DOI: 10.2507/34th.daaam.proceedings.xxx

SPEAR-PHISHING AND ITS SPECIFICS WITHIN SOCIAL ENGINEERING

Miroslav Tomsu, Veronika Rosiková, Petr Vojtek & Monika Hrabakova

This Publication has to be referred as: Tomsu, M[iroslav]; Rosiková, V[eronika]; Vojtek, P[etr] & Hrabakova, M[onika] (2023). Spear-phishing and Its Specifics Within Social Engineering, Proceedings of the 34th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.xxx

Abstract

In recent years, we have observed an increasing emphasis on the digitisation of the environment, which leads to the fact that we also hear more and more loudly about the phishing issue, not only from security specialists and professional groups. Phishing is a social engineering attack consisting of deception and abuse of the human factor to break security and obtain sensitive information.
The article's introduction provides a general view of social engineering and describes its principles, specifics, and forms of social engineering. It mainly emphasises the issue of spear-phishing. The article's primary goal is to solve a practical security problem and emphasises spear-phishing and the importance of digital security and the most vulnerable element - the user. The article is an introductory look at the issue of cyber security in the context of social engineering aimed at spear-phishing and the mapping of concrete measures against this threat.

Keywords: Security; social engineering; phishing; spear-phishing.

1. Introduction

We live in a time when the digital space increasingly penetrates our lives and often becomes the central scene of critical events, not only corporate ones. Digitisation is associated with emphasising information and the possible facilitation of life through modern technologies. Companies increasingly realise that information and its digital form are their greatest assets. [1] Thanks to them, individuals and companies can gain a competitive advantage or confidential information or make the right decision. [2] Therefore, we cannot be surprised that this area, as confirmed by the statistical data of global analytical companies, is becoming more and more attractive for cybercriminals, and it is not for nothing that there is talk of a new digital battlefield. [3]

And so, the well-known Moore's law of exponential growth applies to cybercrime and informatics. This only confirms that the rapid development of information technology does not only have positive effects. As information technology becomes an increasingly common part of our daily lives, cybercrime is on the rise, threatening individuals and companies capable of causing irreparable damage literally in minutes.

We can hear about phishing as one of the most common attacks, which also benefited from the rapid move to the digital space. In recent times, thanks to many publicised problems and successful attacks using phishing techniques, we have observed an increased awareness and, above all, the interest of people and companies in a suitable solution for cyber security and the protection of their digital identity data. [4]

Many authors [5], [6], [7] try to describe spear-phishing as a method that cannot be prevented using traditional methods but emphasises the human factor, which is the most important in this problem. The issue of cyber security in the context of social engineering focused on spear-phishing is not only a technical problem, but it is primarily a problem of the human factor. The goal is to map concrete measures against this hidden threat and propose a possible solution.

2. Social engineering

Technological progress has been enormous in recent years of globalisation. Communication and part of our lives are increasingly moving into virtual space. Personal and sensitive information is often available online through various Internet services and social networks. Unfortunately, all information systems must adequately reflect this speed of change in society, and information is often protected poorly. The designs themselves become challenging to manage and highly vulnerable. Cybercrime is thus an ever-growing problem with an ever-increasing risk supported by the number of connected devices. Thanks to the current pandemic, we are observing a dramatic increase in the daily use of digital devices, internet traffic, entertainment technology, and various operational, corporate and personal agendas. One of the vectors of possible cyber-attacks is social engineering, which uses the human tendency to trust and the relative ease of deceiving the human mind. The difference from other, primarily technical vectors of cyber-attacks is precisely that it does not matter so much on the technical level of the organisation, the robustness of the firewall, the quality of encryption, attack detection systems, and user authentication, but on the weakest link of security, the person himself. This reveals the difference between machines and men. People trust others more than machines and are guided by emotions and feelings. Social engineering attacks cannot be entirely prevented by software or hardware solutions. They can only be limited and detected. The basis is teaching individuals to recognise such attacks [8].

3. The human factor and psychology

As outlined above, the attacker, i.e., social engineering, relies on deception and abuse of human characteristics. His bad habits, stupidity, naivety, gullibility, and inattention often manifest in the so-called operational blindness, i.e., during repetitive and routine work. In the end, the victim does not even realise that he has become a victim and has given away some information that he did not have or did not want. This subchapter focuses on frequently abused human characteristics and the situations that allow abuse, although it does not cover all possible ones. In practice, it is common for the attacker to focus on several characteristics and circumstances simultaneously, thanks to which he creates the best possible position to manipulate the victim [9].

4. Phasis of a social engineering attack

We can rank the social engineer among the modern con artists of today's digital age. To exploit the weaknesses of the company's security policies, they use prepared manipulation scenarios that benefit from the human psychology described in the previous subsection or combine them with technical means.

Individual social engineering attacks differ from each other, yet we can observe a characteristic pattern in them, forming the standard phases of an attack. Since the attacker's work is often iterative, we are discussing a cycle that can happen more than once within the same episode. The attacker deepens the obtained information as part of further iterations, completing the entire attack plan.

- **Information gathering** - the attacker begins by exploring open, freely accessible sources. This is information that the company or individual does not consider sensitive or exploitable and, therefore, does not protect or dispose of it securely. Under such information, we can imagine the company's website, organisational structure, contacts, marketing materials, public tenders, published job advertisements, employee lists, older company documents or guidelines, financial results, information from social networks or public whois databases, discarded memory media, printed or handwritten credentials, etc. This step of the cycle is often referred to as the most important.
- **Building relationships and trust** - based on the information gathered from the previous phase, the attacker considers all possible situations and prepares suitable scenarios of problems and questions that could arise and need to be answered so that he is always one step ahead of his victim. If possible, he chooses as a victim a person who does not realise the importance of the information he is working with. He pretends to be someone else and gradually builds mutual relations and trust with the victim. This is a time-consuming phase in which the attacker must be careful not to arouse suspicion in the victim. Still, on the other hand, he needs to obtain the desired information from the unsuspecting victim. Suppose the exploitation of the victim takes place in the workplace. In that case, it is essential to use a communication style appropriate to the given company, its jargon, commonly used expressions and terms, correct names of employees, addresses, etc.

- **Abuse of trust** - an attacker abuses the trust and relationship gained to get the victim to provide sensitive information or conduct a security incident. It is often a form of cooperation, both on the part of the victim and the attacker who asks for something, but the victim can also ask the attacker for cooperation in good faith.
- **Exploiting information** is the last stage of the cycle, where the attacker receives the desired information and uses it to achieve the desired result of the attack without leaving any evidence. Suppose the data obtained is only a partial step closer to the goal. In that case, the attacker returns to the beginning of the cycle and repeats it until he reaches the final destination [10] [11].

5. Definition of the principle of phishing

The word phishing was created by combining the words fishing and phreaking. This is a slight corruption of the English phrase fishing, meaning fishing, and it is here that we can observe an analogy with a fisherman who throws a hook with bait and hopes that a fish will catch it. Similarly, the attacker expects the victim to fall for the irresistible temptation he has created and thus obtain the desired data. The initial substitution of the letter f for ph comes from the tradition of hacker slang. It originates in the word phreaking, one of the first forms of hacking and targeted free calls through the US telecommunications network [12].

In general, phishing has been defined as "a type of computer attack that communicates socially crafted messages to people through electronic communication channels to persuade them to perform a specific action in favour of the attacker" [13].

The essence of phishing, which is classified as a semantic attack that uses primarily human, not a system, vulnerabilities, is the attempt to obtain sensitive information from an unsuspecting victim that the attacker can then misuse, such as login credentials, credit card information, and other personal information leading to digital theft identity, for later misuse or in combination with ransomware-type attacks (according to (Gupta et al. 2017a), ransomware is attached to 9 out of 10 phishing e-mails) to block the user's access to their data and subsequently demand a ransom for their decryption [14].

6. Types of phishing attack

We will find many ways and views of dividing phishing attacks. The article compiles an overview of the currently preferred types of phishing:

6.1. Spear phishing

A targeted attack against a specific organisation or individual. An email attack is personalised by gathering all available information about the victim and tailoring the content. Such an attack is more demanding to plan, but it tends to be highly successful due to the difficulty of detection [15].

6.2. Whaling phishing

Attacks that target high-ranking people in organisations with privileged access to data or finances. The effort involved tends to be more significant but brings higher profits [16].

6.3. Business Email Compromise (BEC) Phishing

This attack also targets executives. He is not trying to deceive them but to impersonate them. After gaining the worker's awareness, the attacker sends a highly persuasive business email to get the subordinate or partner to open the link or attachment. In 2018, the total loss from reported FBI attacks was approximately $1.2 billion (FBI 2019), the most significant loss recorded for any cybercrime [15].

6.4. Social media phishing

Attackers easily create fake profiles that allow them to access the victim's published data or attack them via private messages. He may also post phishing links on his wall, on official sites, or in groups. A study (Stern 2014) shows as early as 2014 that 22% of phishing scams on the web target Facebook [17].

6.5. Instant Messaging (IM)

Attacks are not only based on links in the text but also use images, gifs, and files that can be included in the conversation. In addition to text, voice and video chat are also supported. Attacks can thus take place in real-time and use multiple attack techniques [14].

6.6. Vishing / IVR (Interactive Voice Response) phishing

Represents attacks through a phone call to manipulate people into providing their sensitive information for verification. They can be done using automated dialling and telemarketing. People generally find voice communication more trustworthy and are used to it. In addition, the older generation prefers the phone, which is also easier to handle [15].

6.7. Smishing

Smishing uses SMS and MMS messages. The attacker usually impersonates a trusted institution such as a bank. The message contains malicious code or links to a fraudulent website [18].

6.8. QRishing

QR codes are used to automate the collection and transmission of information. They are mainly used on mobile devices. The danger is that the user needs to learn what the QR code refers to or contains. It can lead to a fraudulent address or a link to download an infected file without the victim's knowledge. Some QR code readers will present a link for review before opening it. Using address shortening still makes it difficult for users to verify the link's legitimacy [18].

6.9. Sound Squatting

They exploit the voice interface (VUI) to exploit homonyms and input errors. Virtual assistants use keywords to open applications. An attacker registers a fake app with a voice keyword similar to the original app. The virtual assistant will open a phoney app when the user calls a specific app. Once opened, this fake app steals the user's sensitive information or performs other malicious activities [19].

6.10. Fake Phishing Websites

Visually mimic legitimate websites to obtain sensitive information from users. Links to them include e-mails and advertising banners on other legitimate websites, social networks, or video portals such as YouTube. People are generally less cautious when browsing the web [17].

6.11. Wiphishing (Wi-Fi)

Attackers use publicly available networks. A typical form is abusing the login portal or passing off a fake access point as a real one (same SSID network name) and capturing network traffic. A created hotspot from a phone or laptop is often enough for an attack [18].

6.12. Malvertizing

The attacker inserts malware into the ad, activated when clicked. These ads can be placed on legitimate websites without any effort. The victim usually does not consider advertising on a reputable website dangerous. Only some people realise the shortcomings of verifying ads before they are deployed. Thanks to information from websites hosting ads, it is possible to target specific groups [20].

6.13. Typo squatting

Targets a user's typographical error when entering a URL. An attacker on similar domain names creates visually similar websites that they use to steal sensitive information or do other malicious activities [18].

6.14. GUI Squatting

An attack targeting mobile devices. The automated method generates high-quality phishing copies of simple applications that bypass existing phishing prevention and detection techniques and steal user credentials [21].

7. Specifics of spear-phishing

While it is typical for traditional phishing to send out many e-mails, often to the wrong addresses, spear phishing is the opposite. In such a case, the attacker sends an e-mail to a specific person, usually an employee in a particular position or a high-ranking company manager. Such mail addressed to a specific person can be challenging to catch with an anti-phishing filter, mainly because it does not appear in large numbers and shows no signs typical of phishing mail. Please understand that neither the sender's nor the SMTP server's address is on any blocklist, and there are no links to the Internet from the e-mail.

In addition, if such an e-mail is sent to the victim directly from the environment of the given company, the latter usually does not even suspect that it could be phishing, even though they have been instructed in this direction. How could she, when the mail came from a person she knows well, there are no links from the mail to anywhere on the Internet, she is not required to enter any data, and the mail completely corresponds to the company's customs in terms of form and content.

At this point, it must be emphasised that the attacker pays considerable attention to preparing the e-mail. For this purpose, the attacker is quick to familiarise himself in detail with the company culture, organisational structure, and conditions that prevail in the given company. Therefore, the correct language is used, and we do not find any grammatical errors or stylistic flaws in the text of the e-mail.

Such a carefully prepared e-mail containing an attachment with malicious code is used as part of an APT attack when an unsuspecting victim opens the e-mail, clicks on the attached attachment, and, together with the associated application, launches malicious code that exploits some (zero-day) vulnerabilities to successfully load into memory and ensure that it runs even after a computer restart.

In the case of spear phishing, when the attacker's goal is to catch a big fish, if we continue to stick to the above comparison, it is not possible to underestimate its intelligence, so the attacker must first thoroughly explore the territory in which he decides to hunt and arm himself with a harpoon (in English spear, hence spear phishing) because they won't catch a big fish on some smelly bait [22].

Phishing	Spear phishing
Mail is sent to a large number of addresses.	Mail is sent to only one recipient.
The email contains a link to the Internet.	Mail does not have a connection to the Internet.
The mail will come from a person or company you know.	The mail will come from a person or company you know.
Specific data is required.	No data entry is required.
The mail contains (unintentional) errors.	Mail does not contain (unintentional) errors.
Mail usually does not contain any attachments.	Mail usually includes an extension.
The goal is to obtain login or personal information.	The goal is to get sensitive information that is the subject of intellectual property.

Table 1. Comparison of classic phishing and spear-phishing [22].

8. The most common examples of spear-phishing

8.1. E-mail

Spear-phishing can be very difficult to detect if done correctly. Emails come from a person the person knows and expects a response from.

It is especially tragic in the case of native Microsoft clients. When a name is entered in the "from" field that matches the name of a person who works in your organisation, it will pull up his photo and display his status and other information. In that case, the user won't check the header to see what's in the "envelope-from" field.

In most cases, sender users quickly follow what is listed in the "From" field. But that's not entirely true. The problem is that the email has two "from" areas. One is called "envelope-from," which contains the sender's actual address, and the other, called "from", anyone can write whatever they want.

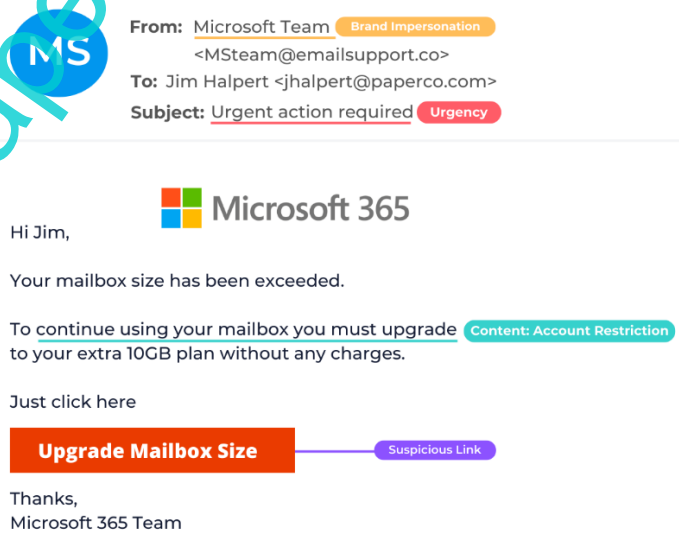

Fig. 1. A typical example of spear-phishing [27].

8.2. O365

Recently, there has been an increased number of attacks on employees of organisations that have moved their communications to O365. After all, thanks to O365, Microsoft has become the most popular brand among attackers who rely on phishing, and it is not surprising that the number of companies and users in O365 is growing at a rocket pace. An attacker can then attack practically anyone from a compromised account.

The attack comes in several phases. It is a so-called multi-phase attack, where there is first classic phishing and then spear phishing on employees of a specific organisation using the Microsoft O365 cloud.

First, the attacker uses phishing to obtain the login data for the account of any employee in the given organisation. From this account, he contacts a specific person through spear phishing. Given that the e-mail comes from someone she knows, she does not suspect it could be an attack [23].

8.3. EML attachments

In other cases, the facts of how attachments are handled were used. They are scanned for malicious code, but if the branch is a file with the EML extension, a standard format for saving e-mails in a file represented by an envelope icon, it already has the same check as in an e-mail not in progress.

And since the EML file can be easily created and edited in any text editor, it is possible to modify it so that both the sender and recipient fields contain the addresses you need. That is lessons from the sender's or recipient's organisation, which the recipient knows well [24].

8.4. Pictures

As part of the spread of SPAM, the text has been replaced with an image for years to bypass various filters. Here, a newly appeared image was created due to saving text in which homomorphic characters were intentionally used.

Such a text is complicated to read with an OCR program and interpret correctly because it needs to make sense in any language during simple machine processing. A person can easily read it, but artificial intelligence is at a lower level to deal with it [24].

9. Defence against spear-phishing

While an attacker only needs a single click from the victim to open an infected attachment, spear-phishing defences consist of four broad, interconnected areas that combine technical, process, and human elements.

9.1. Regular users

For regular users, it is essential to follow several safety principles.

- Do not allow macros in programs (especially Microsoft Office). If macros are required, verify the document's origin with its sender before enabling them. Do not unthinkingly open attachments and links in e-mails, especially from unknown senders.
- Check the e-mail address in case of urgent or unusual requests (payment of an invoice, request for confidential information).
- In case of uncertainty or suspicion of harmful e-mail, contact the IT department or other responsible workplace.
- Limit the sharing of employment information on social media and avoid sharing information about company hierarchy, security and administrative processes.

9.2. Network administrators

Limit the attacker's access to the user. In their spear-phishing e-mails, more sophisticated attackers falsify their addresses to look like addresses within the organisation (spoofing). This technique can be made more difficult by using so-called anti-spoofing tools. These are DMARC (Domain Message Authentication Reporting and Conformance)12 technology, which verifies the sender's domain, and DKIM (DomainKeys Identified Mail)13 and SPF (Sender Policy Framework)14 technologies. These technologies evaluate which e-mail reaches the user and which ends up in spam. The attackers' chances of success can also be reduced by limiting publicly available information about the organisation. This is, for example, the organisation's exact organisational structure or the management's biographies. Users should also carefully consider what and with whom they share online. In this direction, individual organisations can inform users about the options for privacy settings on social networks, allowing users to limit the circle of people who can see the content on their profile. Restrictions on information sharing also apply to employment details, especially in critical

infrastructure, government offices, and strategic enterprises, which are particularly interesting to sophisticated APT groups. The organisation should also be aware of what information is shared about it by third parties (partners, suppliers).

They are protecting the organisation from the effects of successful spear-phishing attacks.

If early threat detection fails, the consequences of a successful attack must be minimised. Here are universal cybersecurity principles that are not limited to spear-phishing:

- The organisation should use anti-virus software;
- Systems should have legal and supported software installed and updated to the latest versions;
- Administrator accounts should be limited based on necessary needs and should not be used for e-mail communication or Internet surfing;
- Limitation of macros for Microsoft Office;
- Using a two-factor authentication password manager (prevents 99.9% of account theft attempts);15
- Create regular data backups in case of data compromise or loss.
- Periodically assess whether the user needs all the access rights he has;
- Continuously delete the accounts of people who no longer work in the organisation.
- Rapid response to incidents.

Help users identify and report spear-phishing e-mails.

This step aims to create an environment where employees are unafraid to report suspicious e-mails. For this, it is necessary to clearly define within the organisation the person or persons to whom such e-mails can be written and how) and to inform employees about this. Given the ever-increasing sophistication of spear-phishing, it is unrealistic to expect users to identify 100% of malicious e-mails. Still, even minimal training and familiarisation with the reality of the threat can help reduce the risk [25].

10. Frequent reasons for failure of existing protection

The e-mail comes from someone the person knows and expects a response from. However, the attacker only sometimes succeeds in hacking the sender's e-mail account and, therefore, has to spoof the sender's address, which increases the chance of detection.

You can quickly tell who the email came from by looking at what is written in the "from" field. But that's not entirely true. The problem is that the email has two "from" areas. One is called "envelope-from", which contains the sender's actual address, and the other, called "from", anyone can write whatever they want.

```
2859:2890:2902:2909:2913:2937:2939:2942:2945:2947:2951:29
4:3934:3936:3938:3941:3944:3947:3950:3953:3956:3959:4042:
388:9392:10010:10049:10175:11026:11233:11473:11529:11651:
80,0,RBL:122.201.87.195-irl.urbl.hostedemail.com-127.0.0.
bulk,SPF:fn,MSBL:0,DNSBL:neutral,Custom_rules:0:1:0
X-HE-Tag: chain43_902aac0ff3e60
X-Filterd-Recvd-Size: 3501
Received: from scuderia.turboservers.com.au (unknown [122
    by im05.hostedemail.com (Postfix) with ESMTP
    for <jonathan@askwinters.com>; Wed,  8 Apr 2015 11:19
Received: from nobody by scuderia.turboservers.com.au wit
    (envelope-from <nobody@scuderia.turboservers.com.au>)
    id 1Yfo1N-0005mn-RS
    for jonathan@askwinters.com; Wed, 08 Apr 2015 21:19:4
To: jonathan@askwinters.com
Subject: About your last Transaction
```

Fig. 2. Spear Phishing Attack Example Raw Source [28]

The e-mail client takes the sender's address from this field, which it then displays to you. The check could be done by SPF (Sender Policy Framework), which ensures that it is not possible to receive e-mail from a mail server that is not authorised to send e-mail for the given domain. But in this case, it doesn't matter because SPF only checks what is stated in the "envelope-from", not what is said in the "from" field.

If the attacker tried to change the value in "envelope-from" as well, then SPF would work, but why would the attacker do that when he needs to change the "from" field, which SPF doesn't check? And who would think to display the header of each email and see if something else is written in "envelope-from" than in "from".

A possible protection would be DKIM (DomainKeys Identified Mail). Still, the problem here is that this protection only creates a hash of the e-mail or only a specific part of it, which is encrypted with the private key that it has right only a person in the given domain. During the check, it was subsequently found that the given e-mail was protected using DKIM, so a query was made for the given environment. This obtains the public key and thus decrypts the message and obtains its hash. This is then compared with the hash calculated on the side of the message's recipient. If it fits, then the e-mail came from the given domain.
The only possible solution is DMARC (Domain-Based Message Authentication, Reporting, and Conformance), which compares the value given in the "from" and "envelope-from" fields, and it is possible to set how to handle an email that has a different address provided in both areas. In practice, however, it is used sparingly because, in many cases, these fields are other, even for legitimate reasons [26].

11. Conclusion

This article aimed to outline how easy it is for an attacker to create a successful phishing campaign and how, if at all, the recipient of such an e-mail can verify its authenticity and discover that it is fake before even clicking on a link in the e-mail. He will be redirected to a fraudulent site where he will be asked to enter his login information.

Company security does not begin and end with the IT professional or IT department. Cybercriminals often target the weakest link, so every employee must be up-to-date on the latest threats and tactics used by cybercriminals to help keep the business safe and protected from cyber threats that can have potentially devastating effects.

It can be expected that the user will soon be the most vulnerable link in all systems. For that reason, there are reasons to emphasise educational programs and users' critical approach to their cyber security is essential, especially concerning the expected future development.

Spear-phishing attempts are usually not by random hackers but organised criminals seeking money, trade secrets, or other information who have vetted their target well to appear trustworthy. The apparent sender of spear-phishing is often one of the company's senior employees. A request in an e-mail is usually urgent and requires an immediate response.

At the same time, it is more than likely that attackers in cyberspace will continue to refine the fraudulent techniques they will use. The opposite of this development can be, for example, integrating all social and age categories of users into the continuous education system.

Healthy prevention, which unfortunately is often underestimated by many users, is to refrain from posting too much personal information in cyberspace because this is the most valuable food source for hackers who work with the spear-phishing method.

Further research aims to raise awareness of the dangers of phishing and teach users how to detect real phishing using software tools. Focus only on preparing phishing content and monitoring user reactions. The goal will also be to focus on preparing phishing content, monitoring user reactions, and evaluating the activities of individual recipients on the relevant phishing pages.

12. References

[1] Tomsu, M. (2022). Reliable Information Sources in the Age of Propaganda, Proceedings of the 33rd DAAAM International Symposium, pp.0437-0443, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-36-5, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/33rd.daaam.proceedings.061

[2] Shao, J., Zhang, T., Wang, H., & Tian, Y. (2022). Corporate social responsibility and consumer emotional marketing in significant data era: a mini literature review. Frontiers in Psychology, Vol. 13, DOI: 10.3389/fpsyg.2022.919601.

[3] McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75, United Kingdom.

[4] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, Vol. 11, No. 4, DOI: 10.3390/fi11040089

[5] Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information & Computer Security, Vol. 25, No. 5, pp. 593-613, ISSN: 2056-4961.

[6] Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015, September). A study of preventing email (spear) phishing by enabling human intelligence. In 2015 European intelligence and security informatics conference, pp. 113-120, DOI: 10.1109/EISIC.2015.38.

[7] Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In Australasian Conference on Information Systems 2015, DOI: 10.48550/arXiv.1606.00887

[8] Salahdine, F. & Kaabouch, N. (2019). "Social Engineering Attacks: A Survey", Future Internet 11, No. 4, DOI: 10.3390/fi11040089

[9] Fan, W.; Lwakatare, K. & Rong, R. (2017), "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations", International Journal of Computer Network and Information Security (IJCNIS), Vol. 9, No. 1, pp. 1-11, DOI: 10.5815/ijcnis.2017.01

[10] Mitnick, K.; Simon, W. & Vasta, L. (2003) The Art of Deception: The World's Most Famous Hacker, Gliwice, Helion, ISBN 978-0764542800

[11] Jamil, A.; Asif, K.; Ghulam, Z.; Nazir, M. K.; Mudassar, A. S. & Ashraf, R. (2018). "MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook," IEEE International Conference on Big Data (Big Data), pp. 5040-5048, Seattle, WA, USA, DOI: 10.1109/BigData.2018.8622505
[12] Fruhlinger, J. (2020) What is phishing? How this cyber-attack works and how to prevent it, CSO Online, 2020, Available: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
[13] Cui, Q.; Jourdan, G. V.; Bochmann, G. V.; Couturier, R., I. & Onut, V. (2017). "Tracking Phishing Attacks Over Time", In Proceedings of the 26th International Conference on World Wide Web (WWW '17), International World Wide Web Conferences Steering Committee, pp. 667–676, Republic and Canton of Geneva, DOI: 10.1145/3038912.3052654
[14] Aleroud, A. & Zhou, L. (2017). "Phishing environments, techniques, and countermeasures: A Survey", Computers & Security, Vol. 68, pp 160-196, DOI: 10.1016/j.cose.2017.04.006
[15] Salahdine, F. & Kaabouch, N. (2019). "Social Engineering Attacks: A Survey", Future Internet 11, No. 4, DOI: 10.3390/fi11040089
[16] Fruhlinger, J. (2020) What is phishing? How this cyber-attack works and how to prevent it, CSO Online, 2020, [online] Available: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
[17] Gupta, B. B.; Arachchilage, N. A. G. & Psannis K. E. (2018) "Defending against phishing attacks: taxonomy of methods, current issues and future directions", Telecommun Syst, Vol. 67, 2018, pp. 247–267, DOI: 10.1007/s11235-017-0334-z
[18] Alabdan, R. (2020). "Phishing Attacks Survey: Types, Vectors, and Technical Approaches", Future Internet, Vol. 12, No. 10, DOI 10.3390/fi12100168
[19] Shashank, K.; Rakesh, D. R.; Vaibhav, S. N. & Balkrishna E. N. (2020). "Applications of industry 4.0 to overcome the COVID-19 operational challenges," Diabetes & Metabolic Syndrome: Clinical Research & Reviews, Vol. 14, Is. 5, pp. 1283-1289, DIO 10.1016/j.dsx.2020.07.010
[20] Nagunwa, T. (2014) "Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors," International Journal of Cyber-Security and Digital Forensics, Vol. 3, pp. 72–83. DOI 10.17781/P001287
[21] Chen, S.; Fan, L.; Chen, C.; Xue, M.; Liu, Y. & Xu, L. (2021). "GUI-Squatting Attack: Automated Generation of Android Phishing Apps," in IEEE Transactions on Dependable and Secure Computing, Vol. 18, No. 6, pp. 2551-2568, DOI 10.1109/TDSC.2019.2956035
[22] Butavicius, M.; Parsons, K.; Pattinson, M. & McCormac A. (2016) "Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails", Available: http://arxiv.org/abs/1606.00887
[23] Dewan, P.; Kashyap, A. & Kumaraguru, P. (2014). "Analyzing Social and stylometric features to identify spear phishing emails," 2014 APWG Symposium on Electronic Crime Research (eCrime), Birmingham, AL, USA, pp. 1-13, DOI 10.1109/ECRIME.2014.6963160
[24] Bullee, J. W.; Montoya L.; Junger M. & Hartel P. (2017) "Spear phishing in organisations explained", Information and Computer Security, Vol. 25 No. 5, pp. 593-613, DOI 10.1108/ICS-03-2017-0009
[25] National Cyber and Information Security Agency, (2020). "Tailor-made phishing emails or social media messages: Spear-phishing and how to protect yourself from it", Available: https://www.nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf
[26] Smejkal, V. (2015), Cybercrime, Ales Cenek, Plzen, ISBN 978-80-7380-849-5
[27] Gilmer, J. (2021) What does spear-phishing look like?, Available from: https://www.meshsecurity.io/spear-phishing
[28] Winters, J. N. (2015) Spear Phishing – Increasingly Common, Available: https://askwinters.com/2015/04/08/spear-phishing-increasingly-common