Social Engineering Attacks: Risks, Vulnerabilities and Countermeasures

Luís Costa

Lusófona University of Porto, Portugal
luiscosta205@gmail.com

Abstract. Social engineering is the procedure of fooling someone to act or give information. The attacker tries to take advantage of the victim preferences, needs or emotional state.

In the past some people practiced social engineering, going door-to-door, trying to lure people to give them money or information in exchange for products/services that they supposedly needed. In some, if not most cases, it was a scam. Nowadays this technique evolved and its mostly used online.

This study will show the tactics used by the attackers and how they execute, the risks involved, how to prevent getting caught in one of these situations and if some type of intervention can reduce the effects. By the end of the paper, it's expected to understand how social engineering is executed and some ways to prevent it with security policies and security training awareness, for example.

In our fast-evolving reality, the population needs to get/maintain informed and updated about this problem and learn how to evade it.

Keywords: Social engineering, Persuasion, Prevention, Risks, Awareness, Vulnerabilities, Countermeasures, Security, Phishing

1 INTRODUCTION

The technological world is evolving at a significant pace with the growth and availability of technologies making this one of the main reasons for the fastest and powerful growing of brands, markets and companies [1]. These companies work with online transactions, social networks and have loads of data and information stored on the internet. This stored information looks appetizing for the cyber-criminals and while technology evolves, the number of cyber-criminal attacks and their complexity evolve as well, causing cyber security to play an important role [2].

To prove and demonstrate the cyber-attacks evolution and money involved, on the 2018 Internet Crime Report, the Federal Bureau of Investigation (FBI) received a total of 351.937 complaints with an estimated loss of $2.7 billion [3] and, just a year later on the 2019 Internet Crime Report, received a total of 467.361 complaints, an average of nearly 1,300 every day, with an estimated loss of $3.5 billion [4], showing an increase of at least 100.000 complaints and an estimated loss increase of $800 million in just one year. The data mentioned above are only related to the United States of

10.11228/dpsc.03.01.004

America. According to Cybersecurity Ventures, in 2021, it's expected a monetary loss of $6 trillion worldwide (more profitable market than all major illegal drugs combined), while, in 2015, the real cost was only $3 trillion. These numbers tend to increase annually due to the access to technologies and the internet all over the world [5].

The information systems safety doesn't solely depend on technological countermeasures, the human factors are a huge problem too when it comes to security. Social engineering attacks explore the human factors in order to obtain information and/or access to something. This type of attack succeeds because of human flaws, like the human's natural helpfulness, psychological weaknesses and the underestimating of value of the information they possess [6]. The human component is indispensable for the operations of every company and its also the most vulnerable component to attacks in a company [7].

This paper will focus on the social engineering type of attack. Section 2 will focus on the definition and origin of the concept "Social Engineering" and its subsections will approach types of social engineering attacks, vulnerabilities and countermeasures. At the end of this paper, on section 3, will be a demonstration on how to create a social engineering attack (email phishing attack) on the SET (Social Engineering Toolkit) that comes previously installed on Kali Linux.

2 SOCIAL ENGINEERING

The concept of "social engineering" on the cyberspace field has been around since, at least, 1995, when it was used in the article "Cracking a Social Engineer" by Al Berg, but it has been practiced on other fields (social and political) for much longer [7]. The term was found at the early 20th century on the political field related to social problems, but, at that time, it had a positive connotation. That positive connotation started to change since World War II, when politicians started using this technique to gain electoral advantage [8].

According to [9], social engineering is defined as "influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation" and its acknowledged as being one of the greatest threats to the security of businesses.

As stated in [10], social engineering is an act "to manipulate people, by deception, into giving out information, or performing an action".

In short, social engineering refers to humans as the weakest link because people can be manipulated and persuaded into providing information to attack computer systems or to perform actions that furnish network access to the attacker [11][12].

The attacks on the social engineering field can be classified into two groups (human based and computer based), as represented in Figure 1 [8][13]:

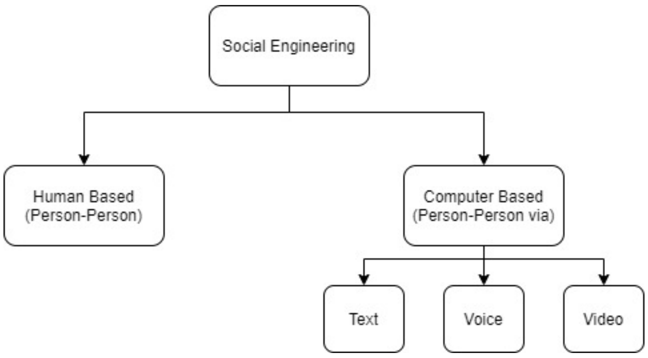

Social Engineering
Human Based (Person-Person)
Computer Based (Person-Person via)
Text
Voice
Video

Fig. 1. Classification for social engineering attacks.

Human-based attacks consist in attacking in person (face-to-face) in order to obtain information. This can be achieved by impersonating a real or fake person.

Computer-based attacks are performed using devices. This type of attack can strike multiple victims in seconds. They can occur via text, voice or video.

It's possible to reconcile the two types of attack in one single attack [8][13].

2.1 Attack Phases

Social engineers use a set of techniques to gain the confidence of their victims. While there are several social engineering attack techniques, Kevin Mitnick [9] created a common methodology to all of these attacks, composed by 4 steps on how to establish a trust relationship with the victims, represented on Figure 2 [12][13][14]:

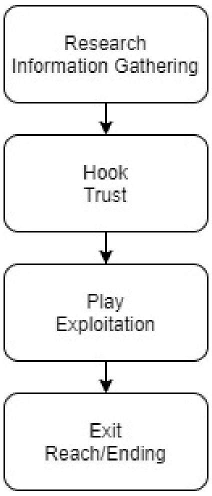


Fig. 2. Attack phases for social engineering attacks.

In the research stage, the attacker chooses the target and tries to gather all the information he cans to create a connection with the victim, while trying to establish some attack possibilities. Next comes the trust phase, also known as relationship development phase, where the attacker starts creating a relation with the victim. Is known that people tend to give away information when they trust someone. In the play/exploitation phase, is expected that the victim already trusts the attacker. The attacker then, tries to exploit the victim to provide private information or to do certain actions through manipulation. In the final step, exit phase, the attacker terminates the interaction with the victim, without raising suspicion preferably, and uses the gathered information to procced to the objectives of the attack [12][13][14].

2.2 Risks

Risk can be perceived as "the possibility that something unpleasant or unwelcome will happen", also known as an attack. For a risk to exist, it must have an associated impact and probability. Impact can be understood as damage, and probability is the chance of the risk happening. If there is no probability of happening, then it's not a risk [10].

2.2.1 Human Based Attacks.

2.2.1.1 Impersonation.

Impersonation consists on the attacker assuming a false or real identity (employee from a targeted company, for example) to keep his real personal identity safe while carrying out an attack to gather information or manipulate someone. It's easy to execute this type of attack and it requires little preparation. Usually is combined with other attacks like tailgating, piggybacking, pretexting and/or reverse social engineering [8][14].

2.2.1.2 Tailgating.

Tailgating is following an authorized person to gain access to restricted areas. It can be considered legal or illegal based on the circumstances. This attack is getting easier to execute because of public databases like LinkedIn, that reveal the organization positions and the name of the people who occupy these positions. [8]

2.2.1.3 Pretexting.

Pretexting can be simply explained as obtaining information under false pretense. For that is necessary a good, fake and convincing story to be able to collect the desired information. Normally is necessary to impersonate an important entity to carry out with this attack, and that requires a lot of preparation [8][13][14].

2.2.1.4 Reverse Social Engineering (also known as quid pro quo).

The attacker impersonates as a person with authority and manipulates the victim to ask the questions instead of the attacker. One approach, for example, used with this type of attack is to previously compromise the network of an organization and then appear with the solution to solve the problem he created, assisting the company in question and gaining trust from the employees. Then he asks the victim to log into the network, achieving his final goal [8].

2.2.1.5 Eavesdropping.

Eavesdropping is when sensitive information is being talked out loud, thinking that only authorized personnel are listening while the attacker is also listening. It can also occur through telephone lines and e-mails [14][15].

2.2.1.6 Dumpster Diving.

The attacker gathers information through the targeted organization's trash. Oftentimes, companies dispose the garbage with documents and even old hardware that contains sensitive information [13][14].

2.2.1.7 Shoulder Surfing.

Shoulder surfing consists on watching the victim writing sensitive information or authentication data [13][14].

2.2.1.8 Piggybacking.

Piggybacking is when an authorized person allows an unauthorized one to enter in a network or physical place (intentionally or unintentionally) [16].

2.2.2 Computer Based Attacks.

2.2.2.1 Phishing.

Phishing is the act of disguising as a trustworthy entity to acquire private information or authentication. This attack is mainly executed through e-mail [8]. Usually this type of scam creates a sense of urgency on the victim in order to manipulate them to act without judging the situation properly [17].

2.2.2.2 Pop-Up Windows Attack.

Pop-Up Windows attacks are windows that appear when visiting a website or when the machine is infected with a malware, that ask for login credentials under the excuse of loss of connection with the server, for example. This attack can also deceive the target under the premise that they won some sort of contest or prize, asking, then, for credentials and personal information or injecting malware on the device [13][16].

2.2.2.3 Baiting.

Baiting, as the name implies, consists in creating a bait, like leaving a USB drive or external disc containing a malware in a public place to be found by the target, that later on, will plug to the computer infecting all the network. Normally the malware attacks on the background, so the victim doesn't know that it's being attacked [13][14][17].

2.2.2.4 Watering Hole.

This attack consists on knowing the legitimates websites that the victim visits often and afterwards search for vulnerabilities in it, infecting the website and waiting for the victim to fall into the trap [14].

2.3 Vulnerabilities

As mentioned before, humans are the weakest link on an organization. Companies could invest millions of dollars on technical security but still have their data compromised, because people need to get educated and informed about the risks and how to proceed on these types of situations [17].

According to [10], there are five flaws of the human psychology that make them vulnerable to social engineering attacks: Follow Instructions, Ignorance, Gullibility, Desire to be Liked and Being Helpful.

2.3.1 Follow Instructions.

Humans tend to think that they decide if they will follow instructions or not. But, in reality, lots of people are getting manipulated every day to do things without questioning. The military, for example, is trained from day one to follow instructions and orders without questioning their superiors. The same can happen when an employee thinks he's talking with some authority entity or superior.

2.3.2 Ignorance.

People, when feeling ignorant, are more open to follow instructions. The IT (Information Technology) field is vast and isn't known by most people and social engineers know that and take advantage of it. If the victim senses he's talking with an expert, they will believe everything and do what they say. This doesn't mean that only people considered less intelligent fall for social engineering attacks.

2.3.3 Gullibility.

When people are offered attractive benefits, their naivety increases. One famous example is the "Nigerian prince" scam. People would receive an e-mail from an alleged Nigerian prince saying that the receiver was a legitimate heir to his inheritance. It was a social engineering attack, where the attacker tried to steal money and information.

2.3.4 Desired to be Liked.

Everybody wants to be liked. In the past, some people connected romantically with foreign diplomats in order to obtain private information.

2.3.5 Being Helpful.

Individuals are encouraged to be helpful in a business environment. Social Engineers use masquerading techniques to impersonate new employees, asking questions about private information, with the excuse that they only need help.

2.4 Countermeasures

Before everything, it's necessary to understand that social engineering attacks can occur to any individual, from executives to cleaning employees. It's important, as well, to perceive that it is impossible to reduce social engineering attacks to zero. What can be done, in that aspect, is mitigating risks and possible damage to infrastructures and data [18].

A good solution to reduce the success of social engineering attacks in an organization, is a multi-layered/multi-level approach, composed of five levels: Foundational level, Parameter level, Fortress level, Persistence level and Offensive/Gotcha level [18][19].

2.4.1 Foundational level.

The roots of information security are the policies. A security policy defines the standards and the level of security of the network and provides procedures and guides for the data and system protection of an organization. It also makes the employees aware of the importance of information's value. Some of the policies that can be found in that document to prevent social engineering attacks are: access approval, password changes and the destruction of confidential documents and old hardware, for example [6][18][19][20].

2.4.2 Parameter level.

Parameter level is the second level and consists in training all users about security awareness. The security policy should be used as a training complement, providing guidelines and motivation. In this level, users will learn about information that can be used by social engineers and types of conversations that they use [19].

2.4.3 Fortress level.

The third level, fortress level, consists in the resistance training of the core staff. Core staff includes everybody that needs to help or talk with the public, for example customer service, help desk and receptionists. The objective of resistance training is to make harder to persuade the key employees, preventing information leaks. This level can be complemented with punishment for employees that break the security policy rules and reminders of the security policy itself [18][19].

2.4.4 Persistence level.

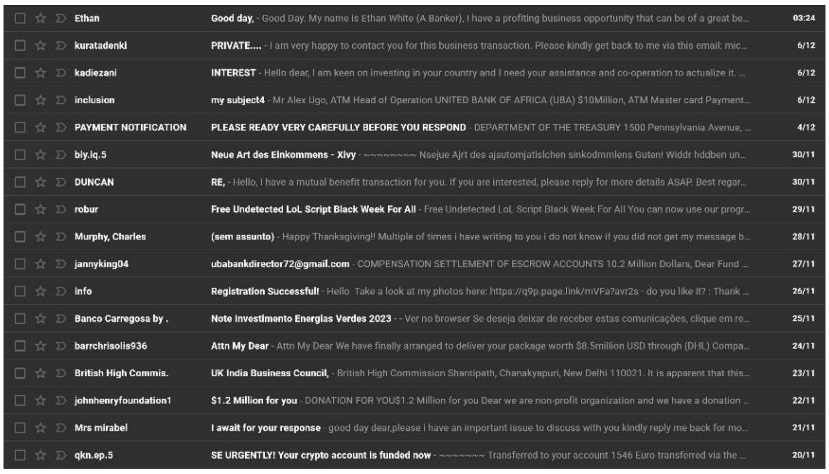
At this level, all the users are reminded, through ongoing reminders, about the necessity of information security. The reminders must be creative and exposed regularly [18][19].

2.4.5 Offensive level/Gotcha level.

Finally, the last level occurs when an attack is happening. The victim will have procedures in place if he suspects that he is experiencing a social engineering attack. To do that, the employee can create traps, called Social Engineering Land Mines (SELMs), that will be able to expose and stop the attackers advance. There are a lot of traps that can be implemented, being the most-known call backs by policy, key questions to the suspect and centralized security logs [18][19].

3 Phishing Attack Example

As previously described, phishing is the act of masquerading as someone in order to scam victims for information or money. People are constantly being victims of phishing and one way to prove that is by visiting the spam folder of their personal e-mail, for example.



□ ☆	Ethan	**Good day,** - Good Day. My name is Ethan White (A Banker). I have a profiting business opportunity that can be of a great be...	03:24
□ ☆	kuratadenki	**PRIVATE....** - I am very happy to contact you for this business transaction. Please kindly get back to me via this email: mic...	6/12
□ ☆	kadiezani	**INTEREST** - Hello dear, I am keen on investing in your country and I need your assistance and co-operation to actualize it, ...	6/12
□ ☆	inclusion	**my subject4** - Mr Alex Ugo, ATM Head of Operation UNITED BANK OF AFRICA (UBA) $10Million, ATM Master card Payment...	6/12
□ ☆	PAYMENT NOTIFICATION	**PLEASE READY VERY CAREFULLY BEFORE YOU RESPOND** - DEPARTMENT OF THE TREASURY 1500 Pennsylvania Avenue, ...	4/12
□ ☆	bly.lq.5	**Neue Art des Einkommens - Xivy** - ~~~~~~~~~ Nsejue Ajrt des ajsutomjatislchen sinkodmmlens Guten! Widdr hddben un...	30/11
□ ☆	DUNCAN	**RE,** - Hello, I have a mutual benefit transaction for you. If you are interested, please reply for more details ASAP. Best regar...	30/11
□ ☆	robur	**Free Undetected LoL Script Black Week For All** - Free Undetected LoL Script Black Week For All You can now use our progr...	29/11
□ ☆	Murphy, Charles	**(sem assunto)** - Happy Thanksgiving!! Multiple of times i have writing to you i do not know if you did not get my message b...	28/11
□ ☆	jannyking04	**ubabankdirector72@gmail.com** - COMPENSATION SETTLEMENT OF ESCROW ACCOUNTS 10.2 Million Dollars, Dear Fund ...	27/11
□ ☆	info	**Registration Successful!** - Hello Take a look at my photos here: https://q9p.page.link/mVFa?avr2s - do you like it? : Thank ...	26/11
□ ☆	Banco Carregosa by .	**Note Investimento Energias Verdes 2023** - - Ver no browser Se deseja deixar de receber estas comunicações, clique em re...	25/11
□ ☆	barrchrisolis936	**Attn My Dear** - Attn My Dear We have finally arranged to deliver your package worth $8.5million USD through (DHL) Compa...	24/11
□ ☆	British High Commis.	**UK India Business Council,** - British High Commission Shantipath, Chanakyapuri, New Delhi 110021. It is apparent that this...	23/11
□ ☆	johnhenryfoundation1	**$1.2 Million for you** - DONATION FOR YOU$1.2 Million for you Dear we are non-profit organization and we have a donation ...	22/11
□ ☆	Mrs mirabel	**I await for your response** - good day dear,please I have an important issue to discuss with you kindly reply me back for mo...	21/11
□ ☆	qkn.ep.5	**SE URGENTLY! Your crypto account is funded now** - ~~~~~~~~ Transferred to your account 1546 Euro transferred via the ...	20/11

Fig. 3. Spam folder example.

As shown on figure 3, there are a lot of e-mails claiming that the addressee won money from some supposed bank or fake entity. A way to forge this type of attacks is through a toolkit called Social Engineer Toolkit (SET), that comes pre-installed on the Linux distribution Kali Linux.

Kali Linux is a Linux distribution based on the Debian GNU that helps companies auditing and penetration testing their IT security systems. This project started back in 2012 when Offensive Security (creator of Kali Linux) wanted to upgrade their last Linux project (BackTrack Linux) that could only be manually updated. This distribution was specifically created to help security professionals and IT administrators [21]. Social Engineering Toolkit is a product created by TrustedSec and was developed on the language Python. With SET is possible to test a large variety of social engineering attacks making it come in handy for every penetration tester and security professional [15].

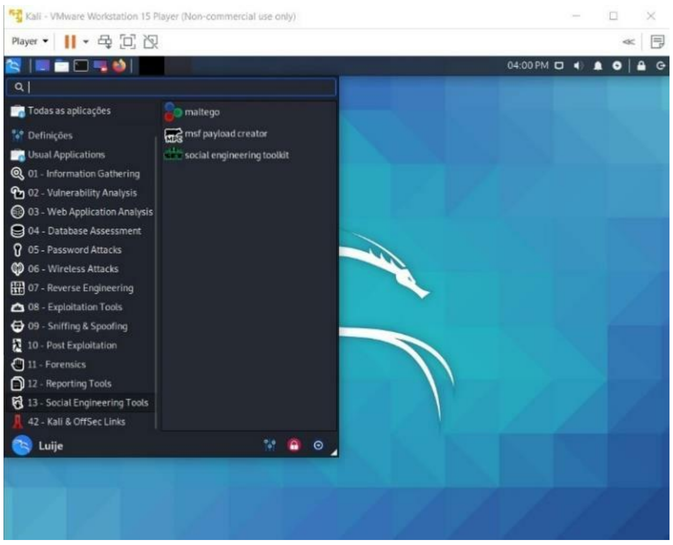
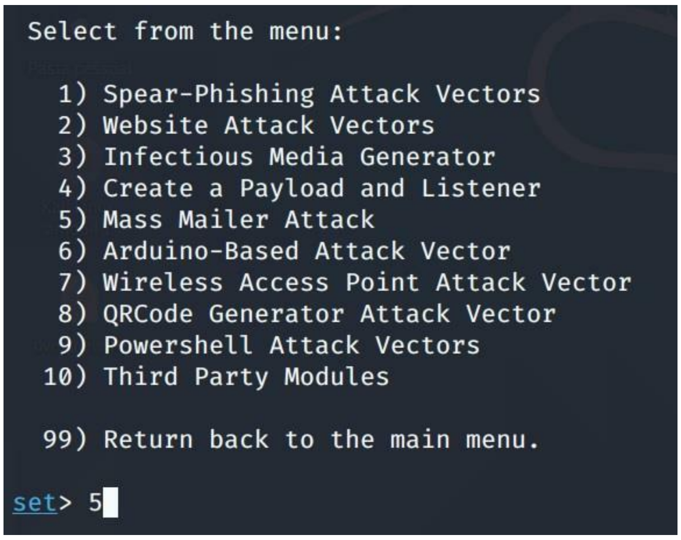


Fig. 4. Pre-installed social engineering tools on Kali Linux.

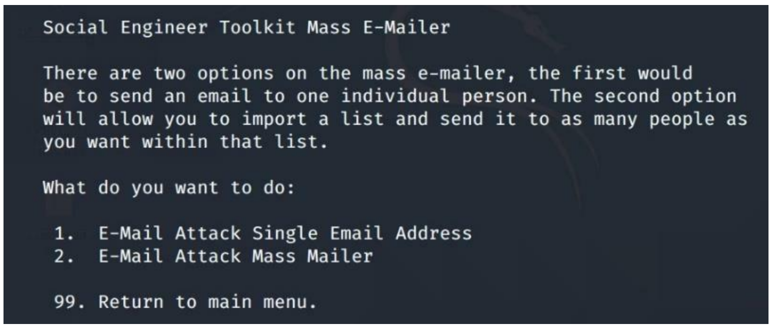
When opened, SET will provide a menu with seven options. Since this study will exemplify a phishing attack via e-mail, the first option was selected (Social-Engineering Attacks), that will open the attacks type list. From there we can choose the desired attack from the list as shown on figure 5.



```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 5
```

Fig. 5. List of SET attacks

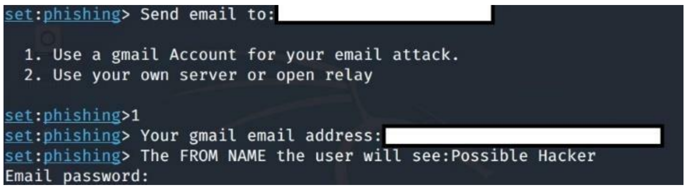
Phishing attacks can be done in two ways on this toolkit: through Spear-Phishing Attack Vectors (focused on website phishing) and Mass Mailer Attack (focused on e-mail phishing). In this case, the Mass Mailer Attack was chosen because the demonstration is about e-mail phishing (Fig.5). After entering the Mass Mailer Attack menu, two options appear: "Attack Single Email Address" and "Attack Mass Mailer" (Fig.6). For the sake of simplicity and demonstration, "Attack Single Email Address" was selected since it only attacks one victim.



```
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

 1.  E-Mail Attack Single Email Address
 2.  E-Mail Attack Mass Mailer

 99. Return to main menu.
```

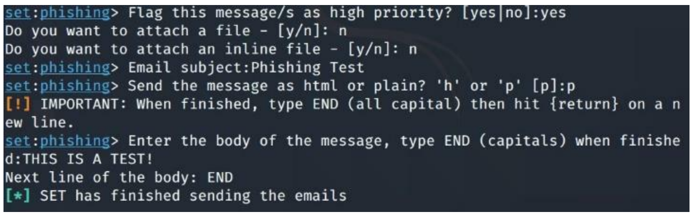
Fig. 6. Mass E-Mailer menu.

After that, some questions will be prompted, asking the receiver email and the sender email, password and "from name" (Fig.7). It will also be possible to flag the e-mail as high priority and to attach files (attackers can attach infected files/malwares). Then the attacker can write the subject and the body of the e-mail and send the attack (Fig.8).



```
set:phishing> Send email to:[redacted]

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:[redacted]
set:phishing> The FROM NAME the user will see:Possible Hacker
Email password:
```

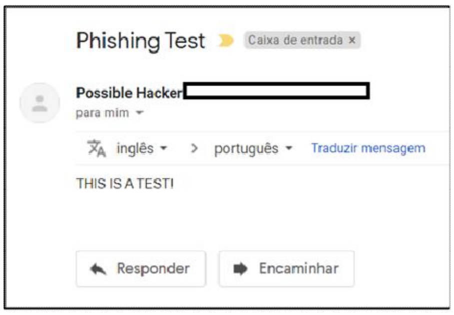
Fig. 7. E-mail related questions.



```
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Phishing Test
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a n
ew line.
set:phishing> Enter the body of the message, type END (capitals) when finishe
d:THIS IS A TEST!
Next line of the body: END
[*] SET has finished sending the emails
```

Fig. 8. E-mail content related questions.

Finally, the result will appear on the victim e-mail inbox or spam folder (Fig.9).



Phishing Test

Possible Hacker [redacted]

para mim

THIS IS A TEST!

Fig. 9. Attack result.

This attack was executed only on one victim, but if the number of target e-mails is bigger, the chance of success increases immensely.

4 CONCLUSION

The expression “Knowledge is power, data is money” [22] couldn’t be more relevant nowadays and on this matter, because that’s what attackers try to do illegally, steal data for their benefit. The access to the world wide web facilitated that process, due to the availability of tutorials and software online that teaches and helps the attackers how to forge an attack, making it even easier to execute one. On that matter, social engineering is one of the most dangerous attacks currently, because it doesn’t require a lot of computer knowledge to be successful which reinforces the idea that is necessary to teach and inform people about the dangers that this type of attacks can cause for companies and even personally and the best ways to prevent it from happening. In conclusion, studying social engineering should be one of the principal focus on the cyber security field, paying special attention to better and more efficient countermeasures, since it’s evolving to be one of the most dominant attack vector in the future and organizations and people in general should be better prepared when that happens.

REFERENCES

1. Sood, A., Tellis, G.: Technological Evolution and Radical Innovation. Journal of Marketing. 69, 152-168 (2005).
2. Bendovschi, A.: Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance. 28, 24-31 (2015).
3. Federal Bureau of Investigation: 2018 Internet Crime Report. (2018).
4. Federal Bureau of Investigation: 2019 Internet Crime Report. (2019).
5. Cybersecurity Ventures: 2017 Cybercrime Report. (2017).
6. Luo, X., Brody, R., Seazzu, A., Burd, S.: Social Engineering. Information Resources Management Journal. 24, 1-8 (2011).

7. Y.Conteh, N., D.Royer, M.: The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. International Journal of Computer (IJC). 20, 1-12 (2016).
8. Ivaturi, K., Janczewski, L.: A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings. 15, (2011).
9. Mitnick, K., Simon, W., Wozniak, S.: The art of deception. Wiley, Hoboken, N.J. (2013).
10. Mann, I.: Hacking the Human: Social Engineering Techniques and Security Countermeasures. Gower Publishing Limited, Hampshire, England (2008).
11. Laribee, L., Barnes, D., Rowe, N., Martell, C.: Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems. 2006 IEEE Information Assurance Workshop. (2006).
12. Gallegos-Segovia, P., Bravo-Torres, J., Larios-Rosillo, V., Vintimilla-Tapia, P., Yuquilima-Albarado, I., Jara-Saltos, J.: Social engineering as an attack vector for ransomware. 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). (2017).
13. Salahdine, F., Kaabouch, N.: Social Engineering Attacks: A Survey. Future Internet. 11, 89 (2019).
14. Breda, F., Barbosa, H., Morais, T.: SOCIAL ENGINEERING AND CYBER SECURITY. INTED2017 Proceedings. (2017).
15. Patel, R.: Kali Linux social engineering. Packt Pub., Birmingham (2013).
16. Maan, P., Sharna, M.: Social Engineering: A Partial Technical Attack. International Journal of Computer Sciences Issues. 9, (2012).
17. Conteh, N., Schmick, P.: Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research. 6, 31-38 (2016).
18. Ghafir, I., Prenosil, V., Alhejailan, A., Hammoudeh, M.: Social Engineering Attack Strategies and Defence Approaches. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). (2016).
19. Gragg, D.: A Multi-Level Defense Against Social Engineering. Sans Institute 2003. (2002).
20. Saleem, J., Hammoudeh, M.: Defense Methods Against Social Engineering Attacks. Computer and Network Security Essentials. 603-618 (2017).
21. Hertzog, R., O'Gorman, J., Aharoni, M.: Kali Linux revealed. Offsec Press, Cornelius, USA (2017).
22. Rossi, B.: Knowledge is power, data is money - Information Age, https://www.information-age.com/knowledge-power-data-money-123458725 (Accessed: December 05 2020).