Journal of Theoretical and Applied Information Technology
15th August 2020. Vol.98. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IDENTIFYING FACTORS THAT INFLUENCE SECURITY BEHAVIORS RELATING TO PHISHING ATTACKS SUSCEPTIBILITY: A SYSTEMATIC LITERATURE REVIEW

[1] AYMAN HASAN ASFOOR, [2] FIZA ABDUL RAHIM, [3]SALMAN YUSSOF

[1] Department of Management of Information Technology, Jubail Industrial College, Saudi Arabia
[2] College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia
[3] Institute of Informatics and Computation in Energy, Universiti Tenaga Nasional, Malaysia
*Corresponding author E-mail:asfour_a@jic.edu.sa

ABSTRACT

Over the past few years, the number of cybersecurity attacks related to phishing has been increasing, whereby users' private information is obtained via Internet banking in an unauthorized manner. This attack places considerable risks to government agencies, businesses as well as other users with sensitive data. In this paper, the published research of factors influencing security behavior associated with phishing attack susceptibility is explored. Four major databases, including journals and conference proceedings from Scopus and a total of 1560 studies were used in our review, and a quality criterion was applied to this set of papers. A total of 68 studies were selected for further analysis, from which 18 factors were successfully identified that are influenced (directly and indirectly) to security behavior relating to phishing attacks susceptibility. This review encompassed other aspects like the focus of the study, adopted theories addressing the factors of security behavior, and the research methodology. The findings indicated that the factors that influence security behavior associated to phishing susceptibility are attitude, self-efficacy, perceived behavioral control, subjective norms, digital guardianship, online target suitability, online exposure to motivated offenders, perceived susceptibility, perceived severity, perceived effective, perceived barriers, experience, knowledge, trust, computer skills and e-mail load.

Keywords: *Phishing Victimisation, Security Behaviours, Online Banking, Conceptual Model*

1. INTRODUCTION

Phishing is considered as an opportunistic attack that had targeted and destroyed the lives of many individuals. Concerning to the phishing attempt, the phenomenon can be perceived through the act of tricking to reveal sensitive or private information [1]. There is a constant increasing effort from attackers to develop complex malware to conduct their hacking activities [2]. In this aspect, the attacker creates a situation that makes the individual believe that their concerns have to do with authorized authority. The attacker then asks the victim for confidential information like financial and credit information [3].

A three-pronged approach can be used to combat this challenge; first, use a filtration system to mitigate the phishing e-mails that the user receives, and then decrease the phishing opportunities along with it. The second prong involves the use of an interface model to present phishing warnings and as such, prevents the users from visiting the site. The last prong entails the users' engagement in awareness and educative games or training, to practice methods of phishing prevention [4]. In the same line of study [5], phishing detection techniques can be classified as either user education or software-based anti-phishing techniques.

Current technology cannot protect end-users from cyberattacks [6], [7], as various cyberattack methods have been developed for preying end-users which are known as the weakest link in the information security domain. As the digital era matures, individuals are more exposed to cyberattacks [8]. It is also found that one of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

most practiced penetration attacks is a social approach rather than technical, to play a significant role in supporting the uttermost majority of cyber offensives [9].

The involvement of end-user (say clicking) is the pre-requisite of ensuring the success of phishing. However, users have intentions that sometimes contrast with their actual behaviors, and that the user responses on a particular stimulus may vary from one to another [10]. By recognizing the factors influencing these security behaviors, more effective solutions can be designed to protect end-users.

Security behaviors are significantly affected by factors related to the risk perception of an individual. These factors are dependent on the cultural and security environment of an organization, and they interconnect with one another, which could lead to behaviors that do not support information security [11]. Some other factors that are linked with human behavior include individual differences, cognitive abilities as well as personality traits, influence security behavior, and eventually information security effectiveness.

For instances, Sharp & Wu [12] have investigated factors such as behavior, perceived barriers to practice, self-efficacy, cues to action, prior security experience, perceived vulnerability, perceived benefits, and perceived severity. Hadlington [13] looked into factors such as trait impulsivity, Internet addiction, attitudes towards cybersecurity, and risky cybersecurity behaviors. Very recently, Whitty [14] highlighted factors such as age, gender, education, lack of premed, sensation seeking, locus of control, and addiction. Indeed, Albladi & George [15] studied factors such as competence, trust, motivation, past experience, conscientiousness, neuroticism, extraversion, agreeableness and openness to experience.

However, only few studies have been dedicated to the systematic identification, description, analysis and organization of the factors. Drawing on specific research questions, we will explore and discuss each identified factor that influences security behaviors relating to phishing attacks susceptibility.

2. BACKGROUND

Users operate technological and physical security measures towards information assets' protection. There is a consensus in the literature that user behavior poses significant risk while using those security measures. For example, a user might accidentally install a malicious embedded plugin to their web browser, which later exposes them to a phishing attack. Thus, it is important for the users to behave securely because this could leads to the successful protection of information assets [16], [17].

Attackers use various techniques to perform phishing attacks to gain confidential information from end-users in an unauthorized manner. These techniques include the use of inauthentic websites, anti-virus, ads, e-mails, scareware, websites on PayPal, awards and free offerings. Also, these techniques can be exemplified through e-mail from a bogus lottery department that presents money prizes, requesting private information and involving clicking on the attached links.

Requested Data could be details of credit cards, insurance, full name, address, pet name, first/dream job, maiden name, place of birth, places that the user has visited and other information. This information could be used to obtain or access personal and confidential online banking/services

Based on the above scenario, a different user might behave differently. This is due to the fact that each individual in this world is unique, with all individuals being characterized by different experiences, knowledge, interests, emotions, cognitive abilities, culture and personality traits that ultimately shape their behavior [18].

In this regard, women are more gullible compared to their male counterparts to phishing, and as well as individuals ages 18 to 25 [19]. In another study [20], women were evidenced to have weaker security behavior intentions when it comes to password generation, update, and awareness in comparison to males. Their finding also found that women often click on phishing links and have a higher tendency to provide information to unknown websites.

Due to the strong dependence of information security on the effective behavior of users who interact with these information assets and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information systems, organizations should focus more on the human aspects of information security. According to Taylor *et al.* [21] and Stanton *et al.* [22], the formation of the security-conscious workforce is good in ensuring effective information security. Hence, the central role played by the user in protecting information assets is the main concern in the current work

3. METHODOLOGY

This paper adopts the systematic literature review (SLR) method, with the search, involving four major online databases, which are, Science Direct, Emerald, IEEE Xplore, Taylor and Francis Online, as well as journals and conference articles indexed by Scopus. The keyword: - "phishing susceptibility" OR "phishing prevention" OR "phishing attack" AND "security behavior" OR "security behavior" and the whole keywords string was searched for the years from 2010 to 2019. The conducted search generated quite a number of studies that contributed to the selection of empirical studies to be reviewed.

The conditions for selecting studies to include for revision include; 1) behavioral studies that investigated and collected data on the subject, 2) studies that are dedicated to the factors of the topic under study, like a specific aspect contributing to the conceptualization of the susceptibility of phishing attacks and 3) English-written studies. In contrast, the conditions for not selecting studies for revision include; 1) studies that are not related to the susceptibility of phishing attacks, 2) studies that focus on the technical aspects, and 3) studies that are written in a language other than English. The search details based on the above set of inclusion conditions are detailed in **Table 1**.

The paper followed three main questions to guide the studies' review;

(1) What are the main factors of security behavior relating to phishing attacks susceptibility? How is security behavior relating to phishing attacks susceptibility investigated in the literature? When? Where? What sample and methodologies are adopted?
(2) Why is security behavior relating to phishing attacks susceptibility considered a relevant topic?
(3) What can literature contribute to recommending towards achieving the research agenda?

The above-formulated questions are aligned to the studies that embarked on providing a review of the literature [23].

Table 1- Selected Studies Related to the Criteria

Database	Total of research	No. of excluded studies	No. of selected studies
Emerald Insight	189	178	11
ScienceDirect	359	343	16
IEEE Xplore	85	81	4
Google Scholar	301	273	28
Taylor and Francis Online	142	137	5
arxiv	44	42	2
SpringerLink	440	438	2
Total	1560	1492	68

4. REVIEW ON RELATED FACTORS

The first addressed question of the literature review entails the establishment of the factors focused on by the scholars on examining security behavior relating to phishing attacks susceptibility. As evident in **Table 2 (Appendix A),** our review reveals that various theories, frameworks are contributed to the variances in security behavior studies relating to phishing attacks susceptibility.

The theories and frameworks are adopted and adapted in the selected studies by focusing on certain factors. Various factors were assessed by using various methodological approach methods on the identified respondents

Most previous studies focused on the Protection Motivation Theory (23 studies), Big-Five Framework (12 studies), Theory of Planned Behavior (11 studies) and Routine Activity Theory (8 studies), as tabulated in **Table 3**.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3-Classical theories synthesized in the literature

No.	Theories	No. of studies
1	Protection Motivation Theory (PMT)	23
2	Big-Five Model (BFM)	12
4	Theory of Planned Behavior (TPB)	11
3	Routine Activity Theory (RAT)	8
6	Theory of Deception (TD)	7
5	Health Belief Model (HBM)	6
10	Technology Acceptance Model (TAM)	5
7	Heuristic Systematic Model (HSM)	3
8	Elaboration Likelihood Model (ELM)	3
9	Interpersonal Deception Theory (IDT)	3
11	Theory of Reasoned Action (TRA)	2
16	Extended Parallel Processing Model (EPPM)	2
12	General Theory of Crime &Victimization (GTGV)	1
13	Integrated information processing model of phishing susceptibility (IPMPS)	1
14	Rational Choice Theory (RCT)	1
15	Suspicion, Cognition, and Automaticity (SCA)	1

In **Table 4 (Appendix B)**, the ranking of factors and descriptions of relevant studies are presented. Of the total reviewed studies, 50% of the studies focused on factors such as perceived susceptibility/perceived vulnerability, perceived severity and perceived effectiveness and experience. It was also found that 44% of the studies examining factors in Big Five Model, self-efficacy and awareness. While, 38% of studies focused on attitude and 33% of the studies concentrated on perceived behavioral control, subjective norms, online guardianship, online target suitability, online exposure to motivate offenders and perceived barriers. However, only 0.6% of the studies focused on trust and computer skills and 0.4% of the studies discussed e-mail load.

Figure 1 showed that the number of studies on phishing attacks susceptibility per country. With 15 unique countries presented by 68 studies, the geography of studies indicated significant diversity. The most published paper was the United States location of 25 studies.

As for multi-country studies, Australia and New Zealand, the United States and Australia were focused on one study each. Based on the respondents, 35 studies were focused on students, 15 studies on employees, 6 studies on online banking customers, and other studies focused on the general public. In particular, a huge portion of work was dedicated to universities in assessing the information security management system effectiveness that used throughout the universities. Such works depended on students' contributions towards understanding the motivations behind their risky cyber-behaviors.

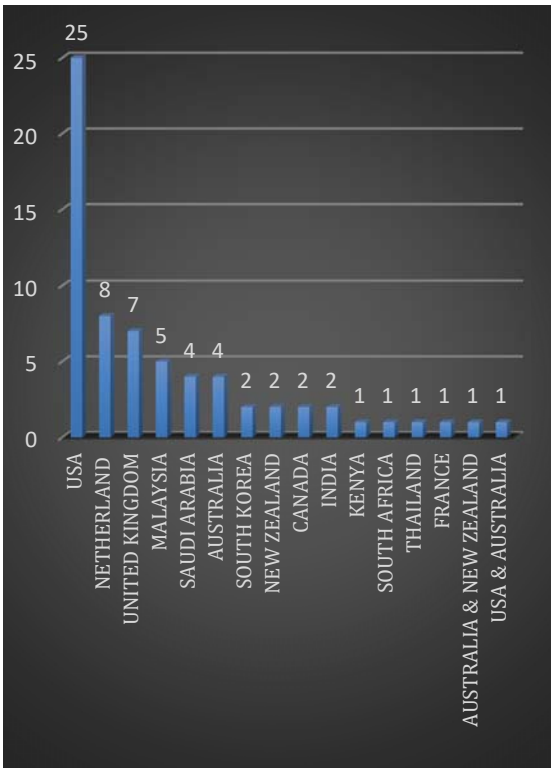

Figure 1 Number of studies per country

With regards to the research methodology adopted in the studies, phishing attacks susceptibility studies were mainly performed via disseminating survey questionnaires and conducting experimental design with a total of 68 studies, as illustrated in **Figure 2**. The experimental approach (phishing simulation) was reported in 11 studies to demonstrate the phenomena such as information security challenges among universities, user perceptions on safe online behaviors and implementation of information security guidelines. Secondary data was reported in 3 studies. Both interviews and mixed methods were used in assessing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

hypotheses, as reported in 4 studies. Survey and phishing simulations were reported in 6 studies.

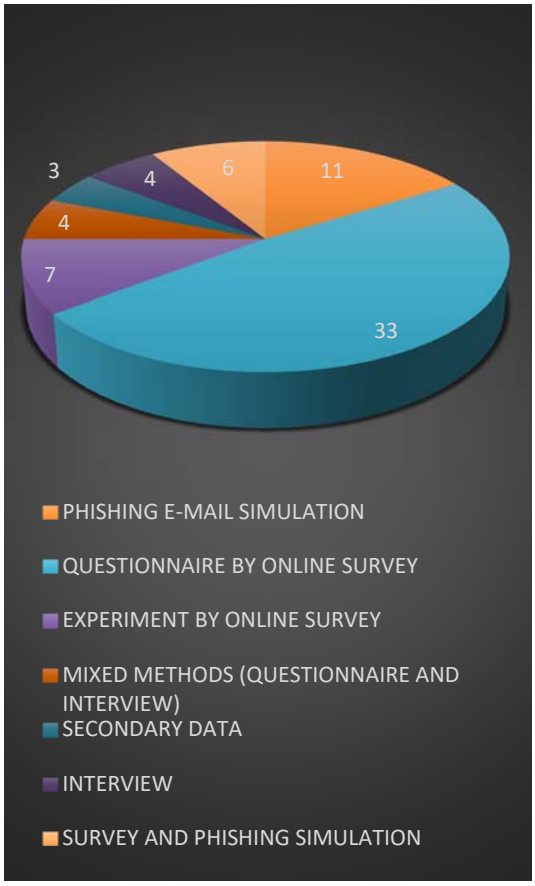

Figure 2 Research Methodologies Adopted in the Studies

Among the well-known quantitative data analysis method, involving the survey studies is Partial Least Squares (PLS), with 27 studies, which can be used in numerous software packages like SmartPLS, SAS, SPSS, and others. PLS analysis was used to examine the relationship between end-users' behaviors and their potential intention/action towards security. In this regard, behavioral models address several interaction effects between formal latent variables and PLS is more suitable to be used to examine the latent variables of relationships and multiple constructs.

5. RELATED ISSUES OF SECURITY BEHAVIORS

The second research question aimed at understanding why security behavior relating to phishing attacks susceptibility is considered a relevant topic. From the selected studies, we found 7 different topics as follows:

(i) Individual Differences
(ii) Demographic Characteristics
(iii) Personality Traits
(iv) Human Behavior
(v) Lifestyle
(vi) Experiential Factors
  a) General Experience
  b) Technological Experience
  c) Professional Experience
(vii) Attacker's Skills in E-mail Contextualization

5.1 Individual Differences

Individual differences are more-or-less the enduring psychological characteristics that distinguish one person from another and thus help to define each person's individuality and IT refers to the extent and type of distinctions among individuals on some of the significant psychological traits, personal characteristics, cognitive and emotional components. Also, it creates differences among people as a result of their behaviors, attitudes, as well it Stand for different variables ranging from gender and educational background to perceptions and proficiency levels that leave an explicit or implicit impact on an individual's behavior.

Individual differences result in varying possibilities of someone to fall victim to phishing threats based on behavioral characteristics, demographic individuality, personality traits, [86],[87],[88]. Author [52] in-depth researched on individual differences in the sense of the vulnerability towards phishing, attitude towards trust and distrust, curiosity, the need of entertainment, the possibility of boredom, shortness of attention span, risk propensity, the amount of Internet usage, attachment to the Internet, and Internet anxiety which are behavior linked to vulnerability and some of these traits were discovered to be positive indicators of vulnerability towards phishing. In the findings, it was found that trust is the most notable trait followed by curiosity, boredom, and risk propensity.

Individual differences were also studied in terms of the effect of national culture on phishing responses and spear-phishing e-mails [46]. The study examined individual differences, including personality traits, information security awareness,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

gender, cognitive impulsivity, and national culture. Research has concluded that the strongest predictor of a learners' capacity to sense these suspicious e-mails was the cultural orientation towards the person's individual needs compared to the society's needs. Based on the obtained results, national culture variables significantly predicted phishing responses.

In a related study [46], culture was also reported to predict the attitude of privacy significantly, but this did not hold the same for security-related behavior and self-efficacy. Also, while online behaviors varied, others including demographics, personality traits and education were significant predictors of effective security and self-efficacy. In their studies, they found that gender has a significant influence on self-efficacy, with the highest difference being documented in the US. However, it had no significant effect on the respondents' security-related behaviors. Based on finding individuals having low cognitive impulsivity and high agreeableness levels were related to the better discerning of phishing emails

Based on the study [20] findings, individual differences explained 5-23% of the variance in the intentions of cyber security behavior. Several characteristics, with the inclusion of financial risk-taking, rational decision-making, extraversion and gender, had a significant distinct role in predicting effective security behaviors. The phishing email is one of the major dangers, to online information security due to its ability to achieve human trust and credulity.

Some people are more susceptible to phishing than others and what characteristics may predict this susceptibility. Such as one of the Big five personality factors, openness, correlated positively with accuracy in detecting phishing e-mail. Despite robust relationships between some variables and phishing susceptibility gender, trust and attention are required to phishing stimuli.

5.2 Demographic Characteristics

The term demographics refers to particular characteristics of a population. The sample is presented in terms of age, gender, ethnicity, number of children, educational attainment, source of income, and socio-economic status. The major purpose of this material is to provide a general social profile of the sample from which the responses were drawn [89].

A significant relationship is discovered between demographic factors and phishing attack susceptibility among students in [27]. The authors found that lower susceptibility was influenced by college affiliation, a progression of the academic year, cyber training, cyber clubs' involvement, a period spent on the computer, and age. However, higher susceptibility was found for phishing awareness, but no significant relationship was found for gender. User susceptibility to phishing remains an issue even when the students are tech-savvy, with 59% of the subjects noted to open a phishing e-mail, and 70% of them answering the clicked on the demographic questionnaire.

A study conducted by [19] involving demographic characteristics (i.e., gender, age and education level) in relation to phishing susceptibility and the authors found female respondents to have higher susceptibility towards phishing in comparison to male respondents, with the age group that was the most susceptible was 18-25-year-old.

Studies in the same line [90] discovered that female user to be more susceptible to entertaining phishing messages compared to their male counterparts, but the former was not necessarily inclined towards clicking malicious links, which made the authors reached to the conclusion that female users are more adventurous in exploring phishing e-mails.

In another study [28], the focus was placed on demographic characteristics (i.e.: age and educational level) and the impacts of cyber security perceptions and behaviors of students in tertiary schools. The study contributes to practice by highlighting the need for more cyber security training and initiatives for different students' groups in schools. The effects and impacts of other factors on cyber security behaviors need to be further examined in this context, with some factors potential integration (e.g., cultural background, academic performance, health habits). They reported that age, gender and education level all had a mediating effect on the relationship between cyber security behaviors among tertiary institution students, with age and gender found to be top factors in attracting higher effects with good statistical significance compared to the level of education,

A lot of cybersecurity breaches occur due to human errors. Institutions need to enhance

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

students 'cybersecurity awareness and capabilities, hence promoting safe cybersecurity behaviors and age, gender, and educational level has an impact on the cybersecurity behavior and beliefs of tertiary institution students

5.3 Personality Traits

Personality traits refer to Big Five personality model according to this model, personality can be broadly classified into five factors [91] (1) extraversion, which describes a person who is more interactive with others (2) agreeableness, which describes a person who is more kind and warm to others (3) consciousness, which describes a person who is more determined.

This model emerged from applying the principles of the psychological approach to personality [91]. It provides an overview of the cognitive level of the individual and offers a way of understanding how a person can respond. The end-user is often the weakest link, and so they are easily the victims of a phishing attack [92].

Studies in personality traits are worth searching, considering that individual and environmental features are significant factors able to motivate persons to fall prey to cybercrime [93] for example, research has shown how personal traits, like neuroticism and openness, can participate to online vulnerability and why particular people are more probable to answer phishing emails or post more information on social media.

However, we must look at the significance of other psychological factors with each other's with personality traits in order to explain human vulnerability to fraud, situational and contextual factors can change the efficiency of phishing efforts [48]

Individuals who are curious and creative have a high in openness to experience; these individuals are curious and like to explore sites and are more likely to try all social media activities when they are online. Moreover, Individuals are trusting, amenable, and giving have scored high on agreeableness[94], found individuals scoring high in agreeableness and conscientiousness are prone to more secure behavior online and are not more susceptible to phishing attacks

In a study [83], the focus of the authors was directed towards proposing a conceptual framework, employing the Big-Five personality traits to provide insight into the reasons behind some people's susceptibility to top phishing attacks compared to others.

The findings indicated that the Big-Five personality traits were invaluable as predictors of human behavior. They found that individuals with different personality traits tended to be more susceptible to different phishing types and that phishing is an issue for individuals and organizations. Female users were more likely to be susceptible compared to male users.

Also, a similar study [24] focused on examining personality traits driving the response decision of employees towards phishing attacks. Based on the findings, employees' technical and general experience was significant in forming their personality towards preventing vulnerability towards phishing attacks.

The correlation analysis results also revealed that conscientiousness and self-monitoring positively related with the security behavior of employees, employees' technical and general experience was significant in forming their personality towards preventing vulnerability towards phishing attacks. The correlation analysis results also revealed that conscientiousness and self-monitoring positively related with the security behavior of employees.

Related studies like those of [54] and [15] addressed the Big-Five model in cyber-crime. The former examined the relationship between cybercrime victimization and the Big-Five personality model's major traits. Their findings revealed that individuals had a low risk of being cybercrime victims and that their emotional stability indicated the lower likelihood to be victims. Meanwhile, in [15] a more recent study, the authors focused on the Big-Five model's explanation of the users' susceptibility towards cyber-attack victimization, using mediating factors. The study suggested that people's different behaviors based on stimuli, call for examining human behavior.

The significance has been evidenced by [90] that employed a five-factor personality model in their attempt to identify the personality-phishing vulnerability relationship. The five-factor used behavioral traits were neuroticism, extroversion, openness, agreeableness, and conscientiousness.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It is important to note that each of the five personality factors represents a range between two extremes. For example, extraversion represents a continuum between extreme extraversion and extreme introversion. In the real world, most people lie somewhere in between the two polar ends of each dimension. The effect of personality traits on the user's online risky behavior is still a controversial topic in cyber security research. Therefore, the present studies proposed a mediation model that includes the five personality traits and the four mediators that together affect the user's likelihood of falling victim to cyber-attacks.

5.4 Human Behavior

Human behavior is the potential or the actual capacity to carry out human life activities (physical, mental and social), consisting of individuals with a combination of various personalities, values, perceptions, attitudes, aspirations, motives and abilities. It stems from the individual characteristics and environmental characteristics interaction. Every individual has a distinct combination of characteristics, with some originating from birth, and others developed throughout the lifetime [95].

Human behavior is exploited by cyber criminals to convince the users to click on links to malicious websites and attachments, relying on common traits that ensure the requested response. Users' greed is exploited by the criminals to former to click on a link – this is the case with money-making schemes, hot stock tips and the like that attracts people and convinces them to click on the link out of curiosity. Email spammers and scammers have also employed major news events, conspiracy theories, celebrity news and information on national disasters to convince users to expose themselves to malware sites or to click on an attachment to an email [96].

The general and widely established belief is that cyber security systems built on robust theoretical evidences frequently fall short in practical performance, with a majority of authors considering the individual users as the system's weakest link [97]. Despite the fact that cyber-security has arisen as a critical issue in the face of assumption of human behavior and the resulting vulnerability, human behavior and its relation to the machines' vulnerability has been a topic under-examined in major operational environments.

In the context of general crimes, such as mugging, a victim is frequently chosen by the mugger based on behavior/characteristics, in that the victim may be walking late at night, elderly, infirm, or have other physical weaknesses. Similarly, the potential and intensity of the attack of malware on the machine have been surmised to be significantly linked to the machine behavior [98], with the premise that only amateurs attack machines, while professionals attack people. The measurement of the behaviors that have the potential to attract cyber-attacks is thus crucial to cope with such attacks, growth and diversity.

It is easy for a human to fall prey to social engineering attacks, requesting them to go to websites or to download files, culminating in the malware introduction. In some cases, they may visit a bogus website that carries out drive-by download attacks [99], and prey on the browser's vulnerabilities, as a result of which, silent file downloads are caused. On the whole, users are generally inclined to download foreign applications and binaries or conduct activities undermining security.

In a similar study [30] it was explained that phishing attacks threaten the security of home users and organizations alike, using social engineering to acquire private information after which targets are chosen to take action by clicking on the link and divulging their information.

However, the level to which human behavior is linked to the host propensity to be the cyber-attacks target has not been clarified. Current works focusing on carrying out designed experiments to shed light on the human behavior-susceptibility to attacks relationship stand out (e.g., [100], [101], [19]) although they are generally conducted in a lab setting using small-sized samples. This may be exemplified by [100] study that involved 215 subjects whose reactions were obtained towards emails that are threatening. Moreover, [101] examined the cyber-security procedures and compliance with such procedures by using the Theory of Planned Behavior (TPB) and the Protection Motivation Theory (PMT).

Furthermore, [100] it was investigated if fear-based manipulation of users through phishing messages threatening the user imprisonment and the like is related to the threat severity, threat susceptibility, self-efficacy and response efficacy perceptions. In the same line of study, it [101]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

involved 215 users, and the author aimed to study compliance with cyber security procedures through the combination of two theories in the field of psychology and they are the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT).

As in [37], the study found that the cognitive process of PMT (threat and coping appraisal), significantly influences human behavior towards adopting precautionary measures. Their findings also showed that the precautionary online behavior of customers ensures a safer online-banking experience and this can be further improved through the use of factors and their integration into security education and initiatives of awareness.

For protecting a human behavior from phishing attacks, a study [36] was adopted by PMT to evaluate the context of fear appeal interventions in reducing the vulnerability of phishing attacks. The study found that self-efficacy and fear were the most important factors that may lead to protection motivation. The study also highlighted the importance of online information-sharing behaviors that must be addressed in developing preventive measures that helps decrease the possibility of phishing attacks.

A research model was developed that is based on TRA disciplines, moral obligation, PMT and organizational context factors to explain the protection of human behavior work (Yoon & Kim, 2013). The findings of the study showed that moral obligation and attitude toward security behavior are the key predictors of employee intentions to practice security behavior.

The importance of security behaviors was highlighted in light of self-efficacy, perceived personal susceptibility to digital threat, guardianship as well as conformity. The results showed that cyber security behaviors were defined by: self-efficacy, perceived personal susceptibility to digital threat, guardianship and conformity [33].

Phishing attacks depend on a combination of Human behavior factors to impact users. Cognitive biases and heuristics can impact how persons perceive risk, for example, individuals may be overconfident, believing that they will not be the target of a cyber-attack (i.e., optimism bias), decreasing the probability that a person will request extra information to locate the legitimacy of the request (e.g., checking the email address, calling the sender)

5.5 Lifestyle and Routine Activity

In the second approach, it concentrated in Lifestyle and routine activity that refers to the habits, attitudes, tastes, moral standards, economic level, etc., that together constitute the mode of living of an individual or group, that stated that no similarity for every person and those different lifestyles impose more threats compared to some other lifestyles [39].

The increase in cybercrime victims can be explained by changes in people's routine activities in daily life [102]. With the advent of the Internet, the way people communicate or interact with others has changed in personal relationships, entertainment, commerce, etc.

Changes in people's routine activities such as the use of the internet and social interaction networks such as Facebook, email, websites, and others have created opportunities for motivated offenders with valuable and easy targets in space. For example, it can be risky when opening emails from anonymous clients through doing an online business transaction, as some of those files could include suspicious software and you will fall prey when opening them.

Cohen and Felson believe that a crime is likely to occur when three factors are met, the motivated offender, the appropriate target, and the absence of guardianship that these three factors are required in order for the crime to occur, and the absence of one of these factors is sufficient to prevent the occurrence of the crime. A motivated guilty can be pointed out as any type of individual who has the real intention to commit an offense against a person or ownership such If a target is suitable, this means that there is a major opportunity that the offense can be committed, rather than, a target that is hard to achieve.

The exposure to a motivated offender can be through time spends via online activities. Time spent on downloading software as well as other multimedia; time spent chatting. Remember that when an individual visit online via banking, they

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

might interact with a pool of offenders without their consent. Suitable targets can be a person or object that is seen by offenders as vulnerable or in particular attractive such individual whether they can offer a chance for a motivated offender.

The act of providing an actual truth in an online status such as giving your bank details as well as all your documents is a factor which can make an individual suitable. Guardianship can be an object or person that is effective to stop crime to occur and occasionally the crime is prevented by the simple existence of guardianship in space and time, such as anti-virus software, antispyware and firewall The three major issues in literature when it comes to the operationalization and testing of an extensive routine activity framework on neglected victimization forms are addressed by lifestyle and routine activity.

In particular, lifestyle and routine activity are used to examine the effects of online exposure, online target suitability and online guardianship on phishing, hacking and malware infection. Additionally, they were also used to identify victimization predictors although distinct victimization types enable the carrying out of a comparison of respective opportunity structures. Users are exposed to different circumstances based on their lifestyles and sometimes, attacks are able to lure users into exposing themselves to significant crime-prone risk situations, leaving them completely vulnerable to attacks [103].

For instance, individuals who have the habit of using Facebook have a higher likelihood to fall for bogus profiles created by phishers to lure them and provide their sensitive information [104]

In a similar study [62], it explored the relationship between user behavior on social networks and online victimization risks. They specifically focused on behaviors on social media, its use and the attitudes of users (their controllability of information, technical efficacy, risk perceptions and risk propensity) and their relationship with cybercrime victimization. Based on the findings, a negative and significant relationship was found between multi-purpose dominant SNS (social network sites) such as (Facebook, Google+) use and victimization. On the contrary, SNS knowledge exchange activities, through LinkedIn and Blogger had a positive and significant relationship with the same. The findings have several practical implications for the social media industry in light of protecting information security on SNS. In other words, online habits do have a hand in affecting the susceptibility of the user to be a phishing victim on social media, convincing them to follow their social media routine use, involving little or no cognitive engagement. This leads to the maximized likelihood that the users will eventually click on the bogus phishing links or to accept request from bogus friends without thinking about the outcome of their action [104]

In addition, [39] it provided an insight into the individual in becoming phishing victims, with the help of integrative lifestyle and routine activity. The authors focused their examination on the risky online daily activities' effects, which exposes the user to the attacker. So risky online activities raise the probability that internet users come across phishers. More specifically, the relations between becoming a phishing goal and four types of online exposure, namely digital copying behavior, risky online self-disclosure, SNS use and online purchasing behavior.

Furthermore, online exposure of users was found to increase their risks towards online phishing, hacking and malware infection by [69]. The study further examined if online guardianship minimized the level of victimization. The author illustrated those habitual buyers online, social networks active engagers and information posters had a higher likelihood to be victimized. It was also indicated that online guardianship had a positive effect but was opposite to what was premised, where installed anti-virus software installing users were more susceptible to becoming victims of phishing.

Installing anti-virus software was related to the temporal ordering issue, where the sample installed software based on their phishing experience. Since the results reached were inconclusive, more studies are required to examine the online behaviors victimization relationship. In [14], the current study, the author urged future researchers to focus on the online activities-cyber fraud relationship. So, psychological and socio-demographic characteristics of the individuals and their online behaviors that drive them to become victims of cyber-fraud

Finally, [25] revealed that although online victimization has grown and permeated

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

throughout the online world, theoretical examinations that account for the behaviors are sadly lacking along with empirical studies that can offer potential explanations for the way online lifestyles and cybersecurity management affect victimization online compared to traditional bullying. So, individuals that participate in risky online leisure activities, lifestyle activities, and risky social networking activities were more likely to be more victim than who do not participate.

5.6 Experiential Factors

While, the third approach concentrated is experiential factors [84], [105] these are likely to be influencing a user's vulnerability to phishing and online deception like CSE (computer self-efficacy), the familiarity of the Web, and security awareness, which is inclined to get better with time within users. Therefore, superiors should be given the means to focus on these experiential factors and strengthen better security. General experiences, technological experiences, and professional experiences are three main aspects of experiential factors.

Experiential factors are regarding the individual's familiarity and skill of computers and awareness of the false activity. Studies on the topic of phishing attacks susceptibility were mostly limited to the examination of the knowledge and familiarity of the end-users in the Internet scam, as a strategy to avoid being victimized. For instance, [84] findings showed that individuals that had high self-efficaciousness in computer, web, security knowledge were more protected against phishing attacks although the use of the internet by itself, is not sole protection.

Thus, [52] it explained that the Internet experience has the potential to be a viable proxy for individual expertise and Internet experience, assuming that this experience will prevent an individual from being subjected to phishing attacks. Another study [67] revealed that a person's processing styles were also evidence of the probability of fraud responding. However, this connection was influenced considerably by personal factors associated with e-mail familiarity and skill. So, to explore individual susceptibility to phishing by conducting the techniques that may impact a person's victimization. The concentration is on the features of the e-mail message, individuals' knowledge and experience with phishing, and the style in which these react and impact how users cognitively process phishing e-mails.

Besides, peer behavior and employees' action experience of cybersecurity issues were found to be important drivers for enhancing security behavior among firms [51]. A positive relationship was discovered between on cue to action towards employees' action experience, which in turn affect their threat perceptions and response perceptions. Consequently, threat perception and response perception of employees positively influence their overall security behavior. So, there is an impact from peer behavior and employees' action experience of cybersecurity is a significant factor for improving cybersecurity behavior in organizations. Peer behavior positively impacts due to action, which positively affects employees' action experience. Work experience of employees has positively affected their perception of threat and response together.

As an outcome, employees' threat perceptions and response perception are positively concerning to their cyber security behavior. This process is a chain reaction.

Additionally, life experiences may sometimes lead to personality changes like being more responsible on the job in terms of conscientiousness to meet deadlines [83]. Majority of experiences are influenced by age in that individuals in early adulthood, entering the workforce or going through the career ladder, those starting families, and those looking at retirement face different from novel experiences.

5.6.1 General Experiences

General experiences are practices not connected to a person's experience with technology or their career. These encounters could be constructive, which is an aspect that has been revealed to encourage agreeableness. In contrast, there could be negative experiences like being a wronged by a scam or in the midst of financial difficulties.

However, there is a lack of empirical evidence at present to connect these negative encounters directly. Based on [83] showed prior victimization to scam attacks does reduce certain sides of an individual's vulnerability to susceptibility to thereafter falling prey when tested, through the lens of consumer behavior. This suggested that negative experiences may

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

have a negative effect on agreeableness as well as on phishing susceptibility.

Experience is one source of intrapersonal information which impact personals' threat and coping appraisal and their intent. It can be both passive and positive and can potentially impact security behavior in various ways. Passive experiences such as a malware infection or having your personal account (such as Facebook).

5.6.2 Technological Experience

Technological experience refers to the extent of a user's self-reported experience using technology, learner perceptions and the use of ICT that includes previous technological application as well as education in the suitable utilization of technology. Training is a crucial countermeasure against social engineering and phishing attacks and, would be hoped to negatively connect with phishing vulnerability.

In terms of experiential influence on personality, a person with comprehensive training is more likely to be more cautious of received e-mails leading to having a negative influence on the agreeableness of the person in the computing situation, or the sense of paranoia about e-mail could be seen thus enabling a constructive consequence on neuroticism. Neuroticism might also influence the technological skill of a person due to its connection with computer anxiety. Based on [83], the result shows that with computer anxiety may not have the same types of experiences with technology that persons with less anxiety may have. Openness also has impacts on technological experience in that it has been correlated with the optimum stimulation level (OSD) of individuals.

5.6.3 Professional Experience

Professional experience means the experience occurred through full-time employment in an education-related field or in a field in which the person intends to be licensed. It includes incidents that are related to the person's career, professional or study. A differentiation between professional and academic practices have been revealed to be associated with phishing vulnerability. Professionally, this can be seen is researches that show learners who have a full-time job were less liable to phishing compared to their peers.

From the academic perspective, researches inclined that several academic fields are more vulnerable to phishing compared to others. Based on the study [83] that mentioned the effect of professional experience could be seen in its effects on, and how it is influenced by, conscientiousness. The relevance could be posited as a transactional one where a person's level of conscientiousness brings about them to demand (or avoid) professional experiences that reinforce (or break down) that same person's level of conscientiousness

individuals who own practical experience has a low susceptible to phishing comparing with counterparts who not have

5.7 Attacker's Skills in E-mail Contextualization

In the fourth approach, it is attacker's skills in contextualizing referred to modifying their framing and content, and the ability of the attacker to contextualize e-mail where e-mails are formed in a way that the victims are convinced of their authenticity based on the information content [106] and that is done by e-mail sent to an individual that is ostensibly from the bank s/he uses leverages fear by suggesting that the recipient will not be able to access her/his bank account unless s/he changes their banking credentials or information by clicking on a given web link. Besides fear, a variety of different emotions regarding psychological traits, for example, curiosity, patriotism, friendship, authority, community and belongingness could be influenced by phishing attacks.

Contextualizing messages are the phishing emails connected to familiar topics such as sporting events, and cultural festivals that individuals are more likely to be acquainted with, and this may increase the perceived trustworthiness of the emails. In this style, the exposure to contextual evidence may create phishing attacks more attracting attention, and throughout the entire event, successfully prepare users for later phishing emails that connect to the current information

Therefore, contextualizing messages increases the effectiveness of phishing [48]. The effectiveness of phishing messages that a produced to target a specific group of users will be seen if individuals recognize the group-relevant worry and provoke particular feelings that activate the wanted outcome and a carefully designed phishing e-mail can trigger basic emotions that persuade individuals to agree with the hidden malicious request. For example, individuals may divulge

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

their credentials to hackers if they fear losing something valuable.

Thus, a contextualised phishing e-mail sent to an individual that is ostensibly from the bank s/he uses leverages fear by suggesting that the recipient will not be able to access her/his bank account unless s/he changes their banking credentials or information by clicking on a given Weblink [107].

In e-mail contextualization, attackers indulge in URL spoofing primarily to obscure their identity and to explore the people's confidence in the websites, while the sender's actual source address remains hidden. As a consequence, [108] explained that users might find it challenging to discern between an authentic URL from one that is fake when under spear-phishing attack as they have a tendency to just take a glance at the URL, presuming its legitimacy. So, that a carefully designed phishing e-mail can trigger basic emotions that persuade individuals to comply with the disguised malicious request, for example, individuals may divulge their credentials to hackers if they fear losing something valuable.

Also, in e-mail contextualization that contains specific concerns, attackers may link the context of hunting e-mail messages to a familiar topic, individuals are likely to be aware of, and this may enhance the trustworthiness of e-mail messages. In this way, exposure to contextual content may make phishing attacks more striking, and throughout the entire event, successfully preparing for subsequent e-mail contextualization linking the current information [109].

Email contextualization acts like pretexting in social engineering attacks. In pretexting, one fakes a scenario and mixes something of certain relevance or significance to the recipient in the scenario, which acts to legitimize the interaction and can encourage, the recipient to reveal information. One can also see email contextualization as a form of spear-phishing, where the hackers target particular persons with personalized messages, usually spear-phishing prey receives an email that shows to be from somebody they know, which raises their confidence in the message.

In the study [34], the author highlighted the effectiveness of phishing through e-mails that have more contextual elements than that may be of concern to the target.
Studies who dedicated their work to the topic of physical attributes of messages include [76], who used experimental designs in the form of fake phishing e-mails among university staff and students from information services requesting accounts verification. Based on the obtained findings, high source credible messages with touting convincing arguments were effective the context of spear-phishing attacks, and [80] showed that time-limited messages had a higher likelihood to be replied to in comparison to the less-urgent ones. This means that the visual cues processing and indicators detection of phishing messages and the decision-making process of the users are all pertinent. The findings showed that visceral triggers and phishing detection indicators, as well as the user's phishing knowledge, are all predictors of phishing attacks detection.

Generally, there is a threat element in the message of arousal of fear that could lead to enhanced acceptance and conviction of the message via a specific effect on information processing [58]. In this regard, fear-arousing content in e-mail contextualization may influence the processing of users of the e-email, improving the tendency of overlooking the fraudulent signals in the message.

6. RECOMMENDATIONS FOR FUTURE RESEARCH

The third research question synthesized recommendations for further research in the field of phishing attacks susceptibility. The suggestions in [32] emphasize future studies to find other ways to maximize interactions with phishing stimuli and the targeted users' participation. In addition, the analysis and results of the model could differ if the data is obtained from a larger pool of participants, the authors also recommended determining whether those who did not interact with phishing e-mail had valid reasons to believe that it was a phishing attack.

In SEM regression analysis, the presence of multicollinearity calls for more analysis to examine the mediating relationships between the variables [44]. Similar to [26], the study also indicated that further studies are needed to examine the personality traits for a better understanding of the construct's relationships via mediating variables. For instance, in order to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

improve the generalizability of research findings, an investigation of neuroticism and self-efficacy in information security and security behavior intention can be conducted among post-college students or working professionals.

Future studies may also reap new information by comparing the results of self-reported behavior and behavioral intention or likelihood of such behavior. For example, an analysis could be conducted to evaluate the moderating role of security policy awareness level, demographic characteristics, as well as other potential factors using other statistical analysis tools or research on the reasons behind the moderating influence of gender and the effect of using various empirical analysis tests [51].

In [14], the study supports socio-demographics, psychological characteristics and routine activities as factors that may predict a person to be a victim of phishing. Hence, future studies are recommended to examine routine activities in detail and to investigate different ways in which individuals can identify authentic content from disingenuous scammer content on the outcome variables.

Moreover, [25] highlighted that future studies might examine time-specific (time-concurrent and time-lagged) and neighborhood-level social contextual factors' effects on the outcome variables. In addition, future studies may integrate criminological and opportunity theories, explaining offending and victimization behaviors to guide their theoretical frameworks. Besides, future studies can use a holistic list of items and measurements to steer clear of internal validity issues. Another recommendation by Williams [41] related to the importance of exploring the potential role of other techniques and message-related factors (time of day the e-mail is received) and their impact on employee susceptibility in the workplace

Research by Leest [38] emphasized on the phishing awareness in the long-run. Also, he suggested that future studies can also examine the significant effect of status and overconfidence on the core judgment of bank e-mails, using a larger number of participants.

Thomas [40] recommended employing a quantitative approach to future studies. Such an approach may be used to explore the themes highlighted in the study to provide insight into their effects on the user's preparation against spear-phishing relating with a majority of reviewed studies in this paper that used the quantitative approach as the main methodology.

Meanwhile, [39] suggested examining more extensive potential risky online activities like hacking, online banking, and online gambling. As the study did not consider online skills of users like digital literacy, future studies can include it along with other online behaviors (e.g., e-mail use frequency), other online protective behaviors (e.g., privacy settings on SNS, using anti-virus software) as well as dispositional factors (e.g., morality). Since the people who fall victim to phishers are more likely, but not necessarily, the same individual who gets targeted, the idea of future study to look at both phishing targeting and victimization into account is intriguing.

Reyns [69] conducted a study and suggested explaining phishing and online victimization further to enhance the comprehension of the audiences' capabilities, and further examination of the way habits and heuristic processing co-exist.

In the other study [88], the researchers highlighted the need for studies concerning the individual differences and their influence on online scams susceptibility, still lack investigating how individual characteristics (demographic individuality, personality traits) influence susceptibility to phishing using the internet.

Studies based on individual differences are still limited, challenges in accessing hard-to-reach locations and little experiments conducted in this context. The future study should also extend on the present body of literature by studying variables that are not or seldom investigated in regards to phishing (i.e. intelligence, confidence, experience and honesty/propriety) with the connection of variables normally researched (e.g., knowledge of computers and phishing, age, gender, five personality factors).

Variables such as intelligence, confidence, and honesty or decency may have often-overlooked, which possibly having important implications in producing a countermeasure to enhance efficient detection of a phishing e-mail.

Also, future studies are recommended by Moody et al. [52] to measure and control personality traits when it comes to phishing susceptibility. They

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

also suggested keeping into consideration the way the context of the message may relate to individual differences and constitute personality traits that may influence the persuasive power of the message and further added that personality traits should be measured and controlled for in future studies on phishing susceptibility.

Future studies may also focus on presenting design interventions based on the personality traits and risk perceptions of users, and determine how they can assist in maximizing secured online behavior among users [110].

The study urged further studies to examine trust as a part of the nomological network of behavioral information security, with the inclusion of its association with protection motivation. Other recommend for mediating factors effects (e.g., delinquent friends and online behavior) on the relationship between personality traits and cybercrime victimization. (e.g., delinquent friends and online behavior) investigate variables along with other personality traits that have been evidenced to be predictors of SNS(Social Networking Sites) behavior (e.g., narcissism, self-esteem, public self-consciousness, and need to be popular).

Moreover, there are suggestions from [61] relate to the predictor variables such as personality factors from the Big Five Model in a quantitative study (e.g., personality factors from the Big-Five Model). It is also suggested to explore the usage of databases or social network sites in light of e-mail addresses of victims that are targeted.

Future studies can also adopt time perspective theory to shed light on the actual behavior variance because behavior is affected by the way individuals relate their present behavior. Based on the study [68] recommended to include adults of different age ranges to determine the level to which cyberbullying victimization happens in the workplace

Other studies may also examine social desirability scales and actual posting behavior, involving extensive controversy range or indiscreet information, and their relationship with cyber bullying victimization. It is suggested that focus is placed on the general security practices and behavior, and attitude towards financial activity online, and the ability to take risks among internet users.

Another recommendation for future studies is to focus on framework enabling individual factors, contextual factors and message factors interaction and their examination, in light of their effects on the susceptibility of the individual towards the influence of malicious online attacks. It is expected that through such an understanding of the susceptibility of the individuals to online scams, responsible entities can effectively develop effective attack mitigations [111].

Harrison, Svetieva, et al. [58] urged the use of other relevant subject groups like organization employees or older population as a sample that holds lower e-mail and phishing awareness. Future studies were also suggested to theoretically examine phishing and experimentally investigate the different aspects of attention and elaboration, with the inclusion of time spent in e-mail reading and the order of noticing and recalling the message elements.

Different groups (IT and non-IT) may also be compared in future studies and they may analyze security behaviors like a selection of passwords, data backup procedures, scanning activity, and the like to further confirm the relationships. It may also focus on post-adoption activity (continuance or discontinuance) using a longitudinal study method

Finally, it was recommended that e-mail phishing threats contain various messages which should be attended to in terms of conscientiousness for the effective reinstallation of an order [86].

It was proposed to examine routine activities in detail and to delve into different ways that individuals can identify authentic content from disingenuous scammer content on the outcome variables, and a better understanding of the construct's relationships via mediating variables, suggestions related to the predictor variables such as personality factors from the Big Five Model in a quantitative study (e.g., personality factors from the Big-Five Model) and the exploration of databases or social network sites in light of email addresses of victims that are targeted and examine more extensive potential risky online activities like hacking, online banking, and online gambling. The study did not consider the online skills of users like digital literacy.

Future studies can include it along with other online behaviors (e.g., email use frequency), other online protective behaviors (e.g., privacy settings

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on SNS, using anti-virus software) as well as dispositional factors (e.g., morality)

7. LIMITATIONS

The limitation of this paper is a selection of sample studies, which only focus on empirical studies of phishing attack susceptibility. This paper is only focused on the identification of related factors that influence security behaviors related to phishing attacks.

8. CONCLUSIONS AND FUTURE WORK

This paper contributes to a review of the empirical literature on security behaviors related to phishing attacks susceptibility, focusing on social solutions.

The paper used 7 databases and identified 15 theories used in empirical phishing studies, with the majority of the authors adapting several theories to underpin their studies. There are four top theoretical underpinnings, namely Protection Motivation Theory, Routine Activity Theory and Theory of Planned Behavior, Big-Five Model. There are 18 main factors identified in the literature that contributed to issues in individual differences, experiential factors and attacker's skills.

There were 7 major and 3 sub various approaches as follow: 1- Individual Differences: 2- Demographic Characteristics, 3- Personality Traits,4- Human Behavior 5-Lifestyle, 6- Experiential Factors: 7- General experience, Technological experience, Professional experience 5-Attacker's Skills in E-mail Contextualization.

We firmly believe that future directions in security behavior studies related to phishing should attempt to address this issue, because lack of research regarding individual differences in susceptibility to online scams such as how and why suspicious individuals may still succumb to scams and still limited, the Big-Five personality traits have proven useful in many areas for predicting different aspects of human behavior.

Their validity in the context of predicting an individual's susceptibility to various forms of phishing attacks is still unclear and will require further research, also in demographic characteristics, previous studies of age and gender have yielded discrepant results. Therefore, it should disambiguate these findings, and studying human behavior factors can help us to understand the present and what the trends in society are, they can help us to predict the outcomes of our design proposals for the future better than we do now.

Email contextualization issue is contributed by investigating the effect of security awareness on users' information security protective behaviors in the context of phishing.

Additionally, researchers can increase their knowledge of the specific factors that contribute to an increased susceptibility to social media-based phishing attacks. This will enable them to identify the specific groups that are susceptible to phishing attacks on social media to conduct targeted security training.

Finally, understanding these issues will enable the development of IT policies and practices, better defensive software tools, and more effective, perhaps tailored, awareness training for the most susceptible users.

REFERENCES:

[1] B. B. G. Aakanksha, T. Ankit, K. Jain, and D. P. Agrawal, "Fighting against phishing attacks : state of the art and future challenges," *Neural Comput. Appl.*, 2016, doi: 10.1007/s00521-016-2275-y.

[2] J. Jang-jaccard, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/j.jcss.2014.02.005.

[3] I. Abdalla and M. Abass, "Social Engineering Threat and Defense : A Literature Survey," pp. 257–264, 2018, doi: 10.4236/jis.2018.94018.

[4] I. Vayansky and S. Kumar, "Phishing – challenges and solutions," vol. 3723, no. January, 2018, doi: 10.1016/S1361-3723(18)30007-1.

[5] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using," *EURASIP J. Inf. Secur.*, 2016, doi: 10.1186/s13635-016-0034-3.

[6] J. Kaur, "Examining the effects of knowledge , attitude and behaviour on information security awareness : A case

on SME Examining the Effects of Knowledge , Attitude and Behaviour on Information Security Awareness : A Case on SME," no. November 2013, pp. 1–6, 2017, doi: 10.1109/ICRIIS.2013.6716723.

[7] S. Furnell, L. Moore, and C. Security, "Security literacy : the missing link in today ' s online society ?," no. May, 2014, doi: 10.1016/S1361-3723(14)70491-9.

[8] F. Breda, H. Barbosa, and T. Morais, "Social Engineering and Cyber Security," *INTED2017 Proc.*, vol. 1, no. August, pp. 4204–4211, 2017, doi: 10.21125/inted.2017.1008.

[9] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.

[10] S. Egelman, E. Peer, and R. Gan, "The Myth of the Average User Improving Privacy and Security Systems through Individualization," 2015.

[11] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security : Individual , Culture and Security Environment," *Sci. Technol.*, no. DSTO-TR-2484, p. 45, 2010, doi: 10.14722/ndss.2014.23268.

[12] J. Sharp and P. Wu, "Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model," *J. Inf. Syst. Appl. Res. Ed.*, vol. 11, no. 3, 2018.

[13] L. Hadlington, "Human factors in cybersecurity ; examining the link between Internet addiction , impulsivity , attitudes towards cybersecurity , and risky cybersecurity behaviours," *Heliyon*, no. June, p. e00346, 2017, doi: 10.1016/j.heliyon.2017.e00346.

[14] M. T. Whitty, "Predicting susceptibility to cyber-fraud victimhood," vol. 26, no. 1, pp. 277–292, 2019, doi: 10.1108/JFC-10-2017-0095.

[15] S. M. Albladi and R. S. George, "Personality traits and cyber-attack victimisation: Multiple mediation analysis," *Jt. 13th CTTE 10th C. Conf. Internet Things - Bus. Model. Users, Networks*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/CTTE.2017.8260932.

[16] S. Al Awawdeh and A. Tubaishat, "An Information Security Awareness Program to Address Common Security Concerns in IT Unit," 2014, doi: 10.1109/ITNG.2014.67.

[17] J. F. Van Niekerk and R. Von Solms, "Information security culture : A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010, doi: 10.1016/j.cose.2009.10.005.

[18] W. R. Flores, "Shaping Information Security Behaviors Related to Social Engineering Attacks," Stockholm, Sweden 2016, 2016.

[19] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," *Proc. 28th Int. Conf. Hum. factors Comput. Syst. - CHI '10*, pp. 373–382, 2010, doi: 10.1145/1753326.1753383.

[20] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, 2018, doi: 10.1016/j.cose.2017.11.015.

[21] P. Taylor, D. Huang, P. P. Rau, and G. Salvendy, "Perception of information security," no. October 2014, pp. 37–41, 2010, doi: 10.1080/01449290701679361.

[22] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," pp. 124–133, 2005, doi: 10.1016/j.cose.2004.07.001.

[23] D. Booth, A. , Sutton, A. , Papaioannou, "Systematic Approaches to a Successful Literature Review," *2nd ed. Sage Publ. Ltd., London* ., p. 106, 2016.

[24] 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.*, vol. 14, no. 5, pp. 2865–2882, 2019.

[25] K. Choi, S. Cho, and J. Ree, "Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth : Application of cyber-routine activities theory with latent class analysis," vol. 100, no. May, pp. 1–10, 2019.

[26] C. Conetta, "Individual Differences in Cyber Security," *McNair Res. J. SJSU*, vol. 15, 2019.

[27] A. Diaz, A. T. Sherman, and A. Joshi,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia*, pp. 1–15, 2019, doi: 10.1080/01611194.2019.1623343.

[28] F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, "The Impact of Age , Gender , and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students : An Empirical investigation on Malaysian Universities The Impact of Age , Gender , and Educational level on the Cybersecurity Behaviors of ," *J. Phys. Conf. Ser.*, 2019, doi: 10.1088/1742-6596/1339/1/012098.

[29] V. Hooper and C. Blunt, "Factors influencing the information security behaviour of IT employees," *Behav. Inf. Technol.*, vol. 0, no. 0, pp. 1–13, 2019, doi: 10.1080/0144929X.2019.1623322.

[30] D. House and M. K. Raja, "Phishing : message appraisal and the exploration of fear and self-confidence," *Behav. Inf. Technol.*, vol. 0, no. 0, pp. 1–21, 2019, doi: 10.1080/0144929X.2019.1657180.

[31] J. Jansen and P. van Schaik, "The design and evaluation of a theory-based intervention to promote security behaviour against phishing," *Int. J. Hum. Comput. Stud.*, vol. 123, no. January 2018, pp. 40–55, 2019, doi: 10.1016/j.ijhcs.2018.10.004.

[32] P. M. W. Musuva, K. W. Getao, and C. K. Chepken, "A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility," *Comput. Human Behav.*, vol. 94, no. December 2018, pp. 154–175, 2019, doi: 10.1016/j.chb.2018.12.036.

[33] B. Venard, "The determinants of individual cyber security behaviours: Qualitative research among French students," *2019 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, Cyber SA 2019*, 2019, doi: 10.1109/CyberSA.2019.8899648.

[34] E. D. Frauenstein, "An Investigation into Students Responses to Various Phishing Emails and Other Phishing-Related Behaviours," in *2018 Information Security for South Africa*, 2018, vol. 973, no. August, pp. 44–59, doi: 10.1007/978-3-030-11407-7_4.

[35] L. Hadlington, "Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 262–274, 2018, doi: 10.5281/zenodo.495776.

[36] J. Jansen and P. van Schaik, "Persuading end users to act cautiously online: a fear appeals study on phishing," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 264–276, 2018, doi: 10.1108/ICS-03-2018-0038.

[37] J. Jansen and P. van Schaik, "Testing a model of precautionary online behaviour: The case of online banking," *Comput. Human Behav.*, vol. 87, pp. 371–383, 2018, doi: 10.1016/j.chb.2018.05.010.

[38] W. Leest, "The effectiveness of hints for online banking customers on reducing phishing susceptibility : A Dutch customer ' s perspective," 2018.

[39] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a phishing target," *Telemat. Informatics*, vol. 35, no. 5, pp. 1277–1287, 2018, doi: 10.1016/j.tele.2018.02.009.

[40] J. E. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks," *Int. J. Bus. Manag.*, vol. 13, no. 6, p. 1, 2018, doi: 10.5539/ijbm.v13n6p1.

[41] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," *Int. J. Hum. Comput. Stud.*, vol. 120, no. June, pp. 1–13, 2018.

[42] A. Algarni, Y. Xu, and T. Chan, "An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 661–687, 2017, doi: 10.1057/s41303-017-0057-y.

[43] I. M. Alseadoon, R. A. Ramadan, and A. Y. Khedr, "Cultural impact on Users ' Ability to protect themselves against Phishing websites," vol. 17, no. 11, pp. 1–5, 2017.

[44] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Human Behav.*, vol. 69, pp. 437–443, 2017, doi: 10.1016/j.chb.2016.12.040.

[45] J. W. Bullee, L. Montoya, M. Junger, and P. Hartel, "Spear phishing in organisations explained," *Inf. Comput.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Secur., vol. 25, no. 5, pp. 593–613, 2017, doi: 10.1108/ICS-03-2017-0009.

[46] M. Butavicius, K. Parsons, M. Pattinson, A. Mccormac, D. Calic, and M. Lillie, "Understanding Susceptibility to Phishing Emails : Assessing the Impact of Individual Differences and Culture," *Proc. Elev. Int. Symp. Hum. Asp. Inf. Secur. Assur. (HAISA 2017)*, vol. 2016, no. Haisa, 2017.

[47] D. Conway, R. Taib, M. Harris, K. Yu, S. Berkovsky, and F. Chen, "A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing," *Proc. Thirteen. Symp. Usable Priv. Secur.*, no. Soups, pp. 115–129, 2017.

[48] S. Goel, K. Williams, and E. Dincelli, "Got Phished? Internet Security and Human Vulnerability," *J. Assoc. Inf. Syst.*, vol. 18, no. 1, pp. 22–44, 2017, doi: 10.17705/1jais.00447.

[49] A. S. Hashim and S. Mahamad, "Factors Affecting Awareness on Information Security in Internet Banking Among Universiti Teknologi Petronas (UTP) Students," *Proc. 6th Int. Conf. Comput. Informatics*, vol. 2004, no. 195, pp. 356–362, 2017.

[50] H. Jafarkarimi, R. Saadatdoost, A. T. H. Sim, and J. H. Mei, "Determinant factors of cyberbullying: An application of theory of planned behavior," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 23, pp. 6472–6482, 2017.

[51] L. Li *et al.*, "Cyber Security Awareness and Its Impact on Employee ' s Behavior To cite this version : HAL Id : hal-01630550 Cyber Security Awareness and Its Impact on Employee ' s Behavior," *10thInternationalConferenceonResearch andPracticalIssuesofEnterpriseIn- Form. Syst.*, pp. 103–111, 2017.

[52] G. D. Moody, D. F. Galletta, and B. K. Dunn, "Which phish get caught An exploratory study of individuals′ susceptibility to phishing," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 564–584, 2017, doi: 10.1057/s41303-017-0058-x.

[53] A. A. Orunsolu *et al.*, "An Empirical Evaluation of Security tips in Phishing Prevention: A Case Study of Nigerian Banks," *I.J. Electron. Inf. Eng.*, vol. 66, no. 113, pp. 25–39, 2017, doi: 10.6636/IJEIE.201703.6(1).3).

[54] S. G. A. Van De Weijer and E. R. Leukfeldt, "Big Five Personality Traits of Cybercrime Victims," *Cyberpsychology, Behav. Soc. Netw.*, vol. 20, no. 7, pp. 407–412, 2017, doi: 10.1089/cyber.2017.0028.

[55] J. Wang, Y. Li, and H. R. Rao, "Coping responses in phishing detection: An investigation of antecedents and consequences," *Inf. Syst. Res.*, vol. 28, no. 2, pp. 378–396, 2017, doi: 10.1287/isre.2016.0680.

[56] G. White, T. Ekin, and L. Visinescu, "Analysis of protective behavior and security incidents for home computers," *J. Comput. Inf. Syst.*, vol. 57, no. 4, pp. 353–363, 2017, doi: 10.1080/08874417.2016.1232991.

[57] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," *Comput. Human Behav.*, vol. 60, pp. 185–197, 2016, doi: 10.1016/j.chb.2016.02.065.

[58] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing," *Online Inf. Rev.*, vol. 40, no. 2, pp. 265–281, 2016, doi: 10.1108/OIR-04-2015-0106.

[59] B. Harrison, A. Vishwanath, and R. Rao, "A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2016-March, pp. 5628–5634, 2016, doi: 10.1109/HICSS.2016.696.

[60] H. Jafarkarimi, R. Saadatdoost, A. T. H. Sim, and J. M. Hee, "Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior," *Comput. Human Behav.*, vol. 62, pp. 545–561, 2016, doi: 10.1016/j.chb.2016.04.024.

[61] J. Jansen and R. Leukfeldt, "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization," *Int. J. Cyber Criminol.*, vol. 10, no. 1, pp. 79–91, 2016, doi: 10.5281/zenodo.58523.

[62] G. Saridakis, V. Benson, J. N. Ezingeard, and H. Tennakoon, "Individual

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technol. Forecast. Soc. Change*, vol. 102, pp. 320–330, 2016, doi: 10.1016/j.techfore.2015.08.012.

[63] J. Wang, Y. Li, and H. R. Rao, "Overconfidence in Phishing Email Detection," *J. Assoc. Inf. Syst.*, vol. 17, no. 11, pp. 759–783, 2016, doi: 10.17705/1jais.00442.

[64] I. Alseadoon, M. F. I. Othman, and T. Chan, "What Is the Influence of Users ' Characteristics on Their Ability to Detect Phishing Emails ?," *Springer Int. Publ. Switz. 2015 H.A. Sulaiman al. (eds.), Adv. Comput. Commun.*, pp. 949–962, 2015, doi: 10.1007/978-3-319-07674-4.

[65] M. Alsharnouby, F. Alaca, and S. Chiasson, *Why phishing still works: User strategies for combating phishing attacks*, vol. 82. Elsevier, 2015.

[66] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks," *SSRN Electron. J.*, 2015, doi: 10.2139/ssrn.2544742.

[67] B. Harrison, A. Vishwanath, Y. J. Ng, and R. Rao, "Examining the impact of presence on individual phishing victimization," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2015-March, pp. 3483–3489, 2015, doi: 10.1109/HICSS.2015.419.

[68] J. V. Peluchette, K. Karl, C. Wood, and J. Williams, "Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem?," *Comput. Human Behav.*, vol. 52, pp. 424–435, 2015, doi: 10.1016/j.chb.2015.06.028.

[69] B. W. Reyns, "A routine activity perspective on online victimisation: Results from the Canadian general social survey," *J. Financ. Crime*, vol. 22, no. 4, pp. 396–411, 2015, doi: 10.1108/JFC-06-2014-0030.

[70] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, 2015, doi: 10.1016/j.cose.2015.01.002.

[71] S. Srisawang, M. Thongmak, and A. Ngarmyarn, "Factors affecting computer crime protection behavior," *Pacis*, p. 31, 2015, doi: 10.1016/j.tet.2014.07.041.

[72] A. Vishwanath, "Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack," *J. Comput. Commun.*, vol. 20, no. 5, pp. 570–584, 2015, doi: 10.1111/jcc4.12126.

[73] E. R. Leukfeldt and M. Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," *Deviant Behav.*, vol. 37, no. 3, pp. 263–280, 2014, doi: 10.1080/01639625.2015.1012409.

[74] S. Purkait, "An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website," *Inf. Manag. Comput. Secur.*, vol. 22, no. 3, pp. 194–234, 2014.

[75] L. Seda, "Identity theft and university students: Do they know, do they care?," *J. Financ. Crime*, vol. 21, no. 4, pp. 461–483, 2014, doi: 10.1108/JFC-05-2013-0032.

[76] X. Luo, W. Zhang, S. Burd, and A. Seazzu, "Investigating phishing victimization with the Heuristic-Systematic model: A theoretical framework and an exploration," *Comput. Secur.*, vol. 38, pp. 28–38, 2013, doi: 10.1016/j.cose.2012.12.003.

[77] C. Yoon and H. Kim, "Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms," *Inf. Technol. People*, vol. 26, no. 4, pp. 401–419, 2013, doi: 10.1108/ITP-12-2012-0147.

[78] I. Alseadoon, T. Chan, E. Foo, and J. G. Nieto, "Who is more susceptible to phishing emails?: A Saudi Arabian study," *ACIS 2012 Proc. 23rd Australas. Conf. Inf. Syst.*, no. Trusteer 2009, pp. 1–11, 2012.

[79] M. Pattinson, C. Jerram, K. Parsons, A. Mccormac, and M. Butavicius, "Information Management & Computer Security Emerald Article : Why do some people manage phishing e-mails better than Why do some people manage phishing e-mails better than others ?," no. March, 2012, doi: 10.1108/09685221211219173.

[80] J. WANG, "Phishing Susceptibility : An Investigation Into the Processing of a

Targeted Spear Phishing Email," *IEEE Trans. Prof. Commun.*, vol. 55, no. 4, pp. 345–362, 2012, doi: 10.1109/TPC.2012.2208392.

[81] F. T. Ngo and R. Paternoster, "Cybercrime Victimization: An examination of Individual and Situational level factors.," *Int. J. Cyber Criminol.*, vol. 5, no. 1, pp. 773–793, 2011.

[82] 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.*, vol. 51, no. 3, pp. 576–586, 2011, doi: 10.1016/j.dss.2011.03.002.

[83] J. L. Parrish, J. L. Bailey, and J. F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," *Southwest Decis. Sci. Inst. Annu. Meet.*, no. February 2015, pp. 285–296, 2009.

[84] R. T. Wright and K. Marett, "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *J. Manag. Inf. Syst.*, vol. 27, no. 1, pp. 273–303, 2010, doi: 10.2753/mis0742-1222270111.

[85] W. R. Flores, H. Holm, M. Ekstedt, and M. Nohlberg, "Investigating the correlation between intention and action in the context of social engineering in two different national cultures," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2015-March, pp. 3508–3517, 2015, doi: 10.1109/HICSS.2015.422.

[86] S. Kleitman, M. K. H. Law, and J. Kay, "It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling," *PLoS One*, vol. 13, no. 10, pp. 1–29, 2018, doi: 10.1371/journal.pone.0205089.

[87] B. Y. I. N. A. Wanca and A. Cannon, "How human behavior and decision making expose users to phishing attacks," *CITIZENS CRIME Comm. NEW YORK CITY*, 2016.

[88] E. J. Williams, A. Beardmore, and A. N. Joinson, "Individual differences in susceptibility to online influence: A theoretical review," *Comput. Human Behav.*, vol. 72, pp. 412–421, 2017, doi: 10.1016/j.chb.2017.03.002.

[89] O. Wori, "Computer crimes : factors of cybercriminal activities," *Cloud Publ.*, vol. 3, no. 1, pp. 51–67, 2014.

[90] T. Halevi, J. Lewis, and N. Memon, "Phishing, Personality Traits and Facebook," 2013.

[91] B. de Raad and B. Mlačić, "Big Five Factor Model, Theory and Structure," *Int. Encycl. Soc. Behav. Sci. Second Ed.*, no. December, pp. 559–566, 2015, doi: 10.1016/B978-0-08-097086-8.25066-6.

[92] H. S. Jones and J. Towse, "Examinations of Email Fraud Susceptibility," pp. 80–97, 2018, doi: 10.4018/978-1-5225-4053-3.ch005.

[93] E. R. Leukfeldt, *FACTOR IN*, no. May. 2017.

[94] D. Liu and W. K. Campbell, "The Big Five personality traits, Big Two metatraits and social media: A meta-analysis," *J. Res. Pers.*, vol. 70, no. August, pp. 229–240, 2017, doi: 10.1016/j.jrp.2017.08.004.

[95] J. Holdershaw and P. Gendall, "Understanding and predicting human behaviour Understanding and predicting human behaviour," no. May, 2014.

[96] T. Admin, "Human Behavior Being Exploited By Phishers," pp. 1–9, 2014, doi: 10.11693/hyhz20181000233.

[97] V. S. Subrahmanian, M. Ovelgonne, T. Dumitras, and B. A. Prakash, "The Global Cyber-Vulnerability Report," *Glob. Cyber-Vulnerability Rep.*, no. November 2013, pp. 33–46, 2015, doi: 10.1007/978-3-319-25760-0.

[98] F. Stajano and P. Wilson, "Understanding scam victims: Seven principles for systems security," *Commun. ACM*, vol. 54, no. 3, pp. 70–75, 2011, doi: 10.1145/1897852.1897872.

[99] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/j.jcss.2014.02.005.

[100] B. A. C. Johnston and M. Warkentin, "FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY1," vol. 34, no. 3, pp. 549–566, 2010, doi: 10.2307/25750691.

[101] P. Ifinedo, "Understanding information systems security policy compliance: An

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007.

[102] E. R. Leukfeldt and M. Yar, "Applying Routine Activity Theory to Cybercrime : A Theoretical and Empirical Analysis Applying Routine Activity Theory to Cybercrime : A Theoretical and," vol. 9625, no. January, 2016, doi: 10.1080/01639625.2015.1012409.

[103] B. W. Reyns, "A routine activity perspective on online victimisation: Results from the Canadian general social survey," *J. Financ. Crime*, vol. 22, no. 4, pp. 396–411, 2015, doi: 10.1108/JFC-06-2014-0030.

[104] A. Vishwanath, "Habitual facebook use and its impact on getting deceived on social media," *J. Comput. Commun.*, vol. 20, no. 1, pp. 83–98, 2015, doi: 10.1111/jcc4.12100.

[105] G. Norris, A. Brookes, and D. Dowell, "The Psychology of Internet Fraud Victimisation: a Systematic Review," *J. Police Crim. Psychol.*, 2019, doi: 10.1007/s11896-019-09334-5.

[106] Y. Han and Y. Shen, "Accurate spear phishing campaign attribution and early detection," *Proc. ACM Symp. Appl. Comput.*, vol. 04-08-Apri, pp. 2079–2086, 2016, doi: 10.1145/2851613.2851801.

[107] F. Hassandoust, H. Singh, and J. Williams, "How Contextualisation Affects the Vulnerability of Individuals to Phishing Attempts," *AIS Electron. Libr. (AISeL)*, 2019.

[108] M. Nicho, H. Fakhry, and U. Egbue, "Evaluating user vulnerabilities vs phisher skills in spear phishing," *Iadis Int. J. Comput. Sci. Inf. Syst.*, vol. 13, no. 2, pp. 93–108, 2018, doi: 10.33965/ijcsis_2018130207.

[109] B. Biswas and A. Mukhopadhyay, "Why do I get phished? The role of persuasion, design authenticity and contextualization," *25th Am. Conf. Inf. Syst. AMCIS 2019*, pp. 1–10, 2019.

[110] A. Dhabi and P. Traits, "Cultural and psychological factors in cyber-security," vol. 13, no. 1, pp. 43–56, 2017.

[111] E. J. Williams, A. Beardmore, and A. N. Joinson, "Computers in Human Behavior Individual differences in susceptibility to online in fl uence : A theoretical review," *Comput. Human Behav.*, vol. 72, pp. 412–421, 2017.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Appendix A: Table 2 Summary of Related Factors

No.	Authors	Factors	Method used	Theories used	Respondents
1-	Anawar, Kunasegaran, Mas'Ud, & Zakaria [24]	**8 Factors** Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism, Self-monitoring, General Experience, Technical Experience	Quantitative survey	Big Five Model	252 of employees in mid-sized IT-related companies in Malaysia
2-	Choi, Cho & Ree [25]	**4 Factors** Cyberbullying Victimization, Risky Online Leisure Activity, Online Lifestyle Activities, Online Risky Social Networking Activity **15 Sub-Factors** Personality details	Quantitative survey	• Lifestyle Exposure Theory • Routine Activity Theory	7109 adolescents (13-17 years of age) among 17 South Korean regions.
3-	Conetta [26]	**4 Factors** Individual Differences, Knowledge, Self-Efficacy, Personality Traits	Quantitative survey	N/A	183 university students in US
4-	Diaz, Sherman & Joshi [27]	**4 Factors** Academic Year Progression, Cyber Training, Involvement In Cyber Scholarship Programs, Time Spent On The Computer, Age Demographics	Phishing experiment	N/A	11,234 undergraduate students currently enrolled at UMBC in US
5-	Fatokun, Hamid, Norman & Fatokun [28]	**13 Factors** Perceived Vulnerability, Perceived Severity, Security Self-Efficacy, Perceived Barriers, Response Efficacy, Cues To Action, Peer Behavior, Computer Skills, Internet Skills, Prior Experience With Computer Security Practices, Perceived Benefits, Self-Reported Cybersecurity Behavior, Familiarity With Cyber-Threats	Quantitative survey	• Health Belief Model • Protection Motivation Theory	340 students in Malaysia
6-	Hooper & Blunt [29]	**11 Factors** Cues To Action, Perceived Likelihood, Perceived Impact, Perceived Impact, Response Costs, Response Efficacy, Response Benefits, Social Norms, Detection, Self-Efficacy, Sanctions	Quantitative survey	• Protection Motivation Theory • Theory of Deception • Theory of Reasoned Action	70 IT employees in New Zealand
7-	House & Raja[30]	**8 Factors** Self-Efficacy, Threat Severity, Response Efficacy, Threat Susceptibility, Self-Confidence Items, Intention to Respond, Fear Arousal, Message Involvement	Quantitative Survey And Phishing Experiment	Extended Parallel Processing Model	400 university students in USA

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

8-	Jansen& van Schaik [31]	**8 Factors** Perceived Vulnerability, Perceived Severity, Response Efficacy, Self-Efficacy, Response Costs, Attitude, Protection Motivation	Quantitative Survey	Protection Motivation Theory	768 internet users in Netherlands
9-	Musuva, Getao & Chepken [32]	**5 Factors** Attack Quality, Motivation To Process, Ability To Process, Detection, Elaboration, Control Variables **17 Sub-Factors** Quality Of Argument, Persuasive Cues, Involvement, Responsibility, Distractions, Emotions Pressure, Threat, Gender, Age, Level Of Education, Role, Years On Internet, Hours On Internet, Computer Skill, E-Mail Load, E-Mail Responsiveness, Online Service Usage, Prior Victimization, Risk Propensity	Phishing Experiment	• Interpersonal Deception Theory • Theory of Deception • Heuristic Systematic Model • Elaboration Likelihood Model	4483 respondents who were students, staff, adjunct faculties, full-time faculties, management, interns and mailing lists in Kenya.
10-	Venard [33]	**6 Factors** Self-Efficacy, Perceived Personal Susceptibility To Digital Threat, Guardianship, Conformity	Qualitative (Face-To-Face Interviews)	N/A	60 students in France
11-	Whitty [14]	**11Factors** Age, Gender, Education, Lack Of Premed, Sensation Seeking lack of perseverance., Locus Of Control, Addiction, Exposure Online, Risky Places, Guardianship	Quantitative Survey	N/A	11, 780 employees In UK
12-	Albladi& George [15]	**9 Factors** Competence, Trust, Motivation, Past Experience, Conscientiousness, Neuroticism, Extraversion, Agreeableness, Openness To Experience,	Quantitative Survey	Big Five Model	316 faculty staff in Saudi
13-	Frauenstein [34]	**2 Factors** Computer and Internet Skill, Social Media Sites, Security Education And Training	Quantitative Survey	N/A	126 Black African Students (58 Males And 68 Female)
14-	Gratian, Bandi, ukier, Dykstra & Ginther [20]	**4 Factors** Demographic, Personality Traits, Take Risks, Decision-Making Styles **5 Sub-Factors** Agreeableness, Conscientiousness, Neuroticism, Openness, Extraversion	Quantitative Survey	Big Five Model	369 faculty staff and students in US

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

15-	Hadlington [35]	**2 Factors** Age, Company Size And Risky Cyber Security Behaviors	Quantitative Survey	N/A	538 full or part-time employee in U.K	
16-	Jansen, J. & van Schaik [36]	**6 Factors** Perceived Vulnerability, Perceived Severity, Fear, Response Efficacy And Self-Efficacy, Response Costs	Quantitative Survey	Protection Motivation Theory	1,201 Internet Users In Netherland	
17-	Jansen & van Schaik [37]	**13 Factors** Perceived Vulnerability, Perceived Severity, Perceived Risk, Trust, Response Efficacy, Response Costs, Injunctive Norms, Descriptive Norms, Locus Of Control, Protection Motivation, Online-Banking Experience, Age	Quantitative Survey	Protection Motivation Theory	1200 online banking users in Netherlands	
18-	Leest [38]	**2 Factors** Gender, Age	Experiment Supported By A Quantitative Survey Using Eye-Tracking Glasses	N/A	27 bank customers in Netherland	
19-	De Kimpe, Walrave, Hardyns, Pauwels & Ponnet[39]	**7 Factors** Impulsivity, Digital Copying Behavior, Risky Online Self-Disclosure, Social Network Site Use, Online Purchasing Behavior, Phishing Targeting, Control Variables	Quantitative Survey	• Lifestyle Exposure Model • Routine Activity Theory	723 online users in Netherlands	
20-	Sharp & Wu [12]	**9 Factors** Behavior, Perceived Barriers To Practice, Self-Efficacy, Cues To Action, Prior Security Experience, Perceived Vulnerability, Perceived Benefits, And Perceived Severity.	Quantitative Survey	Health Belief Model	153 university students in US	
21-	Thomas [40]	**8 Factors** Lack Of Information Literacy Skills, Sophistication Of Miscreant Attacks, High-Impact Job Roles, Transactional Jobs With High Volumes Of E-mail, Unfamiliarity With Phishing, Confidence Level Training, Familiarity With Phishing Victims, Testing Proficiency	Qualitative Case Study	• Protection Motivation Theory • Theory of Planned Behavior	7 experts in US	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

37-	Wang & Rao [55]	**11 Factors** Perceived Phishing Susceptibility, Perceived Phishing Severity, Perceived Phishing Threat, Perceived Detection Efficacy, Phishing Anxiety, Task-Focused Coping, Emotion-Focused Coping, Avoidance, Detection Effort, Coping Addictiveness, Detection Accuracy, Demographic Information **9 Sub-Factors** Age, Gender, Education, Prior Victimization, Income, Internet Experience, No. Of Daily Email, No. Of Credit Card, Dispositional Optimism	Quantitative Survey and Experiment	Protection Motivation Theory	457 individuals throughout 47 states in US
38-	White, Ekin & Visinescu [56]	**5 Factors** Computer Security Education, Perceived Barriers, Self-Efficacy, Cues To Action	Quantitative Survey	• Health Belief Model • Protection Motivation Theory	Adult population mean age of 44 in US
39-	ArachchilageLove & Beznosov [57]	**9 Factors** Avoidance Behavior, Avoidance Motivation, Perceived Threat, Perceived Severity, Perceived Susceptibility, Safeguard Effectiveness, Safeguard Cost, Self-Efficacy, Phishing Threat Avoidance	Mixed-Method using Think-Aloud Procedure And Pre And Post-Tests	Protection Motivation Theory	20 university students in UK
40-	Harrison, Svetieva, & Vishwanath [58]	**7 Factors** Message-Level, Individual-Level, Attention, Elaboration, Phishing Attacks Susceptibility **5 Sub-Factors** Fear Vs. Reward-Based Messages, Presence Of Leakage Cues, Subjective E-Mail, Knowledge And Experience, Objective Phishing Knowledge	Field Experiment	Elaboration Likelihood Model	194 university students in US

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

45-	Wang & Rao [63]	**6 Factors** Cognitive, Motivational, Overconfidence, Control Variables **12 Sub-Factors** Cognitive Effort, Variability In Attention Allocation, Perceived Familiarity With The Business Entities, Perceived Self-Efficacy Of Detecting Phishing Emails, Dispositional Optimism, Gender, Age, Education, Income, Number Of Daily Emails, Online Transaction, Experience, Prior Victimization Task Easiness	Quantitative Survey and Experiment	N/A	600 public individuals of 47 states in US.
46-	Alseadoon, Ibrahim & Othman [64]	**7 Factors** Big Five Personality, Confirmation, Trust, Submissiveness, E-mail Experience, E-mail Richness, Response Susceptibility	Mixed-Method	• Theory of Deception • Big Five Model	187 university students in Saudi
47-	Alsharnouby, Alaca, & Chiasson [65]	**6 Factors** Attention to URL And SSL Indicators, Familiarize with Website, Technical Expertise, Gender, Age, Deduction of Website And Security Indicators	Mixed-Method	N/A	(1750) eye trackers in Canada
48-	Flores [18]	**10 Factors** Intention, Cultural Effects, Resistance To Phishing, Self-Efficacy, IS Policy Awareness, General IS Awareness, Age, Computer Experience, Gender, Formal IS Training,	Quantitative Survey and Phishing Experiment	N/A	2,099 employees of nine organizations in Sweden, USA and India
49-	Halevi,Memon & Nov [66]	**6 Factors** Higher Levels Of Conscientiousness, Use The Internet For More Diverse Purposes, Computer-Mediated Communication Competence, Gender, More Aware Of Cyber-Risks, Not Able To Successfully Estimate Their Likelihood Of Being Phished	Quantitative Survey and Phishing Experiment	N/A	40 employees in India
50-	Harrison, Vishwanath & Rao, [67]	**2 Factors** Social Presence, Richness Cues	Phishing Experiment	Heuristic-Systematic Model	125 university students in US.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

51-	Peluchette , Karl, Wood &Williams [68]	**4 Factors** Risky SNS Practices, Facebook Friends, Self-Disclosure, Big Five Personality Factors	Quantitative Survey	Big Five Model	572 university students from Southeastern US and Southeastern Australia.
52-	Reyns [69]	**7 Factors** Online Exposure To Motivated Offenders, Online Target Suitability, Online Guardianship, Individual Characteristics, Phishing, Hacking, Malware Infection **14 Sub-Factors** Banking, Booking/Reservations, Purchasing Social Networking, Personal Information, Posted Visiting Risky, Web Sites Post, Accurate Information, Anti-Virus Software, Delete E-mails, Change Passwords, Female, Non-White, Age, Married, Income	Quantitative Survey	Routine Activity Theory	Canadians
53-	Shropshire, Warkentin & Sharma [70]	**6 Factors** Perceived Ease Of Use, Perceived Usefulness, Perceived Organizational Support, Perceived Ease Of Use, Perceived Usefulness, Perceived Organizational Support, Conscientiousness, Agreeableness	Quantitative Survey	• Technology Acceptance Model • Big-Five Model	170 university students in US.
54-	Srisawang, Thongmak & Ngarmyarn [71]	**8 Factors** Conscientiousness Personality, Perceived Value Of Data, Prior Experience, Subjective Norm, Security Knowledge, Safeguard Costs, Threat Appraisal, Coping Appraisal, Protection Motivation	Quantitative Survey	Protection Motivation Theory	A Total Of 600 Personal Computer Users In Homes And Workplace In Thailand Were The Respondents.
55-	Vishwanath[72]	**7 Factors** Phishing Attacks Susceptibility, E-Mail Habit Strength, Big-Five Personality, Information Insufficiency, E-Mail Habit, Heuristic Processing, Systematic Processing	Phishing Experiment	Big Five Model	400 university students in US.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

56-	Leukfeldt & Yar [73]	**12 Factors** Background Characteristics, Value, Visibility (Online Activities), Accessibility, Technical Guardian, Personal Guardian, Victimization By Hacking, Malware Infection, Identity Theft, Consumer Fraud, Cyberstalking, Cyber Threats **30 Sub-Factors** Gender, Age, Education Level, Work, Personal Income, Household, Income, Financial Assets, Financial Possessions, Savings, Frequency Of Internet Use, Targeted Browsing, Direct Communication: E-Mail, Direct Communication: MSN, Skype, Chatting In Chat Boxes, Chatting In Chat Boxes, Online Gaming, Active On Online Forums, Active On Social Network Sites Twitter, Downloading, Untargeted Browsing, Buying Online, OS: Windows, Web Browser, No Virus Scanner, Computer Knowledge, Online Risk Awareness	Quantitative Survey	Routine Activity Theory	9161 citizens, aged from 15 years and over in Netherlands.
57-	Purkait [74]	**6 Factors** Internet Usage, Demographic, Cognitive, Awareness Of Phishing, Safe Internet Practice, Internet Skill **12 Sub-Factors** No. Of Years, Frequency, Hours Per Day, Short-Term Memory, Attention Vigilance, Age, Gender, Income, Education, Technical Background, Computer Usage, Income, Family Size, Victim Of Phishing	Quantitative Survey and Phishing Experiment	N/A	621 Internet users in India.
58-	Seda [75]	**1 Dimension** Knowledge	Qualitative using Semi-Structured Interviews	N/A	University students in Australia
59-	Luo, Zhang, Burd & Seazzu [76]	**8 Factors** Argument Quality, Source Credibility, Genre Conformity, Need For Cognition, Time Pressure, Pre-Texting, Less Damage, Victimization	Phishing Experiment	Heuristic-Systematic Model	105 University faculty and staff in US

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

60- Yoon & Kim [77]	**8 Factors** Security Policy, Moral Obligation, Subjective Norm, Attitude, Perceived Threat Severity, Perceived Threat, Vulnerability, Response Efficacy, Self-Efficacy, Computer Security Behavioral Intentions	Quantitative Survey	• Protection Motivation Theory • Theory of Reasoned Action • Health Belief Model • Technology Acceptance Model	162 employees in a number of organizations in Korea	
61- Alseadoon, Chan, Foo & Nieto [78]	**7 Factors** Big Five Personality, Submissiveness, E-mail Experience, E-mail Richness, Susceptibility, Confirmation, Response	Quantitative Survey and Phishing Experiment	Big Five Model	200 university students in Saudi	
62- Pattinson, Jerram, Parsons, Mccormac & Butavicius [79]	**8 Factors** Familiarity With Computers, Extraverted, Agreeable, Conscientious, Neurotic, Open, Cognitive Impulsivity, Behavioral Response With Phishing E-Mails	Phishing Experiment using Scenario-Based Role-Play and Quantitative Survey	N/A	117 university students in Australia.	
63- WANG [80]	**10 Factors** Attention To Visceral Triggers, Title Of Email Message Urgency, Attention To Phishing Deception Indicators, Grammar Sender's Address, Cognitive Effort, Message Involvement, Scam Knowledge, Control Variables, Likelihood To Respond **3 Sub-Factors** Gender, Age, Knowledge Of Emails From The Organization	Quantitative Survey and Phishing Experiment	Theory of Deception	321 Northeast public university members in US.	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

64-	Ngo & Paternoster [81]	**12 Factors** Self-Control, Exposure To Motivated Offender, Target Suitability, Capable Guardianship, Getting A Computer Virus, Receiving Unwanted Exposure To Pornographic Material, Being Solicited For Sex, Encountering Phishing, Experiencing Online, Harassment By A Stranger And By A Non-Stranger, Experiencing Online Defamation, Control Variable **16 Sub-Factors** Internet Hours, E-mail Hours, IM Hours, Chat Room Hours, Communication With Stranger, Provide Personal Info, Click/Open Links, Computer Skills, Security Software, Computer Crime Info, Male, Age, White, Employment, Married, Computer Deviant	Quantitative Survey	• Lifestyles/Routine Activities • General Theory of Crime And Victimization	295 US university students.
65-	Vishwanath, Herath, Chen, Wang, & Rao, [82]	**9 Factors** Involvement, Computer Self-Efficacy, Domain-Specific Knowledge, E-mail Load, Attention To Sender Source, Attention To Grammar And Spelling, Attention To Urgency, Elaboration, Likelihood To Respond	Phishing Experiment	• Interpersonal Deception Theory (IDT) • Theory of Deception • Elaboration Likelihood Model	321 US university students.
66-	Parrish , Bailey & Courtney [83]	**6 Factors** Big-Five Personality Profile, Type Of Lure, Type Of Hook, General Experience, Technological Experience, Professional Experience **19 Sub-Factors** Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism, Security Upgrade, Incomplete Account Information, Financial Incentive, False Account Updates, Reply To E-mail, Link To Website, Reply To SMS Text Message, Reply To Instant Messenger, Positive, Negative Usage, Training, Career, Academic	N/A	• Big-Five Model	N/A

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

67-	Sheng, Holbrook, Kumaraguru, Cranor & Downs [19]	**5 Factors** Prior Exposure to Anti-Phishing Training, Gender, Age, Participants' Technical Knowledge, Risk Perception For Financial, Investment	Quantitative Survey	N/A	1001 respondents represented the study sample gathered through Amazon.com's mechanical turk (mturk) in the UK.	
68-	Wright & Marett [84]	**3 Factors** Experiential, Dispositional, Deception Success **6 Sub Factors** Computer Self-Efficacy, Web Experience, Security Knowledge, Trust, Perceived Risk, Suspicion	Phishing Experiment	Interpersonal Deception Theory (IDT)	446 US university students.	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Appendix B: **Table 4 Ranking of the Main Factors**

No.	Factors	Theories	Description	Relevant studies	Frequency (studies)
1	Experience	N/A	Experience is the knowledge/skill to perform a specific activity that has been gained from the past. It is used to describe prior events, knowledge, feelings that comprise an individual's life/character.	[83], [47], [84], [58], [24], [85], [37], [51], [28]	9
2	Perceived severity	PMT, HBM	Outcomes related by the individual to an event or results like cancer diagnosis. Such outcomes may be linked to an expected future event or a present state like a pre-existing health issue.	[60], [67], [13], [50], [49], [64], [77], [36], [37]	9
3	Perceived effective	PMT; HBM	Perceived effectiveness is described as the subjective possibility that a message will persuade the reader and reading such a message is the first step of the process of persuasion. In cases where readers find it difficult to read and understand the message, it is not likely to persuade them.	[60], [67], [13], [50], [49], [64], [77], [36], [37]	9
4	Self-efficacy	TPB; PMT; HBM TD	Self-efficacy is described as the individual's belief that he/she possesses the skills to perform a specific act to realize an objective.	[44] ,[12], [82], [57], [84] ,[61], [47], [26], [77]	9
5	Perceived susceptibility/ Perceived vulnerability	HBM; PMT	Perceived susceptibility is to the perception of the individual of the potential risk of being infected by a health disease/condition and this covers general susceptibility estimates and general susceptibility.	[60], [67], [13], [49], [64], [77], [36], [37]	8
6	Big-Five personality (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism)	BFM	**Openness** is the inclination of the individual to embark on embracing novel experiences. **Neuroticism** is a feeling of anxiety, anger, distress and depression and refers to an inclination towards experiencing adverse feelings which may include anger, guilt, disgust, fear and sadness. **Extraversion** is a trait of individuals that display outgoing, sociable and gregarious behaviors, Extroverted individuals are friendlier, outgoing and are at home interacting with other individuals.	[83], [54], [15], [72], [64], [20], [70], [24]	8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

			Agreeableness is a behavior reflecting friendliness and cooperation, and are very trusting of others as they are convinced of their honesty and decency. **Conscientiousness** is an individual's trait that involves the display of organization, self-discipline and dutiful behavior.		

7	Awareness	N/A	Enhance the recognition and retention of information.	[41], [43], [46], [49], [74], [73], [85]	7
8	Attitude	TRA; TPB	It refers to the immediate reaction to specific environmental objects towards appreciating them.	[60], [67], [13], [50], [49], [64]	6
9	Digital guardianship	RAT	Digital guardianship comprises of distinct data awareness coupled with visibility of transformative endpoint and behavioral threat detection and response that urges the individual towards data protection without the business getting affected.	[69], [73], [81], [61], [39], [25]	6
10	Knowledge	N/A	Knowledge represents the familiar feeling, awareness or understanding of another individual or a thing like facts, information, descriptions, or skills, encountered or obtained via education or perception, discovery or learning.	[47], [82], [26], [58], [84], [26]	6
11	Online exposure to motivated offenders	RAT	The time spent using the internet for the purpose of banking transactions, online bookings and reservations, buying goods/services and social networking that exposes the user to attackers and potential attackers	[69], [73], [81], [61], [39], [25]	6
12	Online target suitability	RAT	This refers to the individual's attractiveness as a target in terms of posting personal and private information online, visiting questionable websites	[69], [73], [81], [61], [39], [25]	6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

			or posting precise information on the web.		
13	Perceived behavioral control	TPB	Perceived behavioral control refers to the perceived ease/difficulty in the performance of specific behavior, assuming past experience is reflected in such perception, and barriers are anticipated.	[60], [67], [13], [50], [49], [64]	6
14	Subjective Norms	TPB	Subjective norm is the influence of other individuals on the individual's beliefs, owing to their importance to him/her that motivates his/her thought processes.	[60], [67], [13], [50], [49], [64]	6
15	Perceived barriers	HBM	Individual's assessment of the obstacles to behavior change.	[55], [67], [61], [41], [71], [77]	6
16	Computer Skills	N/A	Computer skills consist of the ability to use computers and other technology efficiently and this encapsulates the use of fundamental hardware and software and the comprehension of major IT concepts and components.	[32], [81], [44]	3
17	Trust	N/A	Trust brings about efficient dealings with people with the help of the information obtained through daily senses and good intuition of the held wisdom concerning decision-making and learning while trying to expand trust circles to include other individuals.	[64], [41], [43]	3
18	E-mail Load	N/A	The volume of e-mails an individual receives in a given day.	[32], [82]	2