Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/110413

Employee Awareness on Phishing Threats: A Comparison of Related Frameworks and Models

Mohammed Fahad Alghenaim[*], *Nur Azaliah Abu Bakar and Fiza binti Abdul Rahim*

Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia 54100 Kuala Lumpur, Malaysia

Received: 21 Mar. 2022, Revised: 22 Apr. 2022, Accepted: 5 May 2022.
Published online: 1 Jul. 2022.

Abstract: Data and sensitive information in the public sector are major targets for cyberattacks. Officials in the public sector have developed a wide range of frameworks, models, and technology to help employees understand the risk of phishing attacks. However, these models haven't been able to meet the total needs of institutions in terms of security. This study reviews the awareness frameworks and models used to increase users' awareness of phishing scams and highlights the problems and drawbacks. Moreover, this study compares the various cybersecurity awareness frameworks and models. The findings show a need to enhance current phishing awareness frameworks and models that can handle phishing attacks in the workplace while also converting them into cybersecurity training input, mainly via a digital learning platform.

Keywords: Cybersecurity, Phishing, Public sector, workplace.

1 Introduction

Over the past decade, the high prevalence of security threats in organization setups prompted measures to control the issue. Due to a lack of awareness, phishing continues to wreak havoc on a segment of society. It evolves in the form of viruses and malware directed by attackers to organizations to blackmail them into making payments lest they compromise their security system. It is worth noting that a significant source of concern for organizations is a lack of knowledge about security threats and mitigation measures. It deprives organizations of the ability to deal with Phishing threats.

The public sector is a primary target for attackers due to its sensitivity and valuable data [1]. Officials in the public sector have implemented numerous frameworks, models, and tools to enhance employees' awareness of phishing threats. However, these solutions have not proven sufficiently effective in reaching institutions' security objectives [2]. The COVID-19 pandemic has shown the weaknesses of the implemented awareness frameworks and models because they are used in either the workplace (face-to-face) or e-learning (distance learning) solutions [3]. Some conceptual frameworks and models combine workplace and e-learning awareness training but are not enough to face such a challenge as the COVID-19 situation [3]. Hence, the awareness frameworks and models need to be upgraded through the formulation of a conceptual awareness model that can work in the workplace and e-learning environments using practical awareness tools to prevent the types of issues that occurred during the COVID-19 pandemic due to lack of training from occurring in future pandemics [4]. Hamburg (2021) reviewed the concept of workplace learning and considered the strategies required to adapt it to the pandemic without losing educational efficiency [3]. Workplace learning is culturally bound and combines formal and informal elements. This challenge has emphasized the importance of transforming workplace learning without losing efficiency and employee benefits.

Therefore, a new holistic solution covering awareness and training needs to be developed. This solution should be applied in physical workplaces and through distance learning simultaneously in the public sector. This paper aims to review the awareness frameworks and models used to enhance employee (user) awareness regarding phishing attacks and discuss the challenges and drawbacks of these frameworks and models. The findings of this review will guide the development of a new awareness framework/model that meet the awareness and training needs.

The remainder of this paper is organized as follows: Section 2 introduces the different frameworks and models in employee awareness on phishing threats. Section 3 compares the frameworks and models. Finally, the conclusion is presented in Section 4.

[*] Corresponding author-mail: aalghenaim@graduate.utm.my

2 Frameworks and Models in Employee Awareness on Phishing Threats

2.1 Information Security Awareness and Capability Model (ISACM)

Information Security Awareness and Capability Model (ISACM) [5] is a framework and model that combines the theories of Situational Awareness (SA) and aspects of InfoSec best practice standards. ISACM complements and encourages the quantitative assessment of InfoSec's degree of mindfulness, specifically on phishing, at the three proposed levels.

This model defines three levels of the security model. Level 1 is the perception that is the basis for understanding the characteristics, position, and changing aspects of InfoSec awareness environmental elements. In the cyber-related situation awareness testing stage, an employee's perception is often considered the ground truth. During this stage, an employee's level of understanding of phishing is assessed. Additionally, the conduct of a member that may lead to threats of phishing attacks is also identified in level 1 of the model [5].

Level 2 of the model is comprehension. A member's comprehension of interpretation, pattern recognition, and evaluation process are examined at this level. Level 2 of the model evaluates and improves on the previous level of the model. It aims to develop a more profound understanding of phishing techniques by going a step higher to identify the social causes that affect phishing victims [5].

Level 3 of the model is projection. In this stage, the concerned parties can predict how the various relevant elements in the InfoSec environment perform in the future. The level of mindfulness of the concerned parties to the relevant aspects is assessed. It is the most significant level in the model. The members at this stage can effectively predict the threats of phishing through a wide recognition of the conducts and acts that can result in phishing attacks [5].

2.2 Situation Awareness Model (SAM)

The Situation Awareness Model (SAM) [6] can be described as the systematic process of increasing awareness levels by providing additional awareness sessions. Situation Awareness (SA) has extensively been used in military operations. The process has been critical in the direction and execution of infantry operations within the military. Military trainers and developers can leverage the technique of SA to enhance efficiency in military operations. Military trainers and developers can acquire useful information critical for their operations by synthesizing and integrating situational awareness concepts in military infantry operations. The challenges and complexities of tactical operations such as engaging the enemy in close and urban terrain and dealing with the press, military observes, non-combatants can be simplified by integrating situational

awareness techniques. This study examines and discusses several measures, disadvantages, advantages, and various considerations for their implementation. It looks at how these measures can be effectively applied in field or simulation studies of new technologies and concepts. The study is particularly designed to determine the advantages and disadvantages of the applicable measures of tactical operations to ensure that ineffective and problematic technologies are not adopted [5].

2.3 Power-Knowledge-Practice Triangle (PKPT)

One of the essential tasks to assess the risks associated with social engineering is threat recognition. It should come down to the idea of whether the end-user can address phishing threats or at least spot them promptly [7]. As Heartfield and Loukas [8] suggest, the utmost way of coping with phishing could be specific knowledge intended to protect the given organization from the damage caused by attackers. Therefore, end-users have to realize the risks associated with their activities and propose a backup plan for the organization to focus on when exposed to digital threats. InfoSec would be unlikely to remain strong if there could be no awareness of any kind among employees [9]. This also hints that all knowledge possessed or gained by end-users has to be practical and not theoretical for them to recognize threats. The key reason why this becomes possible is the continual evolution of social engineering attacks that force every stakeholder involved in activities that could be breached by social engineering to build upon their knowledge [9]. In addition, end-users may be interested in pointing out the most viable weaknesses to strengthen the local knowledge base and evade situations where they have no relevant experience to respond to a situation. Power-Knowledge-Practice Triangle (PKPT) is a conceptual framework formulated originally by Foucault [9]. PKPT is used in workplaces to reduce all kinds of risks by increasing knowledge and awareness that uses three (3) components together to ensure the effectiveness of enhancing the process of the employees' awareness, shown in Figure 2.

The figure above contains the following relationships:

Knowledge-Power: (a) without knowledge, one would not have the ability to display power; (b) without power, knowledge cannot be legitimized.

Knowledge-Practice: (a) without knowledge, one cannot deploy practices accordingly; (b) without practice, no opportunities for the team to socialize and share knowledge.

Practice-Power: (a) without practice, power relations cannot be conveyed; (b) without power, organizational transformations are unavailable to employees and executives.

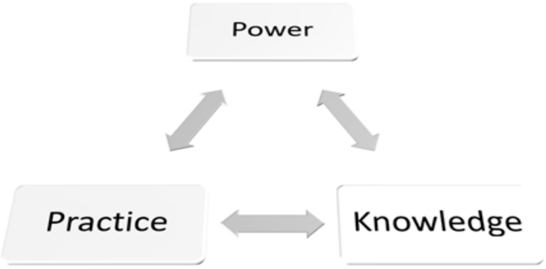

Fig.2: Power-Knowledge-Practice Triangle [9].

Constant learning is required for organizations to gain insight into social engineering basics and develop responses according to the required digital policies [10]. For instance, the researchers in [11] propose using a scoring system for potential risks to establish if a team has all the required resources to address social engineering's highest risks. Accordingly, the team needs to achieve quantifiable scores that can estimate the potential risk of an attack while ensuring that the responsible actors have enough power, knowledge, and practice to make respective decisions. Nevertheless, the team should also gain more insight into the potential threats to improve understanding and close certain characteristics of certain knowledge gaps. The key responsibility of the management, in this case, would be to allocate knowledge equally so that every unit would have access to specific data sets and entries required for the stronger prevention of social engineering attacks.

2.4 Situation Awareness Model for Phishing (SAMFP)

Situation Awareness Model for Phishing (SAMFP) by [12] is a conceptual model that uses e-learning to enhance employee awareness of phishing attacks. According to [12], e-learning has become a primary learning solution during the past few decades; moreover, e-learning has become the best solution for continuing the learning process in the public and private sectors. This security segment of e-learning has affected many spheres of human life to the extent that almost no initiatives have been implemented to strengthen InfoSec measures. SAMFP covers these 16 human factors regarding phishing attacks: temptation, urgency or scarcity, over-confidence or self-consciousness, dispositional trust, authority, threats, social proof, likability and similarity, reciprocation, curiosity, commitment and consistency, overloading, diffusion of responsibility, showing off, convenience, and interpersonal relationships. The current article's key goal is to narrow the knowledge gap due to the lack of pressure on online learners to counter Phishing attacks. This is becoming an essential factor that cannot be ignored if research in security awareness has to advance. According to [12], the current literature has paid ultimate attention to the Phishing hazards that jeopardize InfoSec. Still, it has failed to recognize the predicament of a lack of awareness among online users regarding phishing attacks in practice and research or the factors that compel victims to fall prey to phishing attacks. Even with the integration of sophisticated protection technologies, organizations that do not invest in security awareness are still vulnerable to internal and external hazards.

Therefore, [12] aimed to reduce the negative influence of phishing attacks and enhance employees' awareness by developing a new conceptual framework. This potential solution advocate for a more specific behavioral overview of the factors involved in phishing attacks. It may also measure how attacks could damage institutions or organizations. The exploitation of behavioral factors typical of phishers has to be linked to various aspects of end-user awareness (or security awareness) across the altering spheres of space and time. Space and time are two (2) dynamic variables on which the SAMFP is based and directly impact learning outcomes, as shown in Figure 3.

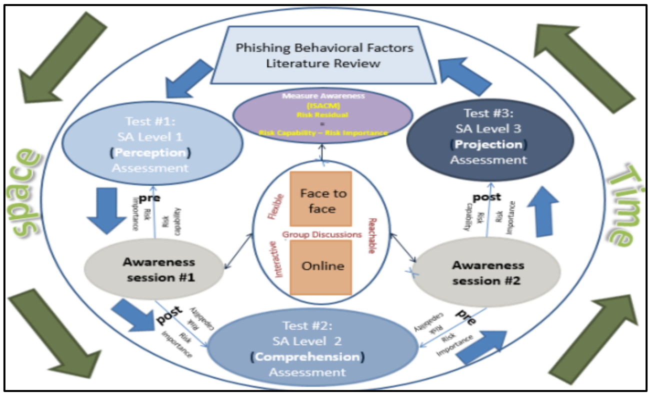
Phishing Behavioral Factors Literature Review
Measure Awareness (ISACM) Risk Residual = Risk Capability – Risk Importance
Test #1: SA Level 1 (Perception) Assessment
Test #3: SA Level 3 (Projection) Assessment
Test #2: SA Level 2 (Comprehension) Assessment
Awareness session #1
Awareness session #2
Face to face
Online
Group Discussions
Flexible
Reachable
Interactive
pre
post
Risk importance
Risk capability
space
Time

Fig. 3 Situation awareness model for Phishing [12].

The lack of security policies and guidelines shows that an in-depth awareness of phishing attacks might benefit. However, another model that has to be considered when assessing the threat of phishing and insufficient employee awareness is the Information Security Awareness and Capability Model (ISACM).

The SAMFP paradigm, based on ISACM framework [5], includes a quantitative evaluation of the subjects' degrees of awareness at the three (3) Endsley levels (perception, comprehension, and projection) that Poepjes,[5] proposed. In the ISACM framework, the approach's efficacy as a dynamic space variable was investigated and evaluated. In summary, the SAMFP is a somewhat effective model because it underpins numerous employee assessments that reveal specific behavioural factors related to awareness. The SAMFP, as one of the most comprehensive frameworks, also allows end-users to meet their learning needs while adhering to organizational awareness-related

Table 1: Awareness frameworks and models comparison table – Part One.

Name	Information Security Awareness and Capability	Situation Awareness Model	Situation Awareness Model for Phishing
Acronym	ISACM	SAM	SAMFP
Advantages	- Upgrading for SA with awareness importance, awareness capability, and awareness risk. - Offers a theoretical framework for application in InfoSec awareness because many incidents/events of InfoSec are upshots of human faults.	- It contains the 39 base controls explained by ISO/IEC 27002, classified into the 11 security control clauses. - Has a solid practical application for organizations wishing to improve InfoSec through improved awareness by identifying gaps (awareness risk) in current levels of InfoSec awareness.	- It can be used to enhance employee awareness about phishing attacks. - It covers 16 factors of human behaviors. - Can be implemented on other social engineering threats. - Is an effective model in enhancing the employees' awareness. - It can be upgraded to cover public sector institutions. - It covers the time and space issue.
Disadvantages	- General and not focusing on specific social engineering threats.	- Does not cover the 39 base controls explained by ISO/IEC 27002.	- Limited to e-learning. - Focusing only on human behaviors. - Does not use PKPT. - It uses Closed-Source online awareness tools. - Does not cover related security policies. - It uses online Closed-Source awareness tools.
Integrated	Situation Awareness (SA)	Situation Awareness (SA)	Situation Awareness (SA), Situation Awareness Model (SAM), and Information Security Awareness and Capability (ISACM).
Target	Workplaces	Workplaces	Workplaces (minimal) and e-learning (primary)
Type	Theoretical Framework and Model	Theoretical Framework	Conceptual Framework and Model
Sources	[5]	[6]	[12]

Table 2: Awareness frameworks and models comparison table – Part Two.

Name	Power-Knowledge-Practice Triangle	Routine Activity Theory	Education Treatment Phase Framework
Acronym	PKPT	RAT	ETPF
Advantages	- It can fit with any field or institution to enhance the awareness and knowledge of the employees to face any kind of risks. - It can be adopted in any awareness framework or model. - It has improved its solid method to counter any lack of knowledge. - It can connect all necessary departments and factors to achieve its security objectives in the short and long terms.	- It focuses on geographical (physical place and neighborhood) places. - The use of an Anti-phishing training program. - It shows the importance of active place management. - It highlights motivated offenders, suitable targets, and the absence of capable guardianship. - It covers the time and space issue. - It explains the importance of handlers, managers, and guardians.	- It uses e-learning by providing the employees with presentations, video clips about spear phishing, available online (open learning), and blogs. - It uses InfoSec Awareness Training for workshops. - It shows the importance of using Information Communication Technology (ICT) and Training Need Analysis (TNA).
Disadvantages	None.	- The selection of the treatment group individuals was not randomly assigned. - Does not cover other variables, such as online activity level subcultural views on cybercrime. - Does not cover related security policies.	- Does not use Open-source awareness tools to access and enhance the employees' awareness regarding Phishing attacks. - Does not cover related security policies.
Integrated	None	Crime Triangle Framework (CTF), Cyber Place Manager (CPM), and the Inter-Loop Anti-Phishing Model (ILAPM)	Knowledge-Attitude-Behavior Model (KAB)
Target	Workplaces and e-learning	- E-learning (online training).	Workplaces and e-learning
Type	Conceptual Framework	Theoretical Framework	Theoretical Framework
Sources	[9]	[19]	[17]

Table 3: Awareness frameworks and models comparison table – Part Three.

Name	**Framework of Phishing Susceptibility**	**Phishing Susceptibility Framework**
Acronym	FPS	PSF
Advantages	- It focuses on the human (users) behavior to achieve the user's self-efficacy. - It focuses on spear-phishing and generic phishing emails threats. - The use of an Anti-phishing training program. - It shows the importance of examining the message-related factors and the group methodology. - It covers the range of potential interventions, such as technical, training, process, and design solutions, and shows how these points are effective exploits within institutions.	- Focus on social susceptibility in the workplace by understanding various emotional and contextual triggers. - It shows that employees' problems disregard the systems in place in their firms for security precautions and standards. - It focuses on creating security standards that necessitate a thorough understanding of personnel behavior to create solid awareness training programs.
Disadvantages	- Does not use Open-source awareness tools to access and enhance the employees' awareness regarding Phishing attacks. - Does not cover related security policies. - Does not focus on the importance of the e-learning scope but mentions some studies related to online awareness tools providers.	- The main focus is on workplace training. - This study does not use phishing simulation to determine the pattern of employee phishing responses. - The occurrence of multicollinearity in the Structural Equation Modelling (SEM) regression analysis necessitates additional research to investigate mediated interactions between the independent variables.
Integrated	Protection motivation theory (PMT), Integrated Information Processing Model of Phishing Susceptibility (IIPM), and the Suspicion, Cognition, and Automaticity Model (SCAM).	Big-Five Personality Model.
Target	Workplaces	Workplaces
Type	Theoretical Framework	Theoretical Framework
Sources	[13]	[18]

Table 4 : The overall comparison between the components of phishing awareness related frameworks and models.

COMPONENTS	ISACM [5]	SAM [6]	PKPT [9]	SAMFP [12]	FPS [13]	ETPF [17]	PSF [18]	RAT [19]	TOTAL
Information Security Awareness and Capability (ISACM)		☒	☒	☑	☒	☒	☒	☒	**1**
Situation Awareness (SA)	☑	☑	☒	☑	☒	☒	☒	☒	**3**
Situation Awareness Model (SAM)	☒		☒	☑	☒	☒	☒	☒	**1**
Crime Triangle Framework (CTF)	☒	☒	☒	☒	☒	☒	☒	☑	**1**
Cyber Place Manager (CPM)	☒	☒	☒	☒	☒	☒	☒	☑	**1**
Inter-Loop Anti-Phishing Model (ILAPM)	☒	☒	☒	☒	☒	☒	☒	☑	**1**
Knowledge-Attitude-Behavior Model (KAB)	☒	☒	☒	☒	☒	☑	☒	☒	**1**
Big-Five Personality Model	☒	☒	☒	☒	☒	☒	☑	☒	**1**
Protection motivation theory (PMT)	☒	☒	☒	☒	☑	☒	☒	☒	**1**
Integrated Information Processing Model of Phishing Susceptibility (IIPM)	☒	☒	☒	☒	☑	☒	☒	☒	**1**
Suspicion, Cognition, and Automaticity Model (SCAM)	☒	☒	☒	☒	☑	☒	☒	☒	**1**
TOTAL	**1**	**1**	**0**	**3**	**3**	**1**	**1**	**3**	

4 Conclusions

Due to the obvious sensitivity and value of its data, the public sector is a prime target for attackers. To increase individuals' knowledge of phishing hazards, officials in the public sector have established a variety of frameworks, models, and technologies. However, these methods have not proved to be sufficiently successful in meeting the security requirements of institutions.

After reviewing the related models and frameworks, this study confirms the need to develop a new awareness and training model that can be used in the workplace and e-learning. The new model should enhance awareness through a dynamic training system without being exposed to direct or indirect risks concerning all the mentioned phishing attacking types by enhancing awareness. There is a necessity to improve the existing phishing awareness frameworks and models that can address the phishing attack at the workplace and at the same time be able to turn it into a cybersecurity training input, especially thru a digital learning platform.

As a result, a severe need to formulate a conceptual awareness model with all necessary factors and components to fit with the public sector needs in enhancing their employees' awareness of phishing attacks. Indeed, the review of the models and frameworks shows that there is a need to formulate a conceptual awareness model that can work in the workplace and e-learning with a practical awareness tool to avoid any lack of training regarding any future pandemic.

References

[1] S. M. Albladi and G. R. S. Weir, "Predicting individuals' vulnerability to social engineering in social networks," Cybersecurity., **3(1)**, 7, 2020.

[2] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," Futur. Internet.,**11(3)**, 73, 2019.

[3] I. Hamburg, “Opinions to Adapt Workplace Learning in the Time of Coronavirus and After,” Adv. Soc. Sci. Res. J., **8(3)**, 277–285, 2021.

[4] T. Daengsi, P. Wuttidittachotti, P. Pornpongtechavanich, and N. Utakrit, “A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization,” in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)., 102–106, 2021.

[5] R. Poepjes and M. Lane, “An information security awareness capability model (ISACM),” 2012.

[6] M. R. Endsley, “Situation awareness misconceptions and misunderstandings,” J. Cogn. Eng. Decis. Mak., **9 (1)**, 4–32, 2015.

[7] W. Hernández, Y. Levy, and M. M. Ramim, “An empirical assessment of employee cyberslacking in the public sector: The social engineering threat,” Online J. Appl. Knowl. Manag., **4(2)**, 93–109, 2016.

[8] R. Heartfield and G. Loukas, “A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks,” ACM Comput. Surv., **48 (3)**, 1–39, 2015.

[9] H. Heizmann and M. R. Olsson, “Power matters: the importance of Foucault’s power/knowledge as a conceptual lens in KM research and practice,” J. Knowl. Manag., 2015.

[10] S. Uebelacker and S. Quiel, “The social engineering personality framework,” in 2014 Workshop on Socio-Technical Aspects in Security and Trust., 24–30, 2014.

[11] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, “Panning for gold: Automatically analysing online social engineering attack surfaces,” Comput. Secur., **69**, 18–34, 2017.

[12] A. Shargawi, Understanding the Human Behavioural Factors behind Online Learners’ Susceptibility to Phishing Attacks. Lancaster University (United Kingdom)., 2017.

[13] E. J. Williams, J. Hinds, and A. N. Joinson, “Exploring susceptibility to phishing in the workplace,” Int. J. Hum. Comput. Stud., **120**, 1–13, 2018.

[14] R. W. Rogers, “A protection motivation theory of fear appeals and attitude change1,” J. Psychol., **91(1)**, 93–114, 1975.

[15] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, “Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model,” Decis. Support Syst., **51(3)**, 576–586, 2011.

[16] A. Vishwanath, B. Harrison, and Y. J. Ng, “Suspicion, cognition, and automaticity model of phishing susceptibility,” Communic. Res., **45(8)**, 1146–1166, 2018.

[17] M. S. bin Othman Mustafa, M. N. Kabir, F. Ernawan, and W. Jing, “An enhanced model for increasing awareness of vocational students against phishing attacks,” in 2019 IEEE international conference on automatic control and intelligent systems (I2CACIS).,10–14, 2019.

[18] S. Anawar, D. L. Kunasegaran, M. Z. Mas’ud, and N. A. Zakaria, “Analysis of phishing susceptibility in a workplace: a big-five personality perspectives,” J Eng Sci Technol., **14(5)**, 2865–2882, 2019.

[19] S. Back and R. T. Guerette, “Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks,” J. Contemp. Crim. Justice, **37(3)**, 427–451, 2021.

[20] D. K. King and J. Hayes, “The effects of power relationships: knowledge, practice and a new form of regulatory capture,” J. Risk Res., **21(9)**, 1104–1116, Sep. 2018.