Social Engineering Aspects of email Phishing: an Overview and Taxonomy

Igor Tomičić
Faculty of Organization and Informatics, University of Zagreb
Artificial Intelligence Laboratory; Center for Forensics, Biometrics and Privacy
Pavlinska 2, 42000 Varaždin, Croatia
Email: igor.tomicic@foi.hr

***Abstract*— Numerous online resources and reports are pointing to the growing effectiveness of email phishing techniques, with some indicating that 85% of IT breaches involve the human element, and that 96% or social attacks arrive via email. Phishing is a common occurrence, and a significantly successful one. While most of the available research on phishing involves phishing detection, prevention, filtering, anti-phishing tools, techniques and countermeasures, the remaining body of research is tackling phishing and social engineering in (too) generic and broad contexts. This paper will propose a focused effort to identify the specific groups of techniques that attackers are using in email phishing and the principles running "behind the scenes" that make these attacks successful. Thus, the goal of this paper is threefold: (1) to propose a taxonomy of the observed email phishing techniques, (2) to associate the principles and factors of influence with observed techniques and shed light behind their effectiveness, and (3) to raise awareness and lay the groundwork for working on the model of human resilience against these manipulative forms of cyber attacks.**

Keywords*— *social engineering; email; phishing; taxonomy

I. Introduction

According to the Verizon Data Breach Reports from 2020 and 2021 (DBIR), 85% of security breaches involved the human element, almost 100 % of social attacks in the public administration sector involved phishing, and 96% or social attacks arrive via email [1]. Some reports state that Internet users on average receive 117 emails per day and that 53% of such emails are spam [2]. Even if the automated spam filters are successful in blocking them 90% of the time, users could still experience few phishing emails in their inboxes every day - and it only takes one wrong click to become compromised. Related statistics can be found via numerous other online resources, emphasizing the importance of further research that needs to be conducted within this domain. Although phishing attacks can be simple and generic, the most successful ones are often highly targeted and elaborate, collecting the publicly available knowledge about the target using OSINT tools and techniques, and leveraging the principles of psychological influence for delivering highly effective campaigns. Technology is ever-developing at rapid speeds, enabling both more sophisticated attack and defense methods and techniques. However, within the same time frame, the human mind has remained relatively unchanged in its basic susceptibility to targeted manipulation. Thus, the main motivation of this work is to shed light on these manipulative techniques and to raise awareness of their existence and usage in phishing campaigns, so people could be trained to recognise indicators of manipulation and do so in a relatively automated fashion.

Phishing is a type of a complex socio-technical attack based on social engineering and interconnecting areas such as social psychology, information security, technologies in general, communication artefacts, even organisation processes. Phishing uses fraudulent communications crafted, for example, with the goal of tricking a person into revealing sensitive information to the attacker, or to deploy malware on the victim's infrastructure, often creating a gateway for future attacks. Phishing seems to be the most common type of attack in a cyber landscape. For example, FBI's Internet Crime Complaint Centre recorded 6 times more incidents of phishing than identity thefts in 2020 [3].

Phishing utilises a category of web threats called semantic attacks, where the focus is typically not on technical vulnerabilities, but on findings of how humans assign meanings to the message contents or interact with computers [4].

This paper is focused on email-related phishing attacks, as this vector is the most prevalent one.

II. Principles of Influence

The effectiveness of the phishing campaigns might be related to psychological principles of influence/persuasion presented by Cialdini [5], which are labeled as follows: reciprocity, commitment and consistency, consensus or social proof, authority, liking, scarcity and unity.

Reciprocity describes the inherent human need to give back to others the form of a behavior, gift, or service that they have received first.

Consistency manifests through people needing to be consistent with their previous attitudes and/or behaviours; it is usually triggered by asking for small initial commitments which could, after complying, lead to bigger ones. People have

aligned commitment with their self-image, so this mechanism is often exploited.

Social proof describes the state in which people tend to look to the actions and behaviors of others to determine their own, which more often happens in states of uncertainty. Social proof is often fabricated in order to trigger and exploit this principle.

Authority describes the state of mind in which people follow the lead of credible, knowledgeable experts - or the ones that are impersonating authority figures.

The liking/sympathy principle establishes that people prefer to comply with requests of those that they "like". Liking in this context is based on several factors, such as physical attractiveness, similarity, sincere compliments, contact and cooperation towards mutual goal. Liking is also triggered by showing vulnerability and using humor in establishing rapport.

Scarcity is not only restricted to physical resources, but to the limited time, limited stock, exclusivity, limited number of spots, etc. These limitations are often fabricated.

The unity principle states that more one feels like part of a group, the greater the chances to be influenced by that group. To exploit this, one has to provide the illusion of a shared identity, interests, goals, etc.

Throughout the years, these principles were exploited in a number of domains [5], and in modern times they are being widely used in the phishing and other forms of social engineering campaigns [6], [7], [8], [9].

Akbar [9] presented a quantitative analysis on suspected phishing emails and found that authority and scarcity were disproportionately the most exploited principles, followed by liking, consistency, reciprocation, and social proof.

III. Related Work

The lack of "a detailed and systematic discussion on the phishing techniques" is noticed by authors in [10], claiming that researchers are "more focused on the discussion of anti-phishing as opposed to phishing" itself. Similar observation was perceived in writing this paper, with observed discrepancies between categorisations of phishing attacks across different papers, inconsistent terminology and phishing domains. The review of related work presented within this section should shed a light on such cases, and later try to reconcile those diverse aspects. Moreover, most papers within the domain are tackling phishing in general, some even generalising to other forms of non-technical social engineering attacks. This paper however, is focusing on email-related phishing attacks because of their exceptional spread and effectiveness, making them often self-sufficient as an attack vector.

The authors in [11] describe phishing as a type of spam that employs two different techniques - social engineering schemes (spoofing a legitimate company, placing links to spoofed (fake) websites, etc.) and "technical" schemes, which rely on malware or security vulnerabilities found in user's system that would support target malicious activities. Such categorisation has its limitations - malware could be delivered by email and the incentive to open/click it could come from social engineering techniques. Attack on the vulnerable components of the user's system might not be related to phishing at all, if it does not include some form of user interaction - and if it does, than it also relies on some form of behavioural manipulation.

In [12] authors recognise two aspects of phishing; one with respect to target specialisation (such as spear-phishing which could lead to a business email compromise [13], [14], or "Fire-and-forget", the most common type according to [15]), and the other with respect to the attack vector (malicious attachment, phishing link). Authors also included several strategies for fighting phishing, such as user training, automated identification of phishing emails, domains, and websites, and aiding users in spotting suspected phishing emails or websites by providing warnings. The paper, however, does not dive deeper into the email phishing techniques themselves.

Authors in [16] are acknowledging several psychological factors within the phishing context. They are referring to manipulations with human curiosity, fear and empathy on top of "traditional phishing techniques" in order to trick the users into submission. Use-cases for all three aspects are provided within the paper. Authors also classify phishing attacks into a range of "techniques": spear phishing, clone phishing, malware-based phishing, search engine phishing. Such classification has its merits, although it may be considered incomplete and somewhat inconsistent, mixing both the target categories and attack vectors/deployment methods.

Authors [17] summarise phishing domain into two aspects: phishing categories (clone phishing, spear phishing, phone phishing, DNS-Based Phishing (Pharming), Man-in-the-middle-attack), and phishing attack techniques (email spoofing, web spoofing, DNS Cache Poisoning, malware). Clone phishing is a term which seems to be used throughout the academic literature and popular articles in two ways: (1) as a method of cloning a legitimate website, or (2) as a method of cloning and modifying a legitimate, previously sent email, all with the intent of utilising the Cialdini's "liking" principle of persuasion [5] for exploitation. DNS-Based Phishing (mapping the domain name of a genuine web site onto the IP address of a rogue website) and man-in-the-middle-attack are usually executed through technical vectors, where social engineering is rarely used - similarly as DNS Cache Poisoning, which authors included again within phishing attack techniques. Also, email/web spoofing and email/web cloning could easily refer to the same phishing methods, respectively.

Web phishing strategies are organized into three groups in [18]: (1) mimicking attack (effectively the same as clone phishing described before), (2) forward attack (a victim clicks on the link provided via phishing email, the link lands on the attacker's website where the victim leaves her personal information, after which it is forwarded to a legitimate site to minimise suspicion), and (3) pop-up attack (the victim is asked to leave her personal information in the attacker's pop-up window delivered by the MITM technique). From the perspective of our paper, where the focus rests on the email phishing, the analysis deals with the email contents - why would the victim be compelled to click on those links in the first place; which mechanisms are in play, which psychological

principles of influence are employed - all of which is not addressed within [18].

Phishing attack methods and defense techniques from five perspectives are described in [19]. Authors tackle the life-cycle and motivation of a phishing attack, distribution methods, taxonomy of various phishing-attacking techniques (Figure 1), provide phishing protection mechanisms and present some performance challenges faced by developers dealing with this domain. Although their taxonomy provides a basic orientation of the phishing context, it is important to note that smishing is susceptible to social engineering techniques in similar ways as email phishing is; and vishing is especially subjected to social engineering, as documented in numerous real-world examples such as presented in [6]. Therefore, there should be a clear link between social engineering and smsishing and vishing within the published taxonomy presented in Figure 1. In relation to the taxonomy proposed within this paper, the taxonomy by [19] does not provide an insight into the email phishing techniques.

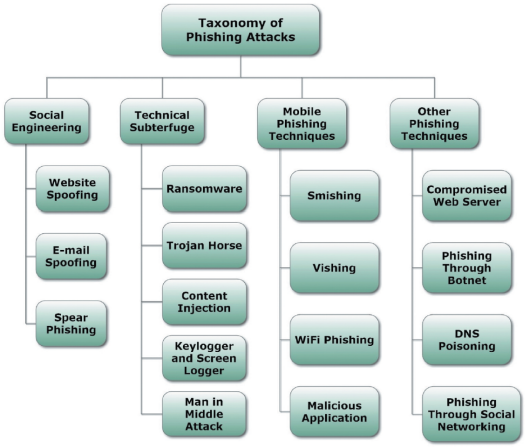

Fig. 1: Taxonomy of phishing attacking techniques by [19]

Authors in [20] have summarised several phishing trends, adding 2 of their own (smishing and vishing) on top of the work presented in [21], which includes: (1) the money scam (mainly targeting human greed in the context of offering some kind of money compensation), (2) information scam (targeting confidential data from the user with the aim of later using it for other malicious purposes - attacker usually present itself as an authority figure in order to exploit human susceptibility to authority, or as a recognisable/reputable institution like a bank, targeting the liking principle of influence, or fear, by using strong action words of threats, consequences and the lack of time to react (utilising the scarcity principle)); (3) malware distribution; (4) multiple file extensions (referring to hiding the real file extensions); (5) disguised links (including cloaked/obfuscated links, misleading named links, Homograph URLs); (6) spear phishing (requiring previous reconnaissance on the target for email customization); (7) Business Email Compromise (sending emails from the compromised or spoofed email accounts, often from the same organization, belonging to some high-ranking individual). Again, this summary of phishing trends cover some of the most important techniques and categories, but do so without apparent structure, which is a challenging task when including phishing across multiple vectors (email, web, voice, sms, even f2f), considering how the same techniques could be effectively used across several of such domains.

Interestingly, authors in [22] have recognised the importance of emotional triggers elicited by phishing emails and have created "a human-centric notification mechanism that extracts prospective psychological triggers, possible malicious intent, and a representative summary from emails." They present these findings to the user in a meaningful way to facilitate a better decision-making process. The work leverages transformer-based machine learning to "(i) analyze prospective psychological triggers, to (ii) detect possible malicious intent, and to (iii) create representative summaries of emails" [22].

Phishing emails often exploit the reciprocity principle (by engineering the context in which the victims feel like they have to return the favour), social proof (creating the impression that "other people" have already done the thing that is asked from the potential victim), and scarcity (creating the impression that the opportunity is limited, or that something has to be done as soon as possible, artificially limiting the time to react).

IV. Materials and Methods

After the systematic overview of the existing literature on the subject of email phishing techniques, hundreds of phishing emails were qualitatively analysed in order to find the indicators of manipulative techniques present in the email headers, subject lines and in the body of email messages. Phishing emails were collected, analysed or re-interpreted (1) from the existing literature review presented in Section III, (2) from the authors' personal collection, (3) from the Cornell University "Fish Bowl", a collection of phishing emails that have been spotted at Cornell [23], (4) from an archive of spoof email and phishing scams [24], and (5) from numerous web articles that have presented various phishing scenarios. During the analysis, various technique patterns were categorised according to their primary target (machine or human) and scope, creating a taxonomy of used techniques.

The paper associates identified email phishing techniques with the Cialdini's work on the principles of influence [5] in an effort to shed light on the evident effectiveness of the phishing email techniques. As those principles are already proven to work in other non-technical contexts, their universal nature is here applied to manipulative email communications. While not explicitly covered through these principles, other related emotional states are also considered, such as greed, fear and compassion/empathy, as significant factors of influence.

V. Email Phishing Techniques in the Wild

This section presents various phishing techniques and tricks discovered in the analysis of online sources and hundreds of different phishing emails. There are two major categories of

phishing techniques identified through the analysis - machine-oriented and people-oriented. Machine-oriented techniques are designed specifically to bypass the software-based email filters and scanners. People-oriented techniques are crafted with the goal to deceive humans through one or more of the influence principles and factors associated with a specific technique. As this paper is focused on the social engineering aspect of email phishing, machine-oriented techniques will be tackled in less detail. Naturally, there are hybrid approaches used with the capacity to deceive both human and software.

A. Machine Oriented Email Phishing Techniques

Some of the identified machine-oriented email phishing techniques are listed as follows:

1) The inclusion of legitimate links. If the email contains hyperlinks which lead to legitimate, well known websites, such an email would also look legitimate - both to software filters and humans [25].
2) Obfuscation of brand logos [25], [26]. Some email filters scan for signatures of HTML attributes that compose company logos, in an effort to detect misusing the logos for deceitful purposes (brand impersonation protection). Such attributes could be changed in ways that are invisible to human eyes, but the logo would become unrecognisable to a software filter.
3) Using less content and noise [25]. If there is no content to scan, the email filters could mark an email as safe. Therefore, the attackers could use images that contain text fused within them, instead of using the text format itself, which is usually not obvious to the average victim and would remain undetectable by some filters. Although, more sophisticated anti-phishing filters use optical character recognition to recover such text and identify potential phishing.
4) Mixing legitimate and malicious code [25]. This technique is used to avoid signature-based detection, and is used more often in phishing pages. A phishing page can for example include CSS and JS code from the legit corporate web pages [26]. The signature can also be obfuscated by adding random values, blank spaces, etc.
5) Linking most of the code in an external JavaScript file.
6) Inserting invisible Unicode characters to break up keywords. This technique is performed in a phishing email body or subject line, in order to bypass automated detection [26].
7) Zero-point font obfuscation [26]. Attackers insert hidden words with a font size of zero into the body of an email in order to avoid machine learning detections.
8) Using procedurally-generated graphics for brand impersonation [26]. There are reported cases of using HTML tables to imitate the logos and branding of legitimate and trusted organizations.

B. People Oriented Email Phishing Techniques

In people-oriented phishing techniques, the goal is to manipulate the perceived context and to deceive a human target. There are two main categories of such attacks: bulk, and personalised (spear) phishing. The bulk phishing techniques are described here as "generic" in the sense that they could be employed to any context or a victim profile.

The following people-oriented bulk email phishing techniques were identified:

1) Using URL shorteners. URL shorteners, as their name suggests, are services that are primarily and legitimately used for the reduction of long URLs. As such, they can completely mask the original (target) URL, as the two are mostly lexically unrelated and have no visual resemblance. The attacker could use this feature to mask any link needed for the attack to succeed. This technique does not directly utilise principles of influence, but can be used after a successful persuasion.
2) Using anchor texts. Links can also be hidden "below" anchor texts, which are usually designed to further motivate clicking on them (for example, "Click here now to renew your account", or "Microsoft Helpdesk", or "CLAIM YOUR ACCOUNT NOW"). They are also in many cases used in combination with URL shorteners to further avoid detection. Revealing links underneath the anchor text by "hovering the cursor" is especially challenging on mobile devices. Principles which are used via the anchor text depend on the message context, such as authority, liking, scarcity, fear, commitment.
3) Using redirections. There are two major techniques used here. Open redirects enable anyone to craft a URL that will redirect a user from the legitimate URL to the website of their choice; it is a vulnerability that allows attackers to use an established business reputation to perform phishing attacks, or in another words, to disguise malicious URLs with a trusted domain. Another type of technique is the post-exploitation redirection - after the user has been tricked into divulging his sensitive data on the phishing site, the victim is redirected to the legitimate site in order to remove potential doubt by exploiting the "liking" principle.
4) Using misspelled URLs. The misspelling is usually done subtly, by making the link appear to belong to the known/reputable organization (for example, facebok.com, mircosoft.com, etc.). Again, mostly the "liking" principle is exploited here.
5) Homograph attacks. Similarly to misspelled URLs, the goal is to craft the URL that is visually identical to a legitimate site by using similarly shaped characters (for a trivial example, micros0ft.com, FACEB00K.COM). More advanced attacks use homographs in internationalised domain names, which could be visually indistinguishable from each other (for example, in Latin the letter "a" is U+0061, and in Cyrillic the letter "a" is U+0430). Online article [27] showed an interesting example of masking the original domain by using the mathematical division operator (U+2215), which looks like a ASCII slash (U+002F) in the following URL:

http://example.com/a-top-level-domain.com/ where the victim could falsely identify the string "a-top-level-domain.com" as a folder located in the root directory under the domain "example.com. Targeting the similarity and familiarity, this technique also mostly exploits the liking principle.

6) The use of subdomains. Attackers can use cloud services to create a malicious app that gets assigned a subdomain, and then host phishing pages. Several phishing URLs hosted on the domains of cloud computing services and platforms were identified in [28], one such company being appspotDOTcom, a Google cloud computing platform for developing and hosting web applications. The same article reports six appspotDOTcom subdomains that have been confirmed as phishing sites as of 2 October 2020. Many similar examples exist in the wild, exploiting the liking principle.
7) Hiding the malicious URL within the subdomain. For example, attackers can use an URL such as this one: legitimate.malicious.com, making it seem like the victim is directed to the legitimate URL, exploiting the liking/-familiarity principle.
8) Creating a sense of urgency, which exploits mostly scarcity and authority principles. By adding the social proof and unity to the mix, one can further increase effectiveness ('the rest of the group had already done it, and the time is running out').
9) Using overwhelmingly long emails "to deceive the recipients to overlook the phishing components and to focus on urgency and/or emotions"
[22], effectively creating cognitive overload and falling back on the emotional decision making process. Such emails might use the scarcity and authority principles, but it would depend on the context itself which ones would prove to be most effective.
10) Complex scenario-based emails. A most popular example would probably be a 419/Nigerian scam - a lengthy email from someone claiming to be a Nigerian prince, which either offers money to the victim (if the victim sends him a small amount first in order to claim it), triggering greed, or the attacker claims he is in a dire situation, and needs money to resolve it, triggering compassion/empathy. The number "419" refers to the section of the Nigerian Criminal Code dealing with fraud, charges and penalties for offenders. Numerous other scenarios are present in modern phishing landscape, targeting various emotions and principles of influence. If a person sees herself as a compassionate one, this would trigger a commitment/consistency principle. The belief that someone would gave a person some money could trigger the reciprocity principle. Although trivial in today's perspective, this technique seems to be quite complex from the persuasion point of view.
11) Attention-grabbing techniques within the subject lines, as detailed below.

Attention-grabbing techniques within the subject lines are using elicitation of emotions, personalised narrative, familiarity, special characters, absence of characters, immediate call for action, etc. Some of the most prevalent examples include:

- Using "RE:" or "FW:", implying the continuance of some past communication, which is in most cases fabricated, but in spear phishing campaign it may refer to some actual intercepted communication, targeting the familiarity/liking principle with possibilities to tackle commitment/consistency.
- Attention locks with special characters inside subject line, such as: ****High Severity Alert****, targeting mostly scarcity and authority principles.
- Call to action in subject line, such as "Action Required! ..." also targeting mostly scarcity and authority principles.
- Explicitly referring to some previous activity/communication which can be fabricated or real ("This is to notify you that your incident has been resolved"), targeting the familiarity/liking principle with possibilities to tackle commitment/consistency.
- Referring to some urgent event, usually fabricated ("High severity alert: Password Expiring Notice..."), targeting mostly scarcity and authority principles.
- Referring to some globally familiar event of interest ("COVID-19 Relief Fund"), targeting the liking principle.
- Empty subject line, eliciting curiosity.

Targeted, personalised (spear) phishing techniques identified in this section are referring to those techniques that are selectively pre-crafted and tailored to the specific context and/or victim profile. Where not explicitly mentioned, the individual technique is typically associated with the liking principle of persuasion, given the artificial context which is intentionally fabricated for the sole purpose of triggering the environmental familiarity with the victim.

1) Spoofing email headers. Attackers can use scripts to change the email header fields such as "from" address and the "reply-to" address, due to inherent vulnerability of SMTP which does not have a built-in method for authenticating email addresses by default. Attackers could thus exploit the liking principle should they use an email address which is known to the victim.
2) Appearing as if the email is coming from your own email (advanced customised email spoofing technique).
3) Cloning the previously sent legitimate email, where the attachment and/or link within the email might be replaced with the malicious version; the success rate of such an email can be increased by claiming to be a resend of the original, or an updated version to the original. We can call this "context hijacking".
4) Adapting the display name to impersonate a sender: for example, sending malicious emails from 'LegitimateName@gmail.com' rather than 'LegitimateName@legitimateCompany.com.'
5) The use of fake news articles. This technique is designed to elicit a strong emotion from the victim, causing him to

click a link without rationally considering where it might lead. The article is crafted with the victim's personal and/or professional interests in mind. It leverages the strong human desire to correct what obviously seems wrong from the personal perspective.

6) Any other personalization of the subject line and message body tailored to the victim's identity or general profile. Crafting such a spear-phishing email requires additional previous effort of performing the OSINT on the target. We can call this "context adaptation". Business email compromise could also fall into this category. Context adaptation could be crafted "real-time", by exploiting some immediate event, situation or circumstances (a business trip, a specific meeting, hardware maintenance or audit, etc.), or "all-time", exploiting victim's habits, hobbies, daily routines, etc. Context adaptation could target any of the Cialdini's principles - liking, authority, scarcity, reciprocity, commitment/consistency, social proof - and the decision on which one(s) to target should derive from the analyzed victim's profile.

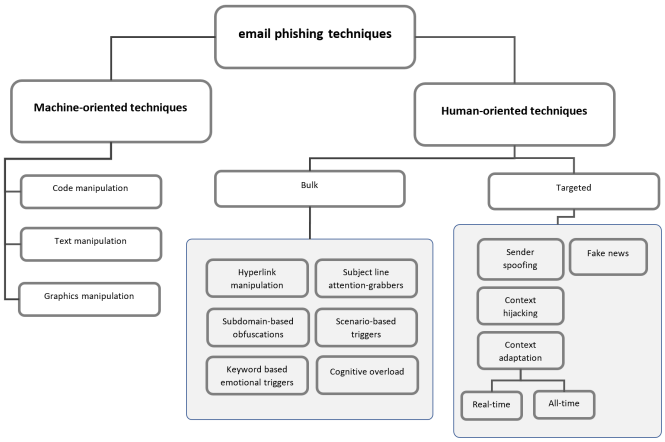

Fig. 2: The proposed taxonomy of email phishing techniques

VI. Conclusion, Limitations of the Study, Future Research

The study made a qualitative analysis of hundreds of email phishing messages from several sources, namely from the existing literature review presented in Section III, from the Cornell University "Fish Bowl" [23], an archive of spoof email and phishing scams [24], from the authors' personal collection and from numerous publicly available web articles.

The main contribution of the paper is the proposed taxonomy of email phishing techniques. Additional contributions include a comprehensive literature overview on the subject of email phishing, associations of phishing techniques with the principles and factors of influence, and raising awareness on the effectiveness of such techniques. The goal is to educate users not only on the technical aspects of phishing but also on the psychological triggers and social engineering techniques that may drive their actions towards unexpected and unwanted results.

Although a large number of messages were analysed in an attempt to identify the most prevalent types of phishing techniques, manual qualitative analysis has its limitations in terms of scope and thoroughness and may miss some of the significant techniques used in the wild. Processing a larger sets of data through automation could supplement such research with additional valuable information. Although there are some demonstrations in current research to automate such a process, there has been little effort to directly associate the specific phishing technique to principles of influence, to the best of author's knowledge.

The study made an observational association between the chosen principles and factors of influence and the phishing email techniques found within the described scope. While Cialdini's framework has been widely used in social engineering settings, it is important to acknowledge that other psychological factors, models, and frameworks beyond the scope of this study could provide additional insights into the effectiveness of phishing emails and social engineering techniques. Calculating specific correlation values might prove to provide deeper insight into the specific technique's effectiveness. By generating statistics that show the number of processed emails falling into different categories of the proposed taxonomy, it would be possible to prioritize a defense model based on the most prevalent attack techniques.

Thus for the future research there are three outstanding challenges: to enable a type of automation for processing larger amounts of phishing emails, to generate insightful statistics on the attack techniques regarding the proposed taxonomy, and to gain a deeper insight through more advanced correlation calculations.

VII. Acknowledgement

This research was funded by the project "Development of CSTI platform for retrieval and analysis of structured and unstructured data". The project received funding from the European Regional Development Fund through OP Competitiveness and Cohesion 2014–2020 within the Call for Proposals "Development of the products and services arising from research and development activities—Phase II", under grant number KK.01.2.1.02.0310.

References

[1] Verizon, "2021 data breach investigations report. technical report 11th edition." 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] Symantec, "Symantec security report 2017," 2021. [Online]. Available: https://www.symantec.com/security-center/threat-report

[3] F. I. C. C. C. U.S. Federal Bureau of Investigation, "Internet crime report 2020," 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[4] B. Schneier, "Inside risks: semantic network attacks," *Communications of the ACM*, vol. 43, no. 12, p. 168, 2000.

[5] R. B. Cialdini, "Influence: The psychology of persuasion," *New York: Quill/W. Morrow*, 1993.

[6] C. Hadnagy, "Social engineering: The science of human hacking. wiley publ," 2018.

[7] D. S. Oliveira, T. Lin, H. Rocha, D. Ellis, S. Dommaraju, H. Yang, D. Weir, S. Marin, and N. C. Ebner, "Empirical analysis of weapons of influence, life domains, and demographic-targeting in modern spam: an age-comparative perspective," *Crime science*, vol. 8, no. 1, pp. 1–14, 2019.
[8] S. Uebelacker and S. Quiel, "The social engineering personality framework," in *2014 Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 2014, pp. 24–30.
[9] N. Akbar, "Analysing persuasion principles in phishing emails," Master's thesis, University of Twente, 2014.
[10] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, 2018.
[11] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013.
[12] J. Petelka, Y. Zou, and F. Schaub, "Put your warning where your link is: Improving and evaluating email phishing warnings," in *Proceedings of the 2019 CHI conference on human factors in computing systems*, 2019, pp. 1–15.
[13] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.
[14] IBM, "Ibm x-force threat intelligence index 2018," 2018. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence
[15] Verizon, "2018 data breach investigations report. technical report 11th edition." 2018.
[16] J. A. Chaudhry and R. G. Rittenhouse, "Phishing: classification and countermeasures," in *2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB)*. IEEE, 2015, pp. 28–31.
[17] M. N. Banu and S. M. Banu, "A comprehensive study of phishing attacks," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 783–786, 2013.
[18] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," *Computer Science Review*, vol. 17, pp. 1–24, 2015.
[19] A. K. Jain and B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, pp. 1–39, 2021.
[20] P. N. Mangut and K. A. Datukun, "The current phishing techniques–perspective of the nigerian environment," *World Journal of Innovative Research (WJIR)*, vol. 10, no. 1, pp. 34–44, 2021.
[21] C. Ross, "The latest attacks and how to stop them," *Computer Fraud & Security*, vol. 2018, no. 11, pp. 11–14, 2018.
[22] A. Kashapov, T. Wu, S. Abuadbba, and C. Rudolph, "Email summarization to assist users in phishing identification," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 1234–1236.
[23] C. University, "Phish bowl," 2020. [Online]. Available: https://it.cornell.edu/phish-bowl
[24] millersmiles.co.uk, "The archive of spoof email and phishing scams," 2020. [Online]. Available: http://www.millersmiles.co.uk/archives/331
[25] R. Basset, "5 common phishing techniques," 2019. [Online]. Available: https://www.vadesecure.com/en/blog/5-common-phishing-techniques
[26] M. D. T. I. Team, "Trend-spotting email techniques: How modern phishing emails hide in plain sight," 2021. [Online]. Available: https://www.microsoft.com/security/blog/2021/08/18/trend-spotting-email-techniques-how-modern-phishing-emails-hide-in-plain-sight/
[27] crypto it.net, "Homograph attack," 2021. [Online]. Available: http://www.crypto-it.net/eng/attacks/homograph-attack.html
[28] W. API, "Attack surface monitoring: Two ways to detect phishing subdomains," 2020. [Online]. Available: https://circleid.com/posts/20201009-attack-surface-monitoring-ways-to-detect-phishing-subdomains