleged shipment, users were tempted to open the attached file, with the .iso extension, called "Shipment Arrival Information", which infected their computer systems with a Trojan with the ability to exfiltrate credentials and financial information (Img. 2). [2]

To avoid falling prey to social engineering scheme it is recommended not to open files received by e-mail unless the source is known and the reference attachment was confirmed by the source.

7. Exploiting the natural tendency to help, compassion and reciprocity

In social psychology, the natural tendency to help falls into the category of types of prosocial behavior. Prosocial behavior is defined as "that intentional behavior, carried out outside the professional obligations and oriented towards the support, conservation and promotion of social values". [3]

When the behaviors of individuals have positive consequences for themselves or others, consequences that can be direct or indirect, we can speak of prosocial behavior. Prosocial behavior, from the perspective of social psychology, refers to acting by virtue of the values promoted and accepted by the society, those positive values that act implicitly or explicitly at the level of a group, society, etc. When it comes to behavior, and especially prosocial behavior, social psychology refers to altruistic behavior, helping behavior, interpersonal attraction, friendship, etc.

Helping behavior is a side of prosocial behavior, because it is defined as an intentional act, performed for the benefit of another person. For helping behavior, intention is a key element. Also, altruistic behavior is considered to be a sub-category of prosocial behavior. These refer to the positive actions aimed at the other social actors, without expecting personal gains for these behaviors. In other words, in social psychology, altruistic behavior is a side of prosocial behavior that does good to a person, without expecting anything in return. [4]

Knowing these issues, even at the level of common sense, cybercriminals exploit the tendency of people to help in many ways. Related to the tendency to help is also the compassion or the feeling of understanding and compassion towards one's sufferings and misfortunes. Compassion involves worrying about the problems of others or the desire to alleviate the negative feelings that others face. Cybercriminals are trying to gain the compassion of the target, which will lower their guard and then be easier to manipulate.

These are used by cybercriminals to sensitize the population to make donations that never reach disaster victims. Not the last cybercriminals can invent human attacks or tragedies in the hope that they will attract potential victims.

8. Exploiting the interest and admiration for celebrities / public figures

Cybercriminals often take advantage of people's interest when it comes to celebrities / public figures. They ask fans / fans to send money for all sorts of alleged reasons - such as claiming prizes, donating to charities, or offering help of some kind. Some celebrities / public platforms are known to raise funds for legitimate causes, but we must make sure every time that the cause and the person requesting this support are real.

Since the beginning of 2019, individuals who used the identities of church figures have requested donations for different social cases, through socialization platforms. But why church figures? According to an INSCOP survey conducted between March 5 and 13, 2019, the internal institutions in which Romanians have the highest level of trust are the Army (68.1%) and the Church (55.1%). [5]

It is also known that the church generally raises money for charitable acts, various social causes or for the erection / renovation of some places of worship. By taking advantage of this, cybercriminals are inventing charitable acts that they promote through platforms to obtain undue income. Most often the images used in the fraudulent schemes are taken from other online sources.

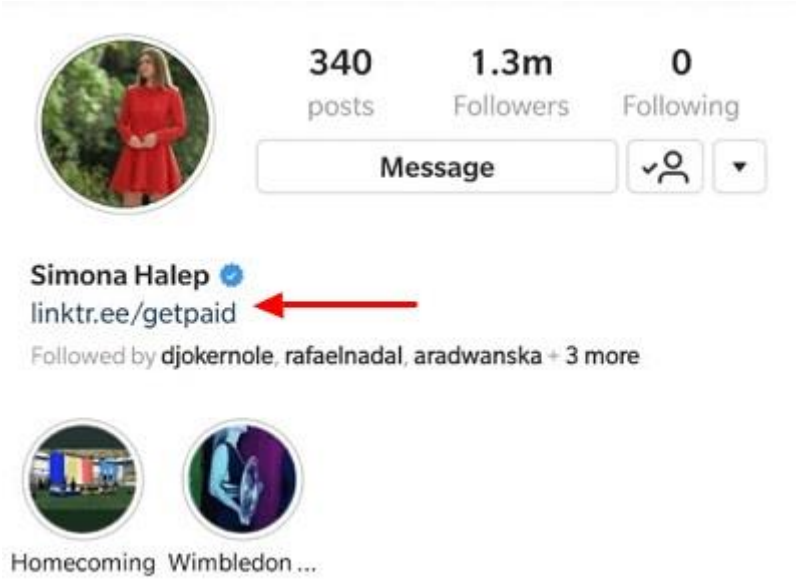
Other times, cybercriminals play the role of a person with whom the victim routinely relates. The tactic is based on the principle of reciprocity, which says that the individual feels obliged to reward in a similar way the gesture of another person. Thus, under the effect of the constraint exerted by this norm, people are determined to help those who have helped them or to give something to a person who previously gave them something. However, this principle makes people more vulnerable to manipulation, as we are obliged to give them a favor even when we did not necessarily want the thing received or when this is practically imposed on us. [6] Moreover, people tend to offer more than they have received, and it follows that the one who first offered always has an advantage. This need to return the aid received also works because of the conformity and the fear of not being sanctioned socially, being cataloged by others as ungrateful or ungrateful. Manipulators often try to lead individuals to concessions through which they try to take advantage of this spirit of gratitude.

Priest Constantin Necula, known to the Romanian public for his numerous appearances at televised conferences and debates, was the victim of online identity theft. Cybercriminals created a fake Facebook account with the identity of the priest, then invented a story that would have made anyone dig deep into their pocket to help. Cybercriminals appealed to different people in the priest's relational circle, trying to persuade them to transfer large amounts of money for alleged treatment. [7]

Before making an online donation, we must consider the following tips:

- if the charity has its own site, it is recommended to check the "WHOIS" information of the domain and the contact address or other details that raise suspicions;
- if the charitable act is promoted through e-mail messages, it is recommended to avoid accessing links or opening attachments (usually the name of these attachments is in the form of "confirmed donation");
- more attention should be paid to charity websites that appear around the holidays.

In July 2019, cyber criminals managed to compromise Simona Halep's Instagram account. They posted several messages on the tennis player's Instagram page, such as: "*If you want to make money taking surveys Swipe up! They pay $ 150 for the first survey you take, worked for me so it definitely can work for you!* ", "*I was hacked, so for all my loyal fans helping me! Free iPhone X's! Swipe up on the next story! Hurry only a few left.*", "*Hey, can anyone help me? I'm stuck in Switzerland and my bank account is not working here. I need $ 500, I'm willing to pay $ 1,500 by the weekend.*" Due to Simona Halep's popularity, cybercriminals hoped to get different amounts of money from at least one of her 1.3 million followers. [8]



Img. 3. Screenshot of a bogus Instagram story posted by hackers on Simona's account [8]

9. Conclusions

With the rapidly increasing dependence on technology, which is evolving very rapidly, it is clear that information protection is becoming increasingly difficult and complex. Much of this complexity tends to stem from the multitude of cyber-attacks. If firewall equipment and antivirus software are generally viable solutions against these types of attacks, the same efficiency and social engineering attacks cannot be talked about. Social engineering techniques are so adaptable and unpredictable that it can never be said that an organization is immune from such an attack.

Generally, organizations attach greater importance to external threats and ignore internal threats from their own employees. Approached by social engineering techniques, employees easily fall prey to the pleasant and seemingly harmless personality of individuals who, through techniques and principles of persuasion and manipulation, manage to convince them to violate internal security rules and procedures and facilitate their way to information. or desired results.

Being based on human psychology, social engineering is very difficult to combat, as it acts exactly in the weak points of the most vulnerable possible target, disregarding laws, morals and ethics and only for the purpose. Corroborating the social skills born or acquired with medium level technical knowledge and with the development and acquisition of specific methods and techniques, the social engineer becomes a significant risk factor in organizations of any kind.

Gaining the confidence of the target is the key to the success of any social engineering attack, whether we are talking about telephone, face-to-face or online approaches. But in order to achieve this effect, the attacker must do intense research and / or behave in such a way that he does not attract any suspicion of the target. Sometimes it can be the manner in which the attacker is dressed and the way he speaks, at other times research needs to be done to find out what are the favorite activities or hobbies of the target in order to acquire them and become so similar to them, thus greatly increasing the chances of being targeted. be perceived as agreeable and credible.

As the company has programmed us to behave in a certain way so that we can coexist within it, we will only be able to reject a person who seems agreeable and well-intentioned. An individual in an organization could never have antisocial behavior in the sense presented above, because if he did, he would probably no longer be an employee of that organization. It is simply a state of normalcy. However, the problem arises when precisely this state is exploited by social engineering.

Of course, with a proper security education, the staff of an organization can detect certain unusual behaviors and block an attack due to this vigilance. For this reason, an objective and realistic risk assessment is required, followed by the elaboration of internal rules and procedures for personnel safety and training to ensure the optimal ratio between efficiency and costs. This assessment must be carried out by specialists in the field of information security, who can provide a complete picture of the vulnerabilities and possible threats. Their underestimation or overestimation inevitably leads to inefficiency and / or poor competitiveness of the organization.

References:

[1] Ştirile PRO TV, *Părinţii sau bunicii, ţintele unei înşelătorii pe Facebook*, November 28, 2018, https://stirileprotv.ro/stiri/actualitate/parintii-sau-bunicii-tintele-unei-inselatorii-pe-facebook.html, accessed on February 26, 2020

[2] Vera IURCU, *Clienţii FAN Courier, ţintele unui atac de phishing prin email*, Start-up, July 24, 2019, https://start-up.ro/clientii-fan-courier-tintele-unui-atac-de-phishing-prin-email/, accessed on February 26, 2020

[3] Adrian NECULAU, *Psihologie socială – Aspecte contemporane*, Polirom Publishing House, Iaşi, 1996, pg.445, ISBN 973-9248-07-1

[4] Psihologie socială, *Comportamentul prosocial*, January 10, 2017, http://psihologiesociala.uv.ro/2017/01/10/comportamentul-prosocial/, accessed on February

26, 2020
[5] INSCOP Research, *22 martie 2019 – Topul încrederii în instituții interne și internaționale*, https://www.inscop.ro/22-martie-2019-topul-increderii-in-institutii-interne-si-internationale/, accessed on February 26, 2020
[6] Nicolas GUÉGUEN, *Psihologia manipulării și a supunerii*, Polirom Publishing House, Iași, 2007, pg.211, ISBN 978-973-46-0540-8
[7] Alin BRATU, *Escrocherie pe Facebook, folosind numele părintelui Necula.”A făcut 27 de conturi false!”*, December 27, 2019, http://www.turnulsfatului.ro/2019/12/27/escrocherie-pe-facebook-folosind-numele-parintelui-necula-a-facut-27-de-conturi-false/, accessed on February 26, 2020
[8] Dan SALES, *COURT OUT Wimbledon champ Simona Halep’s Instagram hacked in bid to scam her 1.3m followers out of £521million*, July 27, 2019, https://www.thesun.co.uk/sport/9599784/wimbledon-champ-simona-haleps-instagram-hacked-scam/, accessed on February 26, 2020