Social Engineering and the Dangers of Phishing

Vanessa Gomes
ISCTE-Instituto Universitário de Lisboa
MGSI
Lisboa, Portugal
vg.pessoal@gmail.com

Joaquim Reis
ISCTE-Instituto Universitário de Lisboa
ISTAR_ISCTE
Lisboa, Portugal
joaquim.reis@iscte-iul.pt

Bráulio Alturas
ISCTE-Instituto Universitário de Lisboa
ISTAR_ISCTE
Lisboa, Portugal
braulio.alturas@iscte-iul.pt

Abstract — **Social Engineering and phishing technique are subjects that have been evolving as the years pass, mainly through email, which is one of the most used communication tools in the world. Phishing emails are usually related to Social Engineering and may be proposed through links and / or attachments in this type of email, both of which are malicious propagation, and may be hacked into personal / confidential information or even complete control of the computer / email without the users noticing. Several studies have already been carried out showing that there have been more and more attacks of this type and increasingly impacting the population. The research described in this article aims to review prevention methods for this type of computer crime. The research included an exploratory study with a qualitative methodology, through interviews with professionals in the area of Computer Security and later a study with a quantitative methodology, through an online questionnaire.**

Keywords - Phishing Email; Hacker; Social Engineering; Information Security; Prevention methods; Cybersecurity.

I. INTRODUCTION

The phenomenon of phishing is increasingly recurrent in our daily lives and there have been more and more computer attacks related to this type of email. Phishing "is a way of sending messages through e-mail, which seems to be from well-known institutions like banks, governments and multinationals" [1]. The factor that most influences the opening of the e-mail are the promotions and campaigns [2] and uses influence and persuasion to deceive people. The Social Engineer is someone who impersonates another person and uses manipulation, taking advantage of this personification to obtain information, with or without the use of technology [2].

This type of attack comes by falsifying the email content. Email is the "most widely used internet resource and is a fast and convenient way to exchange information on the internet" [3], whether in a professional and / or personal environment. This feature can be considered an easy target for hackers to take advantage of these attacks.

The purpose of this type of email is to get attackers to gain the attention of users and hence their confidence to get the most of the information that can be provided to them [4] and through these emails can be asked to a user who clicks on a link where they are invited to enter their personal data or through attachment downloads that may contain malicious software and which automatically installs a program that gives control to the user's computer.

Most of the research carried out indicates that there are increasing attacks as a result of the lack of knowledge about this topic, including ransomware phishing emails such as WannaCry in 2017 that affected 300,000 computers [5], [6].

This article summarizes another larger work [7] on Social Engineering and the Dangers of Phishing. In section II, definitions associated with Information Security are presented. Section III discusses the concept of Social Engineering as well as the phases of its life cycle. Section IV presents the concept of phishing, commonly used methods, a case study on phishing attacks, as well as some characteristics of phishing. Section V refers to the research question, objectives and addresses the methodology used in this research, namely a qualitative methodology, through interviews with professionals in the field of Computer Security, and a quantitative methodology, through an online questionnaire based on in the responses of professionals, to ascertain the knowledge of respondents on this topic and identify measures that are used by them before and after a computer attack. Section VI gives an analysis of the results obtained and section VII presents the conclusions of this investigation.

II. INFORMATION SECURITY

This section covers the definitions of Information Security and cybersecurity.

A. Concept

Information Security is a topic that has been increasingly talked about lately, so much so that companies are looking for practical and effective solutions, in order to bring optimization of their activities, but at the same time, bring security in their mechanisms of work [7].

Information Security refers to the processes and tools designed and implemented to protect confidential business information. Its main objective is to ensure business continuity and minimize business damage, preventing and minimizing the impact of security incidents [9], [10].

Whitman and Mattord define Information Security as "the protection of information and its critical elements, including the systems and hardware that use, store and transmit this information." Associated with this concept are several characteristics: confidentiality, integrity, availability, known as the "CIA TRIANGLE" and then adding accuracy, authenticity, usefulness and possession [11], [12].

E-mail can be the target of attacks that jeopardize information security, but attacks are also increasingly frequent on online social networks and other platforms. And so, new challenges are posed, on one hand to technicians in an attempt to make web systems more secure and reliable, and on the other hand to crackers, that seek to circumvent with varying motivates and use different attack vectors [14].

B. *Cibersecurity*

Cybersecurity has the function of protecting digital information against cyber crime. This term is used to define any illegal activity where a computer is used to access, alter or destroy confidential information, some of which are identity theft, persecution, intimidation and terrorism [13], [13].

To fight Cyber Crime we have, at a national level, the CNCS (Centro Nacional de Ciber Segurança), whose mission is to implement measures and instruments necessary for the anticipation, detection, reaction and recovery of situations that jeopardize the functioning of state bodies, critical infrastructures and national interests. This institution acts in the event of incidents, cyber attacks and on a prevention strategy by raising awareness among cyber security organizations [15]. At the international level we have ENISA (European Union Agency for Cybersecurity) a cybersecurity reference at the European level, and CERT (Computer Emergency Response Team), whose mission is to solve cybersecurity issues, research security vulnerabilities in software products to contribute to long-term changes in networked systems [15].

III. SOCIAL ENGINEERING

A. *Concept*

Mitnick (2002) describes Social Engineering as: “Persuasion to deceive people into convincing them that the Social Engineer is someone he really isn't, or by manipulation. As a result, the Social Engineer can take advantage of people to obtain information with or without the use of technology” [17].

B. *Social Engineering Life Cycle*

This section covers the concept of Social Engineering and the life cycle phases of Social Engineering see also Figure 1:

- Information Gathering: Handles the acquisition of information from various sources that will assist the attacker in adapting to the attack [17].

- Development of relationship: Develops a relationship between the attacker and the victim to build trust with the user and to appear trustworthy and not arouse suspicion about their act [17].

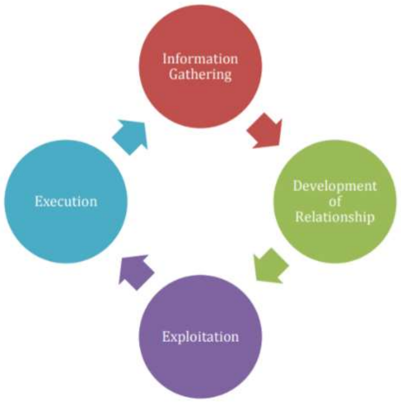

Figure 1 - Life Cycle of a Social Engineering Attack.

- Exploitation and Execution: These are divided into two: Social Engineering technical attacks, which are executed on a technical platform and exploit the victim's confidence. Non-technical Social Engineering attacks, which are executed face-to-face, requiring interpersonal communications and are performed solely by manipulating user confidence [17].

- Execution: When the attack is executed, after the previous 3 steps [17].

IV. PHISHING

This section covers the concept of phishing, commonly used phishing methods, a case study on WannaCry, and some features of phishing.

A. *Concept*

The APWG (Anti-Phishing Working Group), which analyzes phishing attacks reported by various companies, defines phishing as “a criminal mechanism that uses both engineering and technical subterfuge to steal users' personal financial account credentials and information. Schemes used with Social Engineering use fake emails that appear to be from legitimate organizations to mislead recipients, for the purpose of disclosing information such as usernames and passwords” [19].

B. *Most commonly used phishing methods*

The most commonly used phishing method is email. In this method we have the following approaches: the attacker pretends to be someone else, asking users to reply with confidential information; asking users to click on a link displayed, that will redirect them to a fake site. In this approach, logos and trademarks are taken from trusted sites are generally used for the purpose of posting confidential information [19].

The second most used method is via Messengers, spreading phishing messages through automatic messages [19].

The third, most commonly used method of phishing, is web based. In this case, the victim usually enters a website after clicking on an embedded link, in a particular email or a message via Messenger. After clicking on the link, several programs can be installed on the computer in order to steal personal information. It's necessary to take in account that in order for such malicious programs to be downloaded, the user must open a suspicious file [19].

Importantly, both email and automated messaging are the most popular phishing channels and respond to 90% of phishing attacks. Malicious web-based programs lead to 10% of phishing attacks [19].

C. *Phishing Attack Case Study: WannaCry*

WannaCry is a malicious computer attack called ransomware that occurred on a large scale in May 2017. This type of attack is performed on users' computers that are infected through phishing emails, which contain malicious software with a URL (Uniform Resource Locator).

In this case, this type of ransomware spread through a vulnerability found in the SMB (Windows Server Message Block) service used by Windows machines to communicate. Once successfully installed, ransomware blocks user access to files or systems, holding them hostage using encryption until the victim pays a ransom in exchange for a decryption key [21], [21].

WannaCry statistics revealed that hospitals, businesses and at least 150 universities were attacked, with over 300,000 machines infected. 98% of victims were using Windows 7 and only 0.07% of victims paid the ransom [22].

D. Phishing Features

Phishing types are:

- Spear phishing: Focus on large organizations to exploit human error and place the attacker with access to the entire enterprise network, including access to confidential information [23].

- Phishing cloning: Clone from a trusted site where the user is asked to enter their credentials and login, which allows the attacker to save those credentials in a database on their own server and then the attacker redirects the user to trusted sites. as an authenticated user [25].

- Whaling - Aimed at searching for data and information relating to senior positions, which is done through emails or web pages disguised as court notifications, customer complaints or other business issues [25].

The phishing techniques are:

- DNS - Based Pharming: Exploits a DNS (Domain Name System) system vulnerability, and aims to redirect traffic from one trusted site to another fake site and interferes with domain name resolution for an IP address so that the trusted site domain name map to the IP address of the fake site [23].

- Man-in-the-middle-attack: This is when the attacker can secretly intercept the electronic messages between the sender and the receiver and then stick with them to change and modify them during message transmission, whereas this technique essentially uses Trojan horses [25].

- Vshing Scam: The attacker starts by sending various text messages (SMS), emails or even voice messages to the victim's mobile phone. Subsequently and using Social Engineering as a technique, in order to convince the user to call a number, offering various advantages, prizes or assuring that the victim account is locked, requiring some information in order to activate it. Aftewards the user calls to unlock the account, being asked to disclose their personal data. After obtaining all te information, the attaacker can clone credit cards or make financial transactions [26].

- Instant messaging: These are messages that may have untrusted files and links as attachments, and attackers will take advantage of the informality of this type of communication to simulate a false link with the user who will open attachments or load untrusted links [26].

V. Methodology

To study phishing email prevention methods, the following research question has been elaborated: How can we prevent phishing emails?

As a general objective of the research, we intend to answer the question posed above, as well as the following General and Secondary Objectives:

General objectives:

1 - Understand how phishing manifests itself;

2 - Verify the perception of the population before this type of Social Engineering;

3 - Identify prevention methods for phishing cases;

4 - Identify the population most vulnerable to attacks.

Secondary Objectives:

1 - Verify if the context of phishing cases is reached more professionally or personally;

2 - Verify which tools are used to analyze phishing emails in a professional environment.

Regarding the research methodology, two types were chosen: qualitative, where interviews with experts, in the field of Computer Security, were used; quantitative methodology, where we used the instrument of a questionnaire with closed answers, except for one, to obtain quantifiable data, and the questionnaire was conducted based on the interviews.

The interview questions were sent by email and answered in the same way, in total 10 questions were asked, where the interviewee had to answer exclusively to what was asked, and in total there were 7 interviews.

The questionnaire was constructed based on the interviews and was available through the Google Forms platform link for a month and was disseminated through social networks, with 127 responses. Data were processed in the IBM SPSS Statics version 24 for Windows tool.

The questionnaire was divided into two parts. The first part was focused on collecting demographic data, which served to identify the profile of respondents for this research namely: gender, age, level of education, employment status and professional area. The second part corresponding to a set of closed and compulsory answer questions about phishing and Social Engineering where the respondent had to answer on a Likert scale of or 1 to 5, and the last question was open-ended, character answer (not obligatory).

VI. Analysis of Results

This section refers to the analysis of the results obtained.

A. Interviews

For this article the questions posed, with their respective analysis, were only those that are relevant to achieve some of the objectives, namely:

- Forms of phishing manifestation: For experts, phishing manifests itself through engaging emails that are considered to be from known sources and ultimately influence the user to perform a desired action by the attacker. Cracking credentials and spreading malicious files, via attachments and/or links, are two types of attacks most commonly used phishing. The first case being manifested via link access where a page is redirected to an unofficial site, of the proposed site, and that seems official. This with the aim of the user entering the credentials. While in the second case, a download can be made automatically without the user realizing and running a program to steal credentials, this being just a example.

- Population most vulnerable to phishing attacks: Experts indicate that those who are most vulnerable to these attacks are less educated people and, consequently, people with less technical knowledge. They also indicate that the most vulnerable population is unable to detect small details that may indicate the illegitimate origin of the email, ie they are unaware of the security requirements of sender validation, message authenticity or links.

- Population prevention methods for phishing attacks: Experts indicate that users should be more careful about their Computer Security and should take certain precautionary measures. Such as avoiding using public computers to interact with banking entities, maintaining antivirus software and program updated, also take extra care with emails of unknown or dubious origin. In case they consider the email to be phishing, they should delete it without opening it. They should also check whether visited web pages are fully credible and have a security certificate, and your address should start at https:// and if in doubt you should contact a professional in the area to help. Another form of prevention for this type of attack at the professional level is the promotion of information/training via awareness to employees of organizations.

- Tools used to detect / analyze a phishing email: For experts, anti-phishing tools can be used on a personal and/or professional level, as they are open source, open access and unpaid. The tools most commonly used by experts are: “Mxtoolboox” is used for analyzing headers and email content; “Browserling” is used as a virtual machine via browser, and through this virtual machine we can check link content; “Virustotal ”is used to scan all potential malicious links without any risk and to verify information about the potential threat; “Reverse IT ”is used to scan links and files.

B. *Questionaires*

In order to interpret the results obtained from the questionnaires, the sample was characterized by checking that the average age was 30 years old. The youngest respondent was 12 years old and the oldest was 71 years old. The most representative age group is between 25 and 34 years representing 32.28% of respondents. See Figure 2.

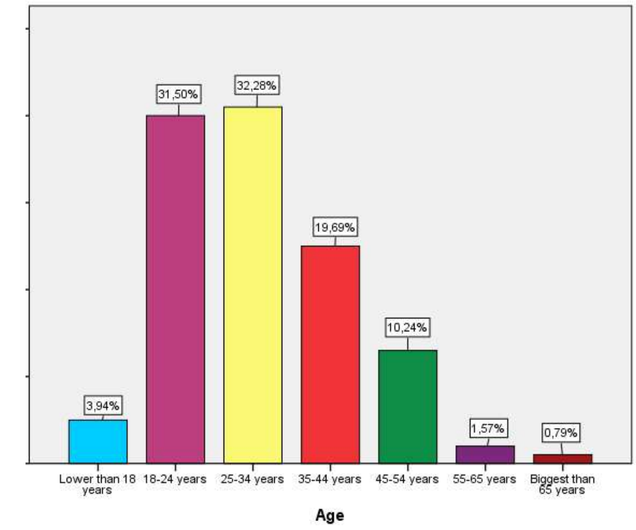

Figure 2 - Distribution by age group

Of the 127 answers, 50.39% were male. In terms of education 44.09% of respondents had secondary education. Regarding their professional situation, 76.38% of the respondents were employed, and 41.73% of the respondents had a professional area Consulting, Management or Informatics. See Figure 3.

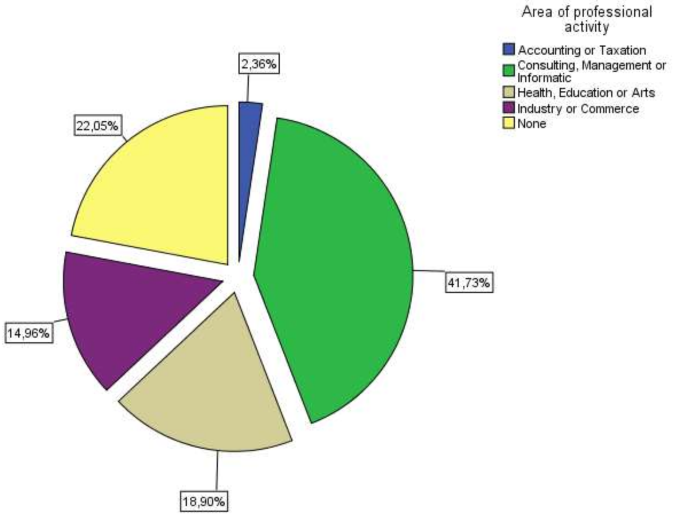

Figure 3 - Distribution by Area of Professional Activity.

A bivariate analysis was performed between two variables to achieve the objectives proposed for this investigation, and one of the variables is always the dependent variable “Have you ever suffered any phishing attacks?”. Note that these results were obtained through the analysis of respondents who have already experienced phishing attacks, and the results were as follows:

- It was found that 25.4% of respondents have heard about Social Engineering a few times, 49.3% of respondents indicated that they have never been subjected to any kind of Social Engineering, 53.5% of respondents indicated that they heard permanently about cybersecurity, 57.7% of respondents indicated that they had heard about hackers permanently. Regarding a fake web page presented, it was found that 66.2% of respondents indicated that the image of the web page was certainly unreliable, 73.2% of respondents indicated that they certainly did not place their credentials on the web page presented. In the case of respondents' knowledge of this topic, we found 52.4% of respondents indicated that they can differentiate between a trusted and an untrusted email, 87.3% of respondents indicated that they know what a phishing email is, 73.2% of respondents indicated that they know Social Engineering attacks could be related to phishing emails, 57.7% of respondents indicated that they know social engineering could be a phishing attack, 73.2% of respondents indicated they would like to have training in the area to avoid being attacked through a phishing email. It was found that in the case of having opened a phishing email, 94.4% of respondents indicated that they did not load links and / or opened attachments, 97.2% of respondents indicated that they did not respond to the email with requested information, 70.4 % of respondents indicated that they would close the email immediately, 59.2% of respondents indicated that they did not point their mouse at the link, not clicking on it.

- Regarding to the measures / actions that respondents took to protect themselves by clicking on a link and / or opening an attachment, the following was found: 42.3% of respondents were always running antivirus, 31.0% of respondents they always disconnected their computer from the network, 36.6% of respondents never formatted their computer, 43.7% of respondents always changed their credentials and 33.8% of respondents never restarted their computer. For measures / actions that respondents were taking to protect themselves from a phishing email, it was found that: 25.4% of respondents are sure to know some kind of phishing email detection method, 45.1% of respondents indicated that surely they should identify / misidentify themselves, 54.9% of respondents indicated that surely they should identify misleading advertisements, 73.2% of respondents indicated that they should always have their computer up to date, 80.3% of Respondents indicated that they should be careful about where they put their personal information, 78.9% of respondents indicated that they should be aware of the email addresses / attachments and 57.7% of respondents indicated that sure that it can be considered a protection measure against phishing emails.

- The majority were found to be between 26 and 50 years old, representing 63.4% of respondents of the questionnaire. Regarding the level of education, it was found that 62.0% of respondents had a secondary level of education. See Figure 4.

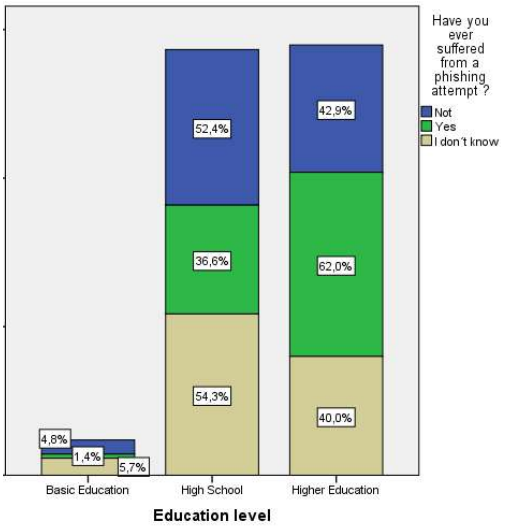

Figure 4 - Educational level / Have you ever suffered from a phishing attempt?

While in the area of professional activity, 53.5% of the respondents had as professional activity Consulting, Management or Informatics.

- It was found that 66.2% of respondents indicated that they use their email professionally, while 53.5% of respondents indicated that they use their personal email. See Figure 5.

VII. Conclusions

Users end up opening phishing emails and then clicking on links and / or opening attachments, even knowing what type of email it is and knowing the danger associated with this type of email, which leads us to identify measures to protect ourselves from email phishing With this study it was possible to answer the research question: how can we prevent phishing emails?

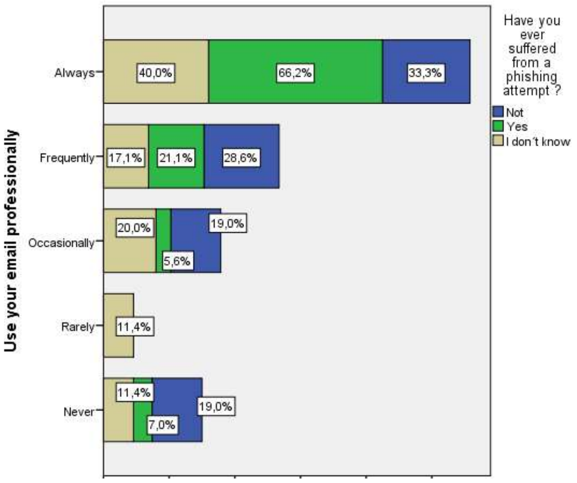

Figure 5 - Use yor email professionally / Have you ever suffered from a phishing attempt?

After analyzing the results, we find that phishing manifests itself through engaging emails in order to influence the user to perform the desired action by the attacker, for example through credential theft or file propagation that could be done through automatically downloaded to your computer and give the attacker the information you want.

Regarding the perception of the population regarding this type of Social Engineering it was found that: respondents who have already suffered phishing attack attempts do not know 100% the topic, as well as the different concepts associated, namely Social Engineering, cybersecurity and hackers; Although most respondents who have already experienced phishing attacks when confronted with a web page can understand when a web page is untrustworthy and should not put their credentials on that web page, some of them are unable to do so; Only 50% of respondents can differentiate between a trusted and an untrusted email; Most respondents know what a phishing email is and they also know that Social Engineering attacks could be related to this type of email and indicated that they would like to be trained in the area to avoid being attacked with this type of email.

Concerning prevention methods for phishing cases, it was found through interviews with experts that users should take certain precautionary measures to avoid being attacked and through these measures several questions were created in the questionnaire to verify the measures used by respondents, In this case, for respondents who have already attempted phishing attacks, it was found that as a protective measure before being attacked, respondents checked where their personal information was placed, paid attention to the addresses / attachments that find in their emails, check if they had their computer up to date, identify misleading advertisements in emails, and then identify erroneous data about themselves, while as a protection measure after being attacked, such as clicking on a link and / or opening an attachment, respondents would change their credentials, start the anti-virus scan and turn the computer of the ethernet. Note that most respondents indicated that training should be considered a protection measure against phishing emails.

Through interviews with experts, it was found that those most vulnerable to this type of attack are less educated and less knowledgeable people, while the questionnaire found that those most vulnerable were between the age of 26–50, and had a higher education level while most had professional acitivty in: Consulting, Management or Informatics. Having said that, and since the interview and questionnaire data do not match, we can consider in the future to make the questionnaire made for this investigation in people with less training and less technical knowledge to verify the truth of what was said by the experts.

About phishing cases it was found that the context of phishing cases is reached more professionally with 66.2% of respondents indicating that they receive more phishing attack attempts through their professional email.

It has been found that the most widely used tools for analyzing professional phishing emails are: “Mxtoolboox”, “Browserling”, “Virustotal” and “Reverse IT”, being used in open source and non-paid environment.

As limitations of this investigation, it is emphasized that the answers to the questionnaire cannot be generalized to the rest of the population, and the veracity of the answers cannot be proven, as the respondents self-completed the questionnaire, unsupervised and it is also noteworthy that the interviews with IT professionals were conducted via email. In this sense, it was not possible to observe their behavior, namely reactions and body movements that could answer certain questions and could allow the elaboration of other questions based on the subject of the interview.

As future work, the same questionnaire could be used by respondents from other countries with different cultures, values and ways of thinking. It would also be interesting to make a phishing email and send it to a group of people checking their reactions to such an email.

ACKNOWLEDGMENT

This work was undertaken at ISTAR-Information Sciences and Technologies and Architecture Research Center from ISCTE-Instituto Universitário de Lisboa (University Institute of Lisbon), Portugal, and it was partially funded by the Portuguese Foundation for Science and Technology (Project "FCT UIDB/04466/2020").

REFERENCES

[1] C. S. Silva, A. C. M. Rosa, D. F. Chaim, R. J. Carvalho and V. C. G. Chimendes, "Engenharia Social: O elo mais frágil da Segurança nas empresas," *Revista Eletrónica do Alto Vale do Itajaí,* pp. 29-40, 2012.

[2] C. Mouro and B. Alturas, "Fatores que influenciam o consumidor a aceitar publicidade via e-mail (Factors influencing the consumer to accept advertising by e-mail)," in *CISTI 2016 - 11th Iberian Conference on Information Systems and Technologies*, Gran Canaria, Spain, 2016.

[3] K. D. Mitnick and W. L. Simon, The art of deception: controlling the human element of security, Indianapolis, IN: Wiley, 2002, p. 368.

[4] W. Oliveira, Técnicas para Hackers II - Soluções para Segurança, Edições Centro Atlântico, 2003.

[5] C. B. Alves, "Segurança da Informação vs Engenharia Social: Como se proteger para não ser mais uma vítima," *Obtenção do grau de bacharel em Sistemas de Informação,* 2010.

[6] Phishme, "Ransomware Delivered by 97% of Phishing Emails by end of Q3 2016 Supporting Booming Cybercrime Industry," 17 11 2016. [Online]. Available: https://phishme.com/ransomware-delivered-97-phishing-emails-end-q3-2016-supporting-booming-cybercrime-industry/.

[7] B. Simões, "O que é o vírus Wannacry, como começou e como está a ser combatido?," 2017. [Online]. Available: https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/o-que-e-o-virus-wannacry-como-comecou-e-como-esta-a-ser-combatido.

[8] V. Gomes, "A Engenharia Social e os Perigos do Phishing," ISCTE-Intituto Universitário de Lisboa, Lisboa, 2019.

[9] M. Peixoto, "Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações," Dezembro 2004.

[10] CISCO, "What is Information Security?," 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html. [Accessed 29 12 2018].

[11] R. Von Solms, "Information security management (3): the code of practice for information security management (BS 7799)," *Information Management & Computer Security,* vol. 6, no. 5, pp. 224-225, 1998.

[12] ISO, "Information technology -- Security techniques -- Code of practice for information security management," 2005. [Online]. Available: https://www.iso.org/standard/50297.html.

[13] M. E. Whitman and H. J. Mattord, Principles of information security, 3rd ed ed., Thompson Course Technology, 2009.

[14] D. Monteiro and B. Alturas, "Segurança e Privacidade na Web 2.0: Foco nas Redes Sociais (Web 2.0 Security and Privacy: Focus on Social Networks)," *Egitania Sciencia,* no. 10, pp. 109-133, 2012.

[15] M. A. Mendoza, "Cibersegurança ou segurança da informação? Explicando a diferença," 2017. [Online]. Available: https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/.

[16] V. Upadhyay and D. S. Yadav, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies: Current Technologies," *International Journal of Engineering Research And Management (IJERM),* vol. 5, 2018.

[17] CNCS, "Missão e Competências," 2018. [Online]. Available: https://www.cncs.gov.pt/sobre-nos/missao-e-competencias/.

[18] A. Leite, "A problemática da cibersegurança e os seus desafios," Setembro 2016.

[19] D. Stergiou, "Social Engineering and Influence," *A Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles - MasterThesis,* 2013.

[20] APWG, "Phishing Activity Trends Report - 1º QUARTER 2018," 2018. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf.

[21] I. Bose and A. C. M. Leung, "Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities," *Communications of the Association for Information Systems,* vol. 19, pp. 544-566, 2007.

[22] A. Koujalagi, S. Patil and P. Akkimaradi, "The Wannacry Ransomware, a mega cyber attack and their consequences on the modern india," *International Journal of Management Information Technology and Engineering,* vol. 6, no. 4, pp. 1-4, 2018.

[23] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5, 2017.

[24] J. Crowe , "WannaCry Ransomware Statistics: The Numbers Behind the Outbreak," 5 2017. [Online]. Available: https://blog.barkly.com/wannacry-ransomware-statistics-2017. [Accessed 17 12 2018].

[25] C. G. Pereira, "Phishing: Conceitos e ações preventivas aplicadas à empresa," Instituto CEUB de Pesquisa e Desenvolvimento - ICPD, Brasília, 2012.

[26] M. N. Banu and S. M. Banu, "A Comprehensive Study of Phishing Attacks," *International Journal of Computer Science and Information Technologies,* pp. 783-786, 2013.

[27] P. Gil, "What Is 'Whaling?'," 2018. [Online]. Available: https://www.lifewire.com/what-is-whaling-2483605. [Accessed 15 12 2018].

[28] D. Martins, Phishing Scam:, Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2008.