DEPARTMENT OF COMPUTER SCIENCE

Unpacking Spear Phishing Susceptibility

Author:

Anurag Tyagi
ite103217@stud.fh-wedel.de

Supervisor:

Prof. Dr. Gerd Beuster
gb@fh-wedel.de

A paper submitted for the Seminar in IT Security (Master)

Winter Semester 2019/2020

February 23, 2020

Abstract

Email has proven to be one of the most convenient and infamous attack vector for Spear Phishing attacks. The prevalence of these attacks has given impetus to a considerable amount of research aimed at explaining the characteristics behind them. As attackers become more skilled and acquire more sophisticated tools (Social Media, messaging apps), the protection against these attacks gets more challenging. This calls for even more general, real world studies and research into the susceptibility of a user falling victim to a phishing scam. This paper attempts to unravel the mechanism behind a spear phishing attack and tries to explain what makes a user susceptible to such an attack. More specifically, it searches for factors that lead to a successful or an unsuccessful attack. It aims to fill the above mentioned research gaps by elaborating on the ways attackers exploit the human element. To accentuate this, it discusses in detail a research paper titled the same authored by Zinaida Benenson and Robert Landwirth of Friedrich-Alexander-Universität Erlangern-Nürnberg, and Freza Gassmann of Universität des Saarlandes, Germany [1]. The paper reports the results of a field experiment where over 1200 University students were subjected to a choreographed spear phishing attack. Moreover, it explores the important hypotheses formulated on factors like age, gender and channel of attack.

Keywords : Spear Phishing, Cognitive Exploitation, Victim Susceptibility

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In today's technological era of constant evolution and innovation, the internet plays a major role in its advancement. With the precipitous expansion of Social Media and Email, people are given countless ways to communicate, share and exchange information. Unfortunately, it also offers new mediums of exploitation to individuals with malicious intents. These malicious intents can be actualised in numerous ways in the cyber world, with the most common being the Spear Phishing attack. This cyber attack has proven to be a constantly growing threat to individuals and industries, resulting in massive losses of finances and time [4, 5, 6]. As more users gain access to the Internet and generate data, the chances of someone falling for a spear phishing attack increase with it.

In the sections that follow, Spear Phishing is explained in relevant detail to create a basis of understanding for the rules that dictate a user's susceptibility to fall for a Spear Phishing campaign. With the primary focus on elucidating this very susceptibility, a detailed analysis of a 2014 study [1] on the topic is examined and the findings illustrated. The statistical data is derived directly from the study and is used to enforce the aforementioned objective. To confirm the validity of observed trends and patterns, original hypotheses and research questions used by the researchers are explored. This paper further goes on to establish a viable case for future research and based on current research extrapolates what manners the issue will assume in the foreseeable future.

CHAPTER 2
THE THREAT OF SPEAR PHISHING

Spear Phishing is a typical masquerade attack where an attacker builds up trust through impersonation, in order to dupe the victim into unwittingly giving up confidential information or unauthorised access to an asset. These type of attacks largely vary from the generic Phishing attacks where an attacker loosely targets or baits a large number of potential victims. A Spear Phishing attack is much more targeted and much less indiscriminate compared to Phishing. It generally involves the attacker gathering data about the target, assuming a trusted identity and launching a personalised attack. The recent years have been observed to effectuate the fact that Spear Phishing campaigns continue to grow and diversify [7].
Spear Phishing has established itself as a persistent threat in the last decade and continues to generate disruption in the field of IT Security [8, 2]. Especially in the recent years, it's reach and speed has magnified enormously with the world's increasing dependence on the Internet. Not only does it cause harm to individuals, it is strategically employed to target large scale companies and industries like E-Commerce [8, 9]. The sections that follow elaborate the motivations and the real life consequences of such attacks.

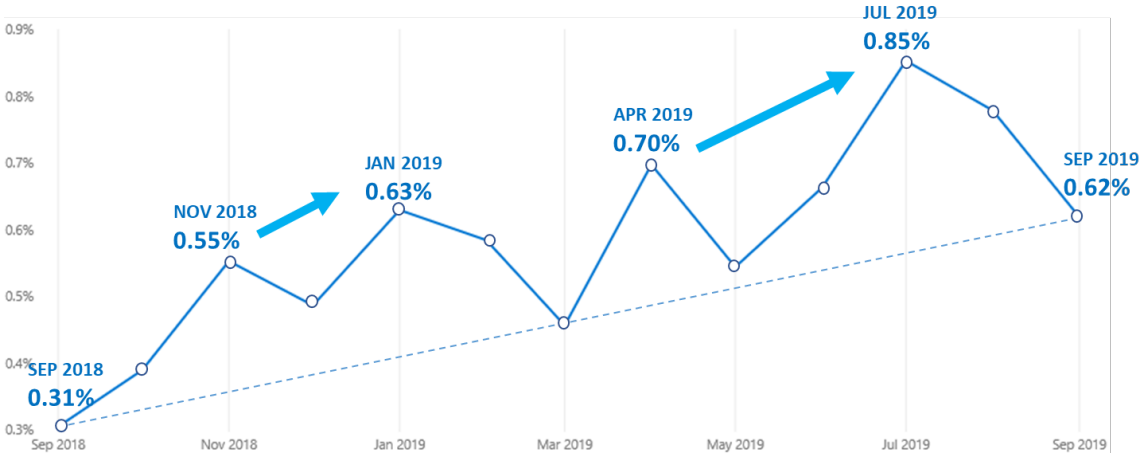

Figure 2.1: Percentage of total inbound emails that are Phishing emails [2]

2.1 Purpose behind such attacks

Spear Phishing has amassed a wide spectrum of applications for cyber attacks, all the while becoming more sophisticated and harder to detect. It's objectives have been found to range from stealing someone's personal identity for petty theft to planting fake news [10] and causing divisions in communities. Phishing has been actively employed by hackers to install spyware to network systems and monitor them to gain an unauthorised access to the information contained in them. An attacker could also be motivated by revenge, acting upon a personal grudge to cause damage to the reputation of the target. In the recent years, spurious phishing emails have been used to deliver ransomware [11, 12] and similar malicious software.

Meanwhile, it is entirely plausible that an attacker would diligently carry out an attack for the sole purpose of acquiring money. In this scenario, tools like ransomware provide an easy and untraceable method to blackmail or extort money from the target [13]. Phishing links received through mail are most commonly used to install malware that locks the data stored on the target machine and blocks the authorised users from accessing it. A more widespread application includes the attacker then negotiating to release the files once a large sum is paid. These incidents are usually preceded by a careful surveillance and collection of the target's publicly or privately stored data, that is then used against them. Blackmail in itself could be utilised to coerce a target to release sensitive information like access credentials where the attacker then proceeds to hijack their digital identity.

2.2 Damages

Spear Phishing attacks have been directly correlated to numerous corporate espionage cases where a significant harm to assets and reputation was caused. A research carried by Phishlabs [14] estimates that damages from such attacks alone have resulted in the loss of Hundreds of Millions of dollars in the U.S. Apart from financial losses and data breaches, targets also often suffer losses of time and productivity. Companies wittingly spend their workforce and resources to constantly defend themselves against these attacks, the time and resources that could potentially have been utilised towards their industrial output. Sophisticated methods enable attackers to bypass these security defenses. Additionally, such attacks have also proven fatal to matters of National Security as targets including staff employed in political circles and the military have been targeted and created major news headlines in the past decade. In one particular case, the senior commander of NATO became the victim of such an impersonation attack where the attackers established a fake Facebook page with his name and attempted to trick his acquaintances into divulging sensitive information [15]. While this attack was averted successfully, it delivers a compelling case on how attackers can gain access to critical information and secrets.

As it is quite difficult to compare the damages caused to individuals and entire organisations, it suffices to say that both cases can yield catastrophes for the target. Individuals falling victim to spear phishing attacks in most cases endure a damage to their reputation, finances or personal information. In such a scenario, the potential payoff for the attacker is significantly larger compared to the campaign efforts.

CHAPTER 3

THE 2014 STUDY

The precursory research paper titled 'Unpacking Spear Phishing Susceptibility' [1] was published at the Targeted Attacks Workshop at Financial Cryptography and Data Security 2017. The encompassed study consists of surveys carried in 2013 and subsequently in 2014, the latter being implemented to bolster the findings of the former. The surveys provide an insight into the characteristics of users' cognitive perception and vulnerability to manipulation based on parameters like the user's age and gender. The survey was carried on over 1255 university students through the mailing list of the Universität des Saarlandes and Friedrich-Alexander-Universität Erlangen-Nürnberg , following all data protection laws and proper ethical guidelines. In order to classify the observed behaviour among the responsive participants, an auxiliary post-experiment survey was held.

3.1 Experiment Design

For the purpose of this survey, students were randomly chosen from the Universities' mailing list and their various Facebook groups. The phishing message was planned to be sent out in January 2014 and customised accordingly. The participants were sent an email or a personal Facebook message with a link from a non-existing person. The message claimed itself to be a link to the pictures from the New Years' party. It is illustrated in Fig 3.1. In case a participant clicked the link sent out, he/she was presented with an 'Access Denied!' message and their clicks were recorded. To implement a follow up mechanism, a questionnaire was sent out to the participants requesting the reason for their clicking or not clicking.
For sending the message, three email accounts and four Facebook accounts were created. The email accounts consisted of a male, a female and an anonymous account while the Facebook profiles were created for two males and two females. One Facebook account for each gender was made private (with only the default male/female picture) and the public ones displayed friends, posts and pictures. As an additional impetus, most popular German names of that year were employed for the senders' names.

Hey!

The New Year's Eve party was awesome! Here are the pictures:

http://<*IP address*>/photocloud/page.php?h=<*participant ID*>

But please don't share them with people who have not been there!

See you next time!

<*sender's first name*>

Figure 3.1: Message with individualised link and text [1]

3.2 Sample Characteristics

The participants comprised of 280 Facebook users (80 male, 200 female) and 975 email users (265 males, 710 females). The two groups had a comparable gender structure with 27% and 29% male participants respectively, as seen in table Table 3.1 Though the data seems to be skewed towards the female population, the results show no significant effect of this distribution bias.

	Email	**Facebook**
Male	265	80
Female	710	200
Total	975 (27% male)	280 (29% male)

Table 3.1: Gender distribution of recruited participants[1]

A statistical overview of the key demographic facts was carried through and depicts the response rate of the survey for both channels of attack (Table 3.2).

	All users	**Email group**	**Facebook Group**
Recruited participants	1255 (28% male)	975 (27% male)	280 (29% male)
Survey Response Rate	57% (22% male)	56% (21% male)	62% male (28% male)
Average age (survey)	23.1 ($\sigma = 4.4$)	23.2 ($\sigma = 4.1$)	22.9 ($\sigma = 5.1$)
% of students (survey)	93%	96%	86%

Table 3.2: Key demographic facts about the participants[1]

3.3 Hypotheses

In order to successfully build a relationship between the key research parameters (age, gender and medium), five hypotheses were formed.

Hypotheses: These factors would be used to explain, or in some cases, correlate the observed success rate of the attack.

- H1: Message received via Facebook
  If receiving a phishing message on Social Media varies from email,

- H2: Friend request from the sender
  If receiving an additional Friend request affects the success rate,

- H3: Message sent from an open Facebook Profile
  If the privacy settings of the sender play a role,

- H4: Female gender of the sender
  If the sender being a female affects the results,

- H5: Female gender of the recipient
  If the receiver being a female affects the results.

In addition to the hypotheses, a set of research questions were used to further draw a distinction between the factors above and their effect on user clicking behaviour:

Research Question 1: Do participants react to a 'suspicious' link differently depending on whether the link was received via Facebook or via email?

Research Question 2: How do people explain their reasons for clicking or not clicking on a link?

The first question seeks to validate the efficiency of email based phishing attacks and evaluate whether the attack medium evidently results in a significant change in the click rate. The second question aims to utilise the scale of the survey to draw out the factors that led to a user clicking or not clicking on the link, naturally through the user's perspective.

3.4 Findings

Based on the web server logs, a statistical representation of the clicking rate was derived. The evaluation of the hypotheses was performed using the descriptive results and the Pearson chi-squared (χ^2)(See Appendix) test results with the effect size reported using Cramer's V (φ_c)(See Appendix). These are depicted in Table 3.3.
A cursory observation of the reported statistics show that only hypothesis H1 was supported by the survey. This pertains to users responding differently based on the channel of attack: Email or Facebook. The reported clicking rates of the second survey proved Facebook(FB 42.5% vs 20% Email) to be more successful as an attack medium. This is concluded from the only significant factor ($p < 0.001$). More interestingly, this observation was entirely disputed in the first post-survey analysis, where email was shown to be better at convincing users to click on a link (FB 38% vs 56% Email). This again goes to show the disparity between results brought by small scale studies. Furthermore, the gender of the sender or receiver did not present a major distinction in creating a more successful attack[1].

Factor	**Clicked**	χ^2	**df**	**p**	φ_c
communication channel	email: 194/975 (20%) FB: 119/280 (42.5%)	59.365	1	**0.000**	0.218
sender's gender (email)	female: 72/325 (22.1%) male: 59/326 (18.1%) undefined: 63/324 (19.4%)	1.742	2	0.419	0.042
sender's gender (Facebook)	female: 64/140 (45.7%) male: 55/140 (39.3%)	1.184	1	0.277	0.065
receiver's gender (email)	female: 152/710 (21.4%) male: 42/265 (15.8%)	3.742	1	0.053	0.062
receiver's gender (Facebook)	female: 86/200 (43.0%) male: 33/80 (41.2%)	0.144	1	0.704	0.023
friend request (FR) from sender (Facebook)	with FR: 58/120 (48.3%) no FR: 61/160 (38.1%)	2.924	1	0.087	0.102
profile information of the sender (Facebook)	closed: 64/140 (45.7%) open: 55/140 (39.3%)	1.184	1	0.277	0.065

Table 3.3: Statistics for clicking rates[1]

[1]It should be noted that though the insignificant gap does not show a clear bias in this particular 2014 study, it does corroborate with other studies which hypothesise that females are more prone to such attacks.

3.4.1 Reported Clicking Behaviour

Contrary to the expected response, only 117 out of 720 participants reported that they clicked and 502 participants reported not clicking. The remaining participants reported that they either did not remember clicking or the message itself. This discrepancy further provides a motive for implementing large scale and real world scientific studies with clearly defined test metrics and analytical criterion.

In the post survey questionnaire, participants were asked to explain their behaviour for clicking or not clicking on the link. Upon a thorough investigation of the statistical data, participants that clicked were divided into seven categories where Cohen's κ(See Appendix) indicated excellent agreement for four of those categories (over 0.75). The remaining three categories also showed good agreement (over 0.60). The categories with their partition spread and respective explanations are detailed in Table 3.4. The responses of the non-clickers were separated into 20 categories where 19 showed excellent agreement with Cohen's κ (over 0.75) and the remaining category showed a promising agreement (over 0.62). The categories with their partition spread and respective explanations are detailed in Table 3.5.

Category	**N**	**%**	κ	**Explanation**
Curiosity	40	34.2	0.91	Curios about the pictures, interested to see their content
Context	32	27.4	0.82	Reception of the message fits the situation of the New Year's Eve celebration
Investigation	21	17.9	0.84	Wish to find out more about the situation that caused this message
Known sender	19	16.2	0.62	Certainty or assumption that one knows the sender
Technical context	13	11.1	0.9	Technical features (operating system, browser, antivirus, university's network) will thwart threats
Fear	8	6.8	0.92	Fear that a stranger may have pictures of the receiver
Automatic	4	3.4	0.71	Clicked without thinking, impulsively

Table 3.4: Categories for reported clicks[1]

The reported clicking behaviour unambiguously shows the most common factors that lead to a user falling for a phishing scam. As demonstrated by the clicking rates (Table 3.4), the topmost supplements to a spear phishing attack are curiosity and context. For a fairly large proportion of participants, the deliberate decision of sending the message after the New Years' Eve played a catalyst that made the arrival of the message seem more convincing and less suspicious. This also exemplifies the fact that a majority of students did not pay much attention to the sender's name or ID, but instead were enticed by the content they received. While most students that clicked were either deceived by or generally callous, some hinted at a suspicion that they were being extorted or harassed with their own pictures. Furthermore, the behavioural analysis also demonstrates how using a common German name misled the participants into trusting the sender.

Category	N	%	κ	Explanation
Unknown sender	254	50.6	0.90	Sender of the message is unknown
Suspicion of Fraud*	250	49.8	0.93	Assumption that the message is fraudulent, phishing, might contain a virus
Situation context*	195	38.8	0.96	Reception of the message does not fit the situation of the New Year's Eve celebration
Life context*	58	11.6	0.75	There are no circumstances in the life of the recipient that would cause such a message
Rule of conduct	47	9.4	0.91	A behavioral rule prohibits clicking on links in such messages
Privacy	28	5.6	0.93	Private message sent to a wrong person
Message context*	27	5.4	0.87	Wrong communication channel or email address for a message like this
Message form*	25	5.0	0.91	Anonymous message, not addressed by name
Link form	20	4	0.93	Link looks suspicious
Bad experience	11	2.2	0.8	Unpleasant experience in a similar situation

Table 3.5: Statistics for reasons to not click. * indicates a merged category. Some participants reported more than one category [1].

In the cases where users were not inclined to click on the suspicious link, certain cautious behaviours emerged. Phishing messages with unknown senders were seen to be less successful and generated a suspicion of fraud or malicious intent. The anonymity of the sender was largely unsuccessful in tricking the users into clicking. This could be partially accounted for by the fact that even the most common names are just a small fraction of the whole population.

While the emergence of most behavioural categories mentioned above can be realistically explained, some are left incomplete due to the limitations on the research scale and depth. As there was no feasible reasoning provided for categories like Suspicion of fraud, fear and Rule of conduct, one can assume it to be user intuition or prior experience. Similarly, awareness or technical training could also have played a role in preventing the participants from opening the link.

CHAPTER 4

MEASURING SUSCEPTIBILITY

In the due process of figuring out mechanisms to properly defend against Spear Phishing attacks, it is imperative to discuss the leading factors directly correlated with them. In addition to the factors presented and explored by the study mentioned previously, the following sections continue to use the same reasoning methods to classify different parameters that lead to a successful phishing attack.

4.1 The weakest link

At the crux of a spear phishing attack is indubitably the user element. In an overwhelmingly significant number of cases reported to date, the receiver has played a vital role in its execution. As attackers grow adept in recognising factors that allow them to deceive another person into believing that a fraudulent link or web page is legitimate, the threat grows deeper. In the pursuit of averting attacks, companies continue to assemble security features in their networks and internal systems to constantly monitor them to detect an intrusion or attempt at the earliest stage possible. While these measures to a certain extent ensure a sufficiently confident and secure system architecture, users are often the compromising gateways. A properly targeted attack campaign against a person can yield a large lucrative return on the attacker's investment. Identification of the right human target thus nullifies the need for an actual intrusion into the network or system.
This persistent popularity of Spear Phishing can be directly linked to the attacker's ability to exploit the human element in a user. A successful attack, when executed strategically with preliminary reconnaissance, can lead to irreparable damages to a company's assets and position in the industrial ecosystem.

4.2 Vulnerability factors

Based on the conclusions drawn from the study already mentioned and others [16, 17], the actual elements that explain a victim's proclivity towards being victimised can be broken down into the following categories. These elements do not always necessarily provide the reasoning behind the success of an attack, but they indubitably paint a clearer picture for its comprehension.

Age

The age of an individual most generally decides the type of spear phishing attack or vector an attacker chooses. At a heuristic level, the number of years spent on the internet, the level of education, the perception of financial risks bring about an effect of age on the chances for falling victim to cyber attacks [18]. Young children and teenagers are more susceptible to phishing scams while using Social media networks (SMNs) and online chat rooms. They are relatively easily groomed and effectively manipulated to trust the attacker. These behaviours could be explained to some extent by the children's lack of technical knowledge/training or simply the naivety.

In age groups comprising of middle aged adults and senior citizens, spear phishing techniques are varied. The most common cases include impersonation of a bank or tax authority where the victims are coerced into revealing sensitive information. In such cases, the victims act on the feeling of fear and under the lack of due information. In the recent years, fake virus removal scam centres have also seen a meteoric rise, especially in Asia [19, 20, 21, 7].

Gender

Throughout the widely available research material on Social Engineering [22, 23, 24] and Cyber Crimes, one fact regarding the gender of the victim remains irrefutable in most cases. Studies have shown that the female participants are more inclined to respond to a spear phishing message and also more likely to continue to give their information. It can be hypothesised that the underlying rationalisation roots from the lack of technical training and knowledge, in contrast to the male population. In the particular study discussed in this paper, although the gender discrepancy seems to be almost negligible, it certainly exists. Furthermore, this disparity has been discerned to be much larger in numerous other studies [25, 26, 17]. Simultaneously, attacks impersonating a female to send phishing messages also enjoy a better success rate.

Inherent traits

While age and gender unveil some basic elements of the general population, they do not abundantly justify the human psyche and what effect it has on a person's decision making. For this purpose, the inherent personality traits perform better when considering the case of a particular victim to decipher their reaction to an attack. As clearly demonstrated by the 2014 survey by Benenson et al [27], curiosity plays a vital role in a person's decision to respond to a phishing message. A meticulously personalised message also significantly increases the chances of the receiver misplacing his/her trust towards the attacker. This manipulative strategy unsurprisingly overpowers the person's intuition and benefits from their disinterest in further investigation.

In a popular study on the Reexamination of Phishing Research [3], it was concluded that the chances of a link getting clicked can be strikingly improved by means of cognitive exploitation. A target is expected to be more responsive when faced with a circumstance of risk or loss. Instilling a sense of urgency and panic takes away the powers of intuition and doubt. On the other hand, a target can also be lured into responding using a fake connotation of benefit or gain. A notable number of successful phishing attacks stem from a target developing excitement over winning a free monetary gift or vacation. Numerous similar studies show that an unsettling number of victims fall into these two categories of cognitive exploitation [28].

4.3 Need for education

It is evident that most crimes associated with Spear Phishing result from a lack of understanding of the security tools or the lack of vigilance. Ongoing studies and practices investigating methods to reduce all variants of cyber attacks are largely focused on the aspect of user training [29, 30, 31]. Anti-phishing education has gained an enormous momentum as the scientific community continues to contemplate its efficacy in preventing future attacks. In a study of the effectiveness of such interventions [17], the number of successful phishing attempts on participants was reduced from 47% to 28%, with the average retention period of at least a week. Web-based training materials, contextual training, embedded training [30], and interactive games show promising results in improving a person's phish detection abilities. More specific educational tools like Domain name highlighting(DNH) [32] have also been explored with ambiguous results. While DNH positively increased the detection capabilities of some user groups, it does not bring a striking improvement for others. Similarly, the effectiveness of traditional training methods can be questioned as users are proven likely to forget their training over time [31].

The research into different ways of ensuring user awareness has led to the development of many educational web based tools like Phish Guru and Anti-phishing Phil [33, 34]. These tools employ embedded training and provide interactive interfaces and challenges to users. As a result, they are accorded as being more successful in teaching a user to detect phishing messages, compared to periodically sent out security notices which have been reported to generate a sense of distrust between companies and their employees.

CHAPTER 5

FILLING THE GAPS

While Spear Phishing is by no means a new phenomenon, the defined guidelines to protect against it are still considered to be in a nascent stage. The widespread presence of SMNs, chat applications and the access to internet in general has escalated the rise in cyber attacks. As organisations and educational institutions strive to find a feasible solution, the effort needed into developing the research and case studies cannot be underestimated.

5.1 Cause for Research

The study on the Reexamination of Research papers [3] on Spear Phishing looks at this exact problem with relation to certain Security Challenges. The preliminary literature collection and analysis of available papers indicated a lack in technical considerations as well as a deficiency in the number of papers on these attacks. The collection result is illustrated in Fig 5.1. Unsurprisingly, the development of more user-centric case studies is pivotal to perform a deep analysis of the users' reasoning behind their behaviour. Additionally, experimental studies outside of lab environments and on massive scales are requisites to properly explaining and confirming the results drawn by current studies.

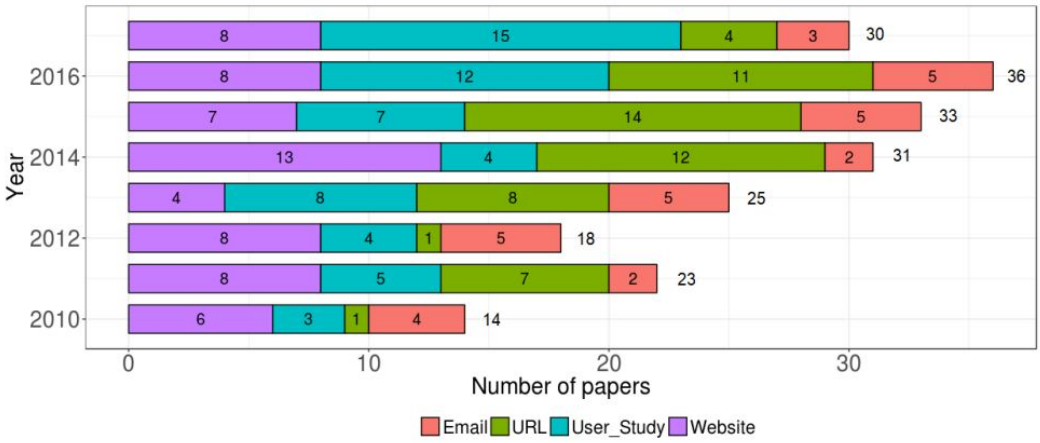

Figure 5.1: Number of papers based on topic[3]

It is also imperative to note the limitations of current studies and the challenges faced by the research groups. A large proportion of limitations are posed by the imbalanced data sets available on past incidents of spear phishing. The current state of available information rarely tackles the issues of dataset diversity, let alone emphasise it. Moreover, while issues like temporal proximity (data recency) and quality play barriers to research, the reluctance of companies to share such incidents further leads to limited data available to researchers. This reluctance might arise from the companies' intention of minimising the damage to its reputation. Majority of present studies are also shown to neglect the important notions of base-rate fallacy(See Appendix) and real-time detection.

5.2 The future of Spear Phishing

The rampant growth of the internet and the ever increasing pervasiveness of SMNs continue to offer limitless opportunities and attack vectors for attackers to target the users for personal gain. Supplementary to this is the rising abundance of handheld devices, which are less secure and much more convenient for data collection [23, 35]. As the attackers develop newer methods, the defense needs to evolve with it. Presently, the usage of Machine learning to detect phishing messages has been partially effective as these algorithms are trained on historical data but might fail to identify a newer form of attack. Techniques Like Natural Language Processing (NLP) and Natural Language Generation [36] analysis have gained research momentum and will play a vital role in the future, both as a positive and negative tool.

Quite naturally, faced with these issues, the focus is ever so slightly shifted to training the users instead to detect malicious messages. More and more organisations are gaining awareness and incorporating security training into their day-to-day operations. The current state of knowledge on these attacks while inadequate, is still relevant and will drive the development of stronger anti-phishing systems going forward. Altogether, Spear Phishing attacks are expected to continue their rampant pace in the cyber space. The abundance of creativity and sophistication on the attackers' part will ensure the debate on cyber security continues to gain traction and scrutiny.

CHAPTER 6

CONCLUSION

This paper has brought to light the major characteristics that contribute to the realisation of a spear phishing attack. It discusses in adequate detail what makes an individual susceptible to them. Demonstrably, it shows how a person's social inclination, age, gender and personality traits affect their proclivity to fall for a phishing scam. The realisation mechanism of cyber attacks is effectively boiled down to the exploitation of an individuals cognitive function. While it is clear how these physical as well as personal identifiers affect a person's rationalization and thinking, there is simply inadequate information available to clearly draw a connection. As people grow more accustomed to social media platforms and continue sharing their personal information online, it provides ample motives and opens doors for malicious parties to launch tailor-made attacks. The 'personalisation' capability of spear phishing attacks makes it even more difficult to detect compared to spam phishing baits and correspondingly makes the intended targets less suspicious. The sections in the paper go on to emphasise the need to educate the users, in addition to strengthening the existing network architectures and implementing more sophisticated safeguards. Essentially, strategically deployed combinations of technology along with user education and stringent security policies can significantly reduce the likelihood that a person will fall victim to this growing threat of Spear Phishing.

APPENDIX A

APPENDIX

1 **Pearson's chi-squared Test** : A statistical tool to test whether the distribution of certain categorical data is correct and to evaluate how likely it is that any observed difference between the sets arose by chance.

2 **Cramer's V or Phi** : A statistic used to measure the strength of association between two nominal variables, and it take values from 0 to 1. Values close to 0 indicate a weak association between the variables and values close to 1 indicate a strong association between the variables.

3 **Cohen's Kappa** : A statistic used to measure inter-rater reliability (and also Intra-rater reliability) for qualitative (categorical) items. It is generally thought to be a more robust measure than simple percent agreement calculation, as κ takes into account the possibility of the agreement occurring by chance.

4 **Base-rate Fallacy** : The base rate fallacy, also called base rate neglect or base rate bias, is a fallacy. If presented with related base rate information and specific information, the mind tends to ignore the former and focus on the latter. In the scope of this paper, it pertains to the incidence of the attack (the base-rate) and the probabilities of false positives and negatives.

BIBLIOGRAPHY

[1] Robert Landwirth Zinaida Benenson, Freya Gassmann. Unpacking spear phishing susceptibility. Report, Friedrich-Alexander-Unversität Erlangen-Nürnberg, Universitäts des Saarlandes (https://www.semanticscholar.org/paper/Unpacking-Spear-Phishing-Susceptibility-Benenson-Gassmann/b9aec954cb5cf4f17fe034848f38c4fdced0f693), 2017 (Date accessed: 16.01.2020).

[2] Seema Kathuria Diana Kelley. Spear phishing campaigns—they're sharper than you think. *Microsoft Blog (https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/)*, 2019 (Date accessed: 16.01.2020).

[3] Ayman El Aassal Rakesh Verma Avisha Das, Shahryar Baki and Arthur Dunbar. Sok: A comprehensive reexamination of phishing research from the security perspective. Report, (https://arxiv.org/pdf/1911.00953.pdf), 2019 (Date accessed: 16.01.2020).

[4] Scott Olson. The impact of spear phishing on organizations and how to combat this growing threat. *HelpnetSecuritz (https://www.helpnetsecurity.com/2019/03/11/spear-phishing-impact/)*, 2019 (Date accessed: 16.01.2020).

[5] Adrien Gendre. How much does a spear phishing attack cost? *VadeSecure (https://www.vadesecure.com/en/spear-phishing-cost/)*, 2015 (Date accessed: 16.01.2020).

[6] Dimitri Perret. What is the financial impact of a spear phishing attack on a brand? *VadeSecure (https://www.vadesecure.com/en/what-is-the-financial-impact-of-a-spear-phishing-attack-on-a-brand/)*, 2016 (Date accessed: 16.01.2020).

[7] Kaspersky. Spam and phishing statistics report q1-2014. *Kaspersky Blog (https://www.kaspersky.com/resource-center/threats/spam-statistics-report-q1-2014)*, 2014 (Date accessed: 16.01.2020).

[8] Inc. FireEye. Spear phishing attacks: Why they are successful and how to stop them (https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf). *White Paper*, 2016 (Date accessed: 16.01.2020).

[9] Jameel A. Qadri M. Tariq Banday. Phishing - a growing threat to e-commerce. Report, University of Kashmir Srinanagar, Middlesex University London (https://arxiv.org/ftp/arxiv/papers/1112/1112.5732.pdf), 2017 (Date accessed: 16.01.2020).

[10] Lorenzo Franceschi-Bicchierai. Russian hackers launch targeted cyberattacks hours after trump's win. *Motherboard Tech by Vice (https://www.vice.com/en_us/article/nz79gb/russian-hackers-launch-targeted-cyberattacks-hours-after-trumps-win)*, 2016 (Date accessed: 16.01.2020).

[11] Jason E. Thomas. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Report, International Journal of Business and Management;(https://doi.org/10.5539/ijbm.v13n6p1), 2018 (Date accessed: 16.01.2020).

[12] Adrien Gendre. Spear phishing and ransomware – a toxic match made in hacker heaven. *VadeSecure Blog (https://www.vadesecure.com/en/spear-phishing-and-ransomware/)*, 2016 (Date accessed: 16.01.2020).

[13] Andrew Tarrh Ashley Hansberry, Allan Lasser. Cryptolocker: 2013's most malicious malware. Report, Boston University, Massachusetts(https://www.cs.bu.edu/~goldbe/teaching/HW55815/cryptolockerEssay.pdf), 2013 (Date accessed: 16.01.2020).

[14] Phishlabs. 2019 phishing trends and intelligence report the growing social engineering threat. Report, Phishlabs (https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf), 2019 (Date accessed: 16.01.2020).

[15] Nick Hopkins. China suspected of facebook attack on NATO's supreme allied commander. *The Guardian (https://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato)*, 2012 (Date accessed: 16.01.2020).

[16] Ersin Dincelli Sanjay Goel, Kevin Wlliams. Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems (https://aisel.aisnet.org/jais/vol18/iss1/2/)*, 18, 2017 (Date accessed: 16.01.2020).

[17] Ponnurangam Kumaraguru Lorrie Cranor Julie Downs Steve Sheng, Mandy Holbrook. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. Report, Carnegie Mellon University,Indraprastha Institute of Information Technology (http://lorrie.cranor.org/pubs/pap1162-sheng.pdf), 2010 (Date accessed: 16.01.2020).

[18] Huizi Yang Donovan Ellis Sandeep Dommaraju Melis Muradoglu Devon Weir Adam Soliman Tian Lin Natalie Ebner Daniela Oliveira, Harold Rocha. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. Report, University of Florida, New York University (https://dl.acm.org/doi/pdf/10.1145/3025453.3025831?download=true), 2017 (Date accessed: 16.01.2020).

[19] Chloe Biscoe. India third most targeted country for phishing attacks. *IT Governance Blog (https://www.itgovernance.asia/blog/india-third-most-targeted-country-for-phishing-attacks)*, 2018 (Date accessed: 16.01.2020).

[20] Alfred Siew. Over 14 million phishing attempts in southeast asia in first half of 2019: Kaspersky. *Techgoondu*, 2019 (Date accessed: 16.01.2020).

[21] Shannon Williams. Southeast asia a hotbed for phishing attacks. *SecurityBrief (https://securitybrief.asia/story/southeast-asia-a-hotbed-for-phishing-attacks)*, 2019 (Date accessed: 16.01.2020).

[22] Malcolm Pattinson Agata McCormac Marcus Butavicius, Kathryn Parsons. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. Report, Australasian Conference on Information Systems(https://arxiv.org/ftp/arxiv/papers/1606/1606.00887.pdf), 2015 (Date accessed: 16.01.2020).

[23] Davide Balzarotti Evangelos Markatos, editor. *The Red Book: A Roadmap for Systems Security Research : The SysSec Consortium (http://www.red-book.eu/m/documents/syssec_red_book.pdf)*. 2013 (Date accessed: 16.01.2020).

[24] Bimal Parmar. Protecting against spear-phishing. *Faronics (https://www.faronics.com/assets/Spearphishing_BP_EMEA.pdf)*, 2012 (Date accessed: 16.01.2020).

[25] Xinguang (Steve) Sheng. A policy analysis of phishing countermeasures. Report, Carnegie Mellon University (http://www.chariotsfire.com/thesis/), 2009 (Date accessed: 16.01.2020).

[26] Ahmed El Zarka Ali Darwish and Fadi Aloul. Towards understanding phishing victims' profile. Report, Zayed University – UAE, American University of Sharjah – UAE (https://ieeexplore.ieee.org/abstract/document/6454454), 2012 (Date accessed: 16.01.2020).

[27] Zinaida Benenson, Anna Girard, Nadina Hintz, and Andreas Luder. Susceptibility to url-based internet attacks: Facebook vs. email. pages 604–609, 03 2014 (Date accessed: 16.01.2020).

[28] Robert Abel. Study shows which phishing attacks most successful. *(https://www.scmagazine.com/home/security-news/network-security/study-shows-which-phishing-attacks-most-successful/)*, 2018 (Date accessed: 16.01.2020).

[29] A.Lefaillet M.Mugaruka C.Raibaud V.Bernard, P-Y.Cousin. Improvement of email threats detection by user training. Report, ECE Paris School of Engineering Paris(`https://arxiv.org/ftp/arxiv/papers/1706/1706.09727.pdf`), 2017 (Date accessed: 16.01.2020).

[30] Jesse D. Freeman M. Eric Johnson Deanna D. Caputo, Shari Lawrence Pfleeger. Going spear phishing: Exploring embedded training and awareness. Report, MITRE, I3P Dartmouth College, Vanderbilt University (`https://ieeexplore.ieee.org/document/6585241`), 2013 (Date accessed: 16.01.2020).

[31] Alessandro Acquisti Lorrie Faith Cranor Ponnurangam Kumaraguru, Steve Sheng and Jason Hong. Teaching johnny not to fall for phish. Report, Carnegie Mellon University (`http://lorrie.cranor.org/pubs/johnny_paper.pdf`), 2009 (Date accessed: 16.01.2020).

[32] Eileah Trotter David Ma John Aycock Eric Lin, Saul Greenberg. Does domain highlighting help people identify phishing sites? Report, University of Calgary, Canada(`https://dl.acm.org/doi/10.1145/1978942.1979244`), 2011 (Date accessed: 16.01.2020).

[33] Alessandro Acquisti Lorrie Faith Cranor Jason Hong Ponnurangam Kumaraguru, Yong Rhee. Protecting people from phishing: The design and evaluation of an embedded training email system. Report, Carnegie Mellon University (`http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.1457&rep=rep1&type=pdf`), 2007 (Date accessed: 16.01.2020).

[34] Ponnurangam Kumaraguru Alessandro Acquisti Lorrie Faith Cranor Jason Hong Elizabeth Nunge Steve Sheng, Bryant Magnien. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. Report, Carnegie Mellon University (`https://cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf`), 2007 (Date accessed: 16.01.2020).

[35] David Wagner Adrienne Porter Felt. Phishing on mobile devices. Report, University of California, Berkeley (`https://pdfs.semanticscholar.org/94b2/44c518f431f84d2e00317709c98771a91eca.pdf`), 2011 (Date accessed: 16.01.2020).

[36] Nicola Dragoni Alberto Giaretta. Community targeted phishing: A middle ground between massive and spear phishing through natural language generation. Report, Centre for Applied Autonomous Sensor Systems (AASS), Orebro University, Sweden, DTU Compute, Technical University of Denmark(`https://arxiv.org/pdf/1708.07342.pdf`), 2017 (Date accessed: 16.01.2020).