Why Phishing continues to work

Asela Jayatilleke, Parakum Pathirana

Abstract— Phishing is an attack vector that is increasingly being used as part of social engineering campaigns to 'trick' unsuspecting users into ultimately revealing their credentials to sites containing sensitive information. Whilst technological controls are being implemented, as the term 'social engineering' suggests, phishers mainly attempt to befriend and instruct users to unknowingly share their credentials with the phisher. With limitations on how technology can assist in detecting phishing attacks, it has become essential that users have a sound knowledge on how to identify and respond to phishing attacks.

This research focuses on the available publications and scientific studies carried out to assess the current knowledge on phishing and why users become victims of phishing attacks. The work of this research attempts to identify the various avenues in which phishing attacks take place which would greatly assist in identifying the methods adopted by phishers to carry out the attacks. The research then attempts to identify reasons as to why users continue to become victims of phishing attacks and analyze the incorrect assumptions made by them, which would serve as a valuable input in order to carry out increased information security and phishing awareness, focusing on users' weak points so as to ensure maximum success of the initiative.

Index Terms— Phishing, Social Engineering, identity theft, unauthorized access, cyber attacks, cyber impersonation, email security

1 Introduction

Attackers are no longer dependent solely on technology to gain unauthorized access to information systems. With the ever increasing number of information system users, attackers now resort to building up relationships with unsuspecting users and elicit information through them. This is commonly known as "Social Engineering". A commonly used Social Engineering technique is 'Phishing'. The Anti-Phishing Work Group (APWG), 2017 [1], defines phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials."

Despite awareness and continuous technological improvements, malicious individuals are increasingly adopting social engineering techniques in order to gain access to unauthorized information. The APWG Phishing Activity Trends Report for the fourth quarter of 2016 highlights some alarming statistics which show that users are increasingly becoming victims of phishing attacks.

Some of the key highlights of this report are as follows:

1. The total number of phishing attacks in the year 2016 was 1,220,523, a 65% increase over the previous year.
2. The fourth quarter of 2004 saw an average of 1,609 phishing attacks per month. The fourth quarter of 2016, APWG saw an average of 92,564 phishing attacks per month, an increase of a staggering 5,753% over just 12 years.
3. An average of 318 different brands was exploited by phishing attacks.

The cost of phishing attacks is rising rapidly. The Federal Bureau of Investigation (FBI) in the US estimates the damages caused by phishing attacks to be in excess of USD 2.3 billion each year (Federal Bureau of Investigation, 2016) [2].

In the light of the above statistics, the key question arises – why do users increasingly continue to become victims of phishing attacks?

2 Literature Review

Phishing is one of the many different, yet popular, Social Engineering techniques. In order to gain a better understanding of how phishing works, it is essential to gather an understanding on the concept of Social Engineering. Social Engineering is not a new concept. In fact, much research has been conducted on Social Engineering and Phishing as a technique to gain access to unauthorized information. Harl (1997) provides a definition for Social Engineering as "the art and science of getting people to comply with your wishes"[3]. In the context of information and information systems, the 'wishes' are to gain access to information which is otherwise unavailable to the attacker. Thus, Social Engineering can be considered as 'psychological manipulation' to achieve one's goals.

However, this does not imply that social engineering does not depend on technology. Indeed, technology plays a crucial part in social engineering schemes as attackers are heavily dependent on technology to 'play' around with the psychology of potential victims. Cialdini (2000) identifies six basic tendencies of human behavior [4] which an attacker could 'exploit' in order to achieve his/her objectives. These are namely - authority, scarcity (e.g. comply with the attackers request in order to take advantage of a limited time offer), liking, reciprocation, commitment (consistency) and social proof (i.e. attempting to convince victims to comply by presenting facts and figures showing how much others have complied, so as to provide assurance). Stevens (2002) refers to behavioral traits [5] such as 'conformity' and the 'desire to be helpful', which may be exploited by 'phishers'. Jordan and Goudey (2005) makes reference to 'inexperience' and 'curiosity' of users [6] as factors that could allow them to become victims of phishing attacks.

Phishing can broadly take place in two forms. The first is via social engineering where attackers use emails claiming to be from legitimate businesses direct customers to counterfeit websites, which are designed to impersonate the business entity, where users are asked to enter usernames, passwords and/or other confidential information which an attacker could then use to his or her advantage.

The other, phishing via technical subterfuge involves automatically infecting end user computers with malware that either redirect users to phishing websites or capture keystrokes which are then transmitted to the attacker, without any indication to the user. Robila and Ragucci (2006) states that 'Evolution does not only apply to plants and animals; it also applies to human technology' [7]. When faced with threats, defenses are strengthened to meet and counter those threats. However, it does not stop there. When defenses are brought forward to counter threats, the threats change their approach and become stronger, making the new defenses weaker once again. Information Technology security and the threat landscape evolves in the same manner. 'Throughout this ongoing race, one thing remained constant as the weakest link, the human factor' [7].

It is based on these premises that Karakasiliotis, Furnell and Papadaki (2006) carries out an empirical study [8] to determine the level of susceptibility of computer users to fall victim to phishing attacks. For this purpose, a questionnaire consisting of 20 email messages is presented to the participant and participants are asked to judge its legitimacy. Participants have to mark each email message with one of the following answers – 'legitimate', 'illegitimate' and 'don't know', with the option for users to provide reasoning for their responses.

Karakasiliotis, Furnell and Papadaki [8] identifies six elements, which can be detected by a recipient, that would help them decide if a particular email message was legitimate or not. These elements are as follows:

1. Recipient: Did the message include a part that addressed the recipient by his/her name or some other wording (e.g. an account number, registration number etc.) which makes it easier convince the recipient that the sender was in possession of valid information about them?
2. Sender: Did the message body contain details of a specific individual whom a recipient could attempt to contact for further information, instead of a generic claim such as 'XYZ Service Desk' etc. This could also take the form of email spoofing to make the email appear to have been sent by an individual/party known to the recipient.
3. Use of Images and logos: Did the message include graphical content (including logos of the brand/entity the email is attempting to impersonate) that could help to improve the appearance, enforce brand identity etc. that would overall help better convince the recipient that the mail is genuine.
4. Unformatted layout: Was the message presented in an unformatted and unprofessional manner (e.g. mid-sentence line breaks, improper alignment etc.)?
5. Typographical / linguistic errors: Did the message contain any spelling mistakes or grammatical errors?
6. URL / link: Did the message attempt to encourage the recipient to click on a hyperlink?

Upon analysis of the results of the above, Karakasiliotis, Furnell and Papadaki (2006) notes that the overall level of correct classification is 42%, with 32% wrong classifications and 26% responses of "don't know" [8]. This can alternatively be interpreted as 58% of emails not being classified correctly, which raises concerns on the awareness levels among users.

Comments submitted by users are also considered in the analysis. From a total of 89 respondents providing 1,653 distinct comments, the following first level and second level grouping is derived:

1. Visual
   a. Colored, formatted email vs. Plaintext email
   b. Logo/Trademark
   c. Footnote
   d. Copyright statement
2. Technical
   a. Whether URL shown in the message appears to be related to the sender
   b. Presence of secure URLs (https)
   c. URL verification - directly typing the URL as opposed to clicking the link
   d. Sender's email address (domain)
3. Language and Content
   a. Personalized email (recipient's name, other personal data)
   b. Typographical/grammatical errors
   c. Forceful language
   d. Attempts to trigger a desire to be helpful
   e. Asserting authority
   f. Social proof
   g. Scarcity

In-depth analysis of the responses together with the comments stated gives rise to the following observations:

A near 25% of the respondents mention logos, footers and copyright symbol elements as justification for identifying an email as 'legitimate' when in fact it is actually an illegitimate email.

Although many participants cite technical cues within emails as justification for their answers, in many instances the interpretations were incorrect. For example, email addresses such as admin@ebay.replymsg1223.com were considered as legitimate due to the fact that a reputed organization's name was part of the email domain. This clearly show that many users do not have adequate technical awareness on how to identify phishing emails. The danger in this trend is that users may take incorrect decisions based on their 'limited' technical knowledge, which would ultimately result in them actually becoming victims.

Merwe, Loock and Dabrowski (2005) states that there are five individual issues [9] that have to be addressed in order to combat phishing: education, preparation, avoidance, intervention and treatment. However, the work of Merwe, Loock and Dabrowski only gives minimal attention to education and focuses only on the fact that education and awareness needs to be created. The researchers do not, however, suggest a medium for effectively delivering the required awareness. A study carried out by Jagatic et al (2007) suggests that the likelihood for internet users to become victims of phishing attacks may rise up to four-fold if the soliciting email is spoofed to appear as being sent by a known party [10]. The accelerated use of social media and professional networks provides much of the required information for a phisher to pose as an 'acquaintance' of a victim. This study involves 1,700 students who were sent phishing emails based on web browsing history and email communications with fellow students (in order to spoof email addresses). Analysis of the findings show that the experiment yielded a high success rate (over 50% in some instances), primarily due to the use of social context information. A unique feature of this experiment is that the students were informed of their participation in the survey and a discussion forum was setup for respondents to discuss and share ideas on the study. The overall conclusion of the study is that 'context-aware' phishing attempts (phishing attempts which are based on user habits) are far more likely to be successful.

Workman (2007) states that most research focuses on security technologies and security infrastructure management practices in order to strengthen information security defenses [11]. The author further states that the behavioral aspect of users and people's failure to take necessary precautions against information security threats, leading to information security breaches, has been greatly ignored. The U.S. Department of Justice (2004) [12] estimates that one in every three people will fall victim to social engineering attacks at some point in their lifetime. The author further mentions that whilst social engineering is a major avenue for information security breaches, there has been limited research and as a result, little assistance to managers in order to address such concerns.

Workman (2007) [11] highlights that social engineering takes many different forms, although the techniques mainly rely on the theory of 'Peripheral Route Persuasion'. 'Peripheral Route Persuasion' is introduced in the work of Petty & Cacioppo (1986) who propose the Elaboration Likelihood Model (ELM) [13] to better understand how humans are convinced to carry out a particular task. (i.e. in this research, respond to a phishing email). In the ELM, persuasion based on relatively high degrees of thinking is called the central route to persuasion, whereas persuasion that occurs with relatively little thinking is called the peripheral route to persuasion. The two different routes identified can mean either of the following:

1. Different people respond to the same information in varying manners.
2. The same people respond in different manners to the same information under differing circumstances.

Petty and Hinsenkamp (2017), in their study of the Elaboration Likelihood Model [14], focuses on the peripheral route to persuasion and suggests that humans are unable to focus their attention 100% to every little detail in a situation (i.e. a phishing email in this context) and tend to rely on simple heuristics or 'peripheralcues' in order to arrive at a conclusion. Thus, potential hackers can make use of these simple details to exploit individuals who exercise the peripheral route to persuasion.

The results of the empirical study carried out by [11] arrives at the following conclusions:

1. People who are high in normative commitment feel obliged to reciprocate social engineering gestures such as receiving free software, gift certificates etc. by providing company email addresses, employee identification numbers, financial and insurance data, and other confidential and sensitive information to the 'phisher' who gave the 'freebies' in the first place.
2. People who are high in continuance commitment tend to provide information to escalating requests. Such individuals will even give up increasingly sensitive information as part of an online game just to try to win the game.
3. High affective commitment was also found to contribute to successful social engineering. These individuals tend to provide information because they want to be part of a socially desirable group or be accepted.

Jensen, Durcikova and Wright (2017), in their research [15], suggests that phishing attacks rely on a single person within a group to respond, in order to commence propagating the malware across networks. This concept of eliminating the 'weakest link' within a group is suggested in the research where users are encouraged to work in groups in order to create a 'human firewall' thereby increasing their defenses. This theory is further supported by the authors' suggestion to maintain a centralized knowledge base which can be accessed by users to help them take more accurate decisions when attempting to identify phishing emails. However, the authors also state that it is vital for users to update the knowledge base with new knowledge to ensure its increasing success.

Jakobsson & Young (2005) provides an in-depth discussion [16] into 'Distributed Phishing Attacks' (DPAs) which makes it increasingly difficult for law enforcement agencies to track and shut down phishing sites. The underlying theory is that if the links in phishing emails direct the user to websites hosted at different locations, it becomes difficult to detect and shutdown such sites as there is no way of proactively identifying a phishing site, since there are no links between one another (i.e. distributed).

MailFrontier has developed a tool to assess the 'Phishing IQ' of users. This test presents users with a combination of phishing and legitimate emails and requires them to be identified correctly. Within a period of 12 months, an average 82% of the test takers identified phishing e-mails correctly, but legitimate e-mails are only identified correctly by 52%. This could be attributed to the fact that some respondents identify all emails in the experiment as phishing emails. Nonetheless, the figures show that respondents tend to be more risk averse in such situations, which is a good indication (i.e. it is better to identify a legitimate mail as a phishing attempt than to identify a phishing attempt as a legitimate mail).

Robila and Ragucci [7] further point out that the adopting the MailFrontier test within a university environment could result in incorrect results. The primary reason for this is since the test in question is generic, there would be mails (both phishing and legitimate) from entities which students have not interacted at all. In such instances, they could be categorized as either Spam or as phishing emails. In order to overcome this, Robila and Ragucci suggest a hybrid approach. This is to develop a similar IQ test, but with emails from services/entities which the target group have a high probability of using. This would help eliminate the inexperience factor and help identify more focused reasons as to why a user may falsely identify an email. However, results from this study also revealed an average IQ of 57.29%. This implies that approximately one out of every two e-mails are erroneously identified – either a legitimate message as a phishing attack, or a phishing attack, as a legitimate e-mail.

Some interesting observations can be derived from the work of Jagatic et al (2007) [10]. Upon analysis of the posts made by participants, the authors have been able to identify some of the emotions displayed by the subjects:

1. Anger – certain respondents called the experiment as being 'unethical', 'inappropriate', 'illegal' and called for the researchers to be 'prosecuted', 'expelled', or otherwise 'reprimanded'. These reactions clearly show that apart from potential monetary losses of phishing attacks, there is a significant psychological impact on victims. Despite the fact that no sensitive information was obtained in this experiment, the subjects appear to be 'upset and annoyed' by the fact that they became victims of the (staged) attack.
2. Denial – there were no posts by students where they admitted to becoming victims of the attack. Several posts claim that the poster did NOT become a victim and attempts to highlight that they are well aware of how to identify phishing attempts and stay safe. This tendency of denial could result in a great number of successful phishing attacks going unreported.
3. Misunderstanding of email – Many subjects were of the opinion that the phishing emails were circulated through technical manipulation of the email system by the researchers together with the University IT team and it is not possible otherwise to receive such emails. This line of thinking highlights two concerns: a) users believe spoofing emails/generating phishing mails is a difficult task and b) the security mechanisms of email is much stronger than what it actually is. The result is that many users believe that it is a phishing attack is an extremely rare occurrence.
4. Dangers of publicly posted personal information: Many subjects were not properly aware of how the researchers had obtained information about their friends, and assumed that they had accessed their address books (again, possibly with the assistance of the University IT). Others, having understood that the information was gathered from publicly posts on social network sites, objected that their privacy had been violated. The users failed to understand that in the same way the researchers access the information, other parties too could do the same. They also failed to appreciate that such information was highlighted as a result of this study. Many believe that their information is protected by in-built privacy controls and terms of service and fail to realize that almost anyone (with malicious intent and disregard for ethics) can easily gain access to this information.

Studying the work of [7], [8] and [10], it is observed that a common element present is the methodology used to identify why individuals fall victim to phishing attempts. The studies commence by asking a sample user base to identify phishing emails from legitimate ones. The researchers then attempt to find out why a respondent makes a particular choice which would in turn help to identify factors that 'assist' users in differentiating between phishing emails and legitimate ones.

However, there are several shortcomings that can be observed in these studies. The first is that sample sizes are not adequate. Since the year 2016 saw a staggering 1,220,523 SUCCESSFUL phishing attacks, with probably much more going unreported, it is essential that a larger sample size is selected.

This however, has been addressed to an extent in the work of Jagatic et al (2007) where the sample consisted of 1,700 users [10]. However, it should be noted that this sample consisted of university students. From the perspective of a 'phisher', the value of gaining unauthorized access to confidential information of university level students should also be considered. Phishers are most likely to target white-collar employees and other senior professionals. This is due to the fact that they are likely to have information which would be of greater value to the malicious individual (e.g. a 'phisher' would derive greater value by obtaining the internet banking credentials of a high net-worth executive as opposed to that of a college student). Hence, a study of this nature would be of greater value if the sample chosen is a better representation of the potential victims.

Another shortcoming is the type of sample emails used. In most cases, it is a generic set of emails that are circulated amongst the sample user group. As pointed out by [7], this could result in phishing emails being filtered simply because the respondent has no affiliation to the organization the email claims to be from. As such, greater use of 'context-aware' emails would help better test the capabilities of users in identifying phishing emails.

Based on the above analysis of the existing literature and the shortcomings identified, this research aims to identify the degree of awareness among computer users in five aspects of phishing, as illustrated in Fig. 1.

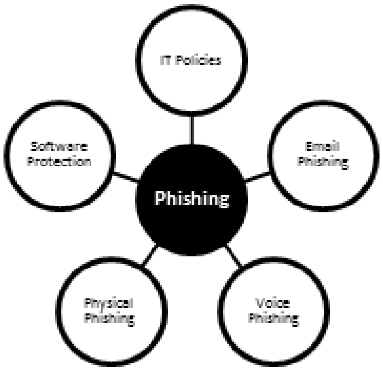


Fig. 1. Phishing Awareness Model. The above diagram illustrates five aspects based on which awareness among computer users will be assessed.

The research aims to address the following questions:

1. Are users aware of how organizational IT policies address phishing concerns?
2. Are users aware of how to identify email phishing attempts?

3. Are users aware of how to identify voice phishing attempts?
4. Are users aware of how to react to physical phishing attempts?
5. Are users aware of the limitations with regard to software based protection mechanisms?

3 Research Methodology

This study was carried out using a quantitative design. Multiple choice answer questionnaires were used to capture the required data.

3.1 Population

The population comprised of the executive and managerial level staff of a leading conglomerate in Sri Lanka. The population consists of both male and female respondents and amounts to 734 persons. The stated staff categories were selected as they heavily use computers and IT systems as part of their work, which makes them highly prone to phishing attacks.

3.2 Sample

A sample of 250 persons was identified for the purpose of carrying out this research. This was based on the formula for determining sample size introduced by [17]. The suggested number was 248, which was rounded to 250.

3.3 Sampling Technique

Stratified Random Sampling was used for selecting the sample for this survey. The participants were divided into strata on the basis of a single characteristic – gender (Male or Female).

4 Data Collection

Data collection was carried out primarily through the use of questionnaires. Google Forms were used to develop the questionnaires and distribute easily among the sample (using an email link). A period of 3 weeks was given for individuals to respond with periodic reminders being sent out via email.

The questionnaire created is based on the conceptual framework derived from the literature review. The questionnaire aims to identify the awareness levels among the sample with regards to phishing and where wrong responses were provided, identify the nature of incorrect assumptions made so that suitable training could be provided.

Part I of the questionnaire is designed capture demographics such as gender and age group. Part II presents 4 multiple choice answer questions which structured to capture the user awareness on phishing attacks. The questions address the following areas relating to phishing:

1. Coverage of phishing in IT policies and procedures
2. Email phishing
3. Voice phishing
4. Physical phishing
5. Software protection

The questionnaire was reviewed by 2 persons in the Information Security and Enterprise Risk domains and found to be suitable to capture the required data.

5 Data Analysis

The results from the questionnaire responses were analyzed and the following information indicated in Table 1 and Table 2, were derived.

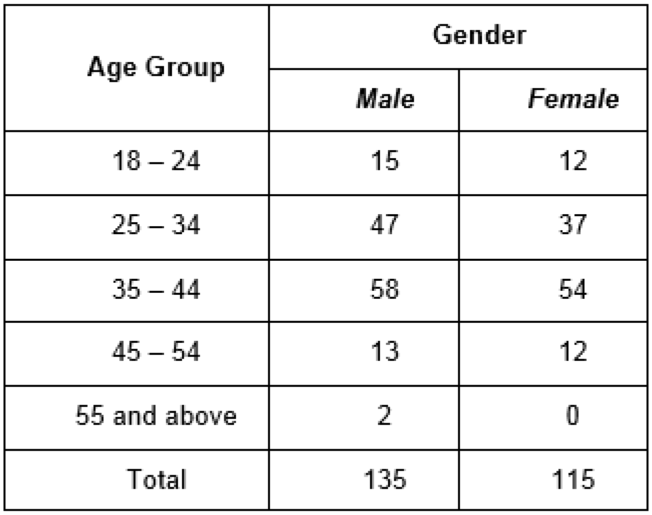
6 Results and Discussion

Based on the findings of Part I, it was observed that 54% of the respondents were Male as opposed to 46% female. It was also observed that majority of the respondents (45.70%) fall within the 35-44 years' age category. This indicates that the majority of the sample selected are young, yet experienced persons, who can be expected to make informed decisions regarding IT security.

Based on the analysis of the findings of Part II, a number of conclusions can be arrived at, especially with regards to the incorrect responses provided. These are listed below as follows:

6.1 Coverage of phishing in IT policies and procedures

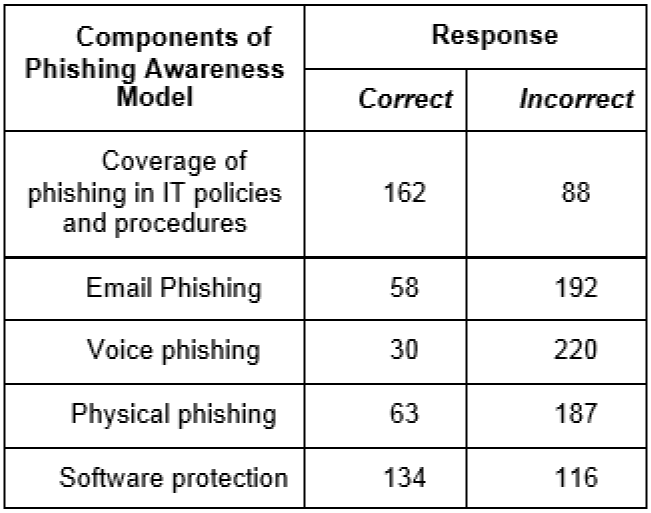
TABLE 1
Questionnaire Part I



Age Group	Gender	
	Male	*Female*
18 – 24	15	12
25 – 34	47	37
35 – 44	58	54
45 – 54	13	12
55 and above	2	0
Total	135	115

Findings from Part I of Data Collection Questionnaire

TABLE 2
QUESTIONNAIRE PART II



Components of Phishing Awareness Model	Response	
	Correct	Incorrect
Coverage of phishing in IT policies and procedures	162	88
Email Phishing	58	192
Voice phishing	30	220
Physical phishing	63	187
Software protection	134	116

Findings from Part II of Data Collection Questionnaire

Analysis of the 88 incorrect responses show that 73% of respondents stated that they have read the organization's IT policies, but they did not contain any information/advice on phishing. However, a brief review of the company's IT policies shows that phishing attacks and methods of avoiding them are included. This implies that either a) staff have not understood the contents of the policy or b) they have not read the documents in depth.

6.2 Email Phishing

A majority of the responses (77%) for this question were incorrect. Analysis of the incorrect answers provided show that many users are of the belief that if there are no visual misrepresentations in emails (logos, colors, formatting, genuine sender ID), there is no necessity to verify with the sender and/or carry out other checks such as hovering the mouse pointer over links to identify the actually destination web link. This implies that staff have severely underestimated the intelligence levels of phishing attackers and expect them to make obvious mistakes in phishing emails.

6.3 Voice Phishing

The responses to this question bring out some interesting insights to the thought patterns of respondents. Only a mere 12% provided the correct answer. However, the most interesting observation is that the remaining 88% had selected the same incorrect answer. The question presents a situation where a person pretending to be from the company IT Service Desk calls and asks the user for their Windows Login password in order to perform routine maintenance. Whilst the correct response is not to give out the password, the incorrect respondents have stated that they would give out the password and then change later on (probably within the day). This shows that whilst users do understand the risks in sharing passwords (even with IT technical staff), they believe that changing them later would mitigate those risks. What users fail to understand is that a) IT staff would not need to know individual Windows login passwords in the first place and b) after sharing your password with a third party, it takes only a matter of minutes for attacker to misuse the credentials.

6.4 Physical Phishing

Whilst phishing primarily takes place via remote electronic communications, there exists a possibility for physical phishing whereby the attacker would use social engineering techniques to work his or her way into restricted areas in an organization and then attempt to gather information. A majority of responses for this question too were incorrect (75%). Most of the respondents who provided incorrect answers chose to ignore unfamiliar persons in the office environment. This could mean that users placed absolute trust in the security personnel in the organization and that they believed that any intruders would be identified by security personnel.

6.5 Software Protection

Another area which provides some interesting insights is usage of software such as antivirus solutions and other endpoint protection mechanisms. Whilst 54% of respondents had provided the correct answers, analysis of incorrect answers show that majority of users responded stating that they need not worry about phishing attacks if a reputed antivirus/end point protection mechanism is deployed and kept up to date. Whilst such solutions can detect and block many phishing attempts, attackers strive to be 'one step ahead' and are constantly devising methods to bypass security controls. This understanding was not found among the respondents.

7 CONCLUSION

Analysis of the above results show that there is a considerable gap in the levels of awareness amongst the sample selected. On average, on 36% had provided correct answers. In order to bridge this gap, periodic awareness sessions need to be carried out. This could be in the form of email campaigns, short videos as well as physical training sessions. A Learning Management System could also be implemented to 'push' these trainings to users as well as engage them in interactive awareness sessions. Also, given the fact that the respondents were from across Sri Lanka, carrying out the awareness sessions in Sinhala, Tamil AND English media should also be seriously taken into consideration. Whilst most computer applications and email communication takes place in English, language should not be a barrier for effective information security awareness.

APPENDICES

A summary of the findings in this literature review is presented in Appendix A – Summary of Literature Review.

REFERENCES

[1] Anti-Phishing Working Group, 2017. *Phishing activity trends report*. Anti-Phishing Working Group.

[2] McCabe, J., 2016. FBI Warns of Dramatic Increase in Business E-Mail Scams. media release, Phoenix field office, Federal Bureau of Investigation, 4.

[3] Harl. (1997, May) The Psychology of Social Engineering. Text of Harl's talk at *Access All Areas III*.

[4] Cialdini, R.B (2000), *Influence: Science and practice*, HarperCollins, New York

[5] Stevens, G., 2002. Enhancing Defenses Against Social Engineering, *SANS Institute*, GIAC.

[6] Jordan, M. and Gouday, H., 2005. The signs, and semiotics of the successful semantic attack. In *14th Annual EICAR Conference* (pp. 344-364).

[7] Robila, S.A. and Ragucci, J.W., 2006, June. Don't be a phish: steps in user education. In *ACM SIGCSE Bulletin* (Vol. 38, No. 3, pp. 237-241). ACM.

[8] Karakasiliotis, A., Furnell, S.M. and Papadaki, M., 2006. *Assessing end-user awareness of social engineering and phishing*.

[9] van der Merwe, A., Loock, M. and Dabrowski, M., 2005, January. Characteristics and responsibilities involved in a Phishing attack. In *Proceedings of the 4th international symposium on Information and communication technologies* (pp. 249-254). Trinity College Dublin.

[10] Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F., 2007. *Social phishing. Communications of the ACM*, 50(10), pp.94-100.

[11] Workman, M., 2007. *Gaining access with social engineering: An empirical study of the threat. Information Systems Security,* 16(6), pp.315-331.

[12] Department of Justice (2004), Violation of 18 U.S.C. § 1030(a)(5)(B): Gaining unauthorized access, *Cybercrime Report*, 17, 188–219

[13] Petty, R.E. and Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. *Advances in experimental social psychology*, 19, pp.123-205.

[14] Petty, R & Hinsenkamp, L 2017, 'Routes to persuasion, central and peripheral', in Moghaddam, F (ed.), *The sage encyclopedia of political behavior*, SAGE Publications, Inc., Thousand Oaks,, CA, pp. 718-720, viewed 19 August 2017, doi: 10.4135/9781483391144.n330.

[15] Jensen, M., Durcikova, A. and Wright, R., 2017, January. Combating Phishing Attacks: A Knowledge Management Approach. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

[16] Jakobsson, M. and Young, A.L., 2005. Distributed Phishing Attacks. *IACR Cryptology ePrint Archive*, 2005, p.91.

[17] Krejcie, R.V., & Morgan, D.W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, 30, 607-610