Gamifying Cybersecurity Knowledge to Promote Good Cybersecurity Behaviour

Fatokun Faith B.
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
evangfatoks@gmail.com

Zalizah Awang Long
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
zalizah@unikl.edu.my

Suraya Hamid
Department of Information Systems,
Faculty of Computer Science & IT
Universiti Malaya
Kuala Lumpur, Malaysia
suraya_hamid@um.edu.my

Fatokun Johnson O.
Department of Mathematical Sciences,
Faculty of Science
Anchor University
Lagos, Nigeria
jfatokun@aul.edu.ng

Christopher Ifeanyi Eke,
Department of Computer Science,
Federal University of Lafia,
Nasarawa State, Nigeria.
eke.christopher@science.fulafia.edu.ng

Azah Norman,
Department of Information Systems,
Faculty of Computer Science & IT
Universiti Malaya
Kuala Lumpur, Malaysia
azahnorman@um.edu.my

***Abstract*— Cybersecurity is a major issue in contemporary times as security breaches are prevalent in organizations due to cyberattacks. The bulk of these attacks is caused by human errors as well as a lack of cybersecurity knowledge by online users. Though there is advancement in the provision of technological solutions to enhance online safety, humans are still very vulnerable to cybercrime. It is therefore important to consider novel and attractive ways to educate as well as spread awareness of cybersecurity knowledge that can help in enhancing good online behaviours and avoiding cyber threats. This paper via an exploratory approach proposes the gamifying of cybersecurity knowledge to promote good online behaviour. This is ongoing research that intends to develop a gamification model that will integrate cybersecurity knowledge and behaviour into one comprehensive immersion. Specifically, this paper discusses the components needed for the proposed model which will be presented in future works.**

Keywords*— *cybersecurity; online safety; cybersecurity knowledge; cybersecurity behaviour; gamification

I. Introduction

Security breaches are prevalent in organizations due to human errors. As a result of the swift escalation of Internet access across the globe, building necessary safeguards against privacy and security will only be of more importance. This actuality, therefore, makes cybersecurity, as well as other outstanding practices that safeguard personal computers, all digital data, and programs from attack to be the major critical problems of the present generation [1-3]. Information systems are still highly vulnerable to threats from users' undesirable behaviours, which are closely related to IS users' information security awareness.

Despite advancements in technological solutions to enhance online safety, humans still fall victim to cybercrime. An estimation by experts reveals that between 70-80% of the cost ascribed to cyber-attacks comes mainly as a result of human error [4]. Simple actions such as opening the wrong email attachment, using a virus-affected Universal Serial Bus (USB) drive, or even clicking on a bad link can be vulnerable to network security. In view of this, it can be stated that the most robust security network universally is as good as the human with the right access and virtually secured behaviour.

According to Gratian, Bandi [5], humans are often recognized as the weakest link in cyber security, since any technical security solution brought to the market is still prone to failures caused by human error. As such, there is a considerable amount of research that seeks to better understand users and the factors that influence their security behaviours [1, 6-9]. Online threats continue to be a growing concern. Current systems are designed for the general audience, without regard to differences in their users' personalities. Halevi, Memon [10] suggest approaching applications and system design from a user-targeted perspective. In particular, understanding the factors that contribute to secure online behaviour is an important step toward creating such tailored defence systems. Cyber-victimization has extensive economic and personal consequences for Internet users as well as negative consequences for economies and the cyberinfrastructure [11]. It has been widely recognized in the psychology of cybersecurity literature that ordinary users rather than technology systems are the weakest link in cybersecurity [12].

Cybersecurity knowledge is of utmost importance regarding how users face or handle cybersecurity challenges [13], this could also affect their cybersecurity behaviours. Therefore, it would be fantastic to perform an empirical study on a larger set of the population such as tertiary institution students, thus interacting with the cyber-users and extracting quantitative information. Cybersecurity knowledge refers to the know-how, familiarity, awareness or understanding, and experience, of persons regarding cybersecurity practices, alongside cyber threats, to ensure cybersecurity assurance [14]. Security technologies are increasingly being developed with a user-centric approach. Part of the challenge of user-centered security is that people interacting with security systems possess tremendously different levels of computer and security knowledge and even different levels of basic literacy [15]. Another interesting study focused on assessing cybersecurity behaviour and knowledge from an anti-phishing perspective [14]. The results of the study indicated that the technical knowledge of the participants regarding the risks of online phishing and solutions correlated positively with their intentions of adopting and making use of anti-phishing solutions.

The threat landscape of computer security is continuously changing and new threats are emerging all the time. As a result, users are likely to be familiar with certain online threats more than others. As informed by Zukarnain, Hashim [16], the world is hyperconnected and children grow in an environment filled with an increase in digital connectivity. Cybersecurity training is one way to imbibe adequate and lasting practical knowledge that can help nurture the cybersecurity awareness of the upcoming generation. This will consequently assist the younger generation in becoming good users of the web as well as maintaining a status quo of well-behaved digital citizens. Tertiary institution students are also in the formative stages of their life, especially those at undergraduate levels, this stage could determine what the rest of their lives may look like. Hence, if cybersecurity knowledge is been immersed into them via proactive measures such as gamification appropriately at the college stage, it is possible to impact their cybersecurity behaviours moving forward [12, 13].

Several forms of testing experience of internet users exist in the literature. One of these is gamification, which is the process of improving services with affordances that are motivational to invoke gamely experiences and additional behavioural outcomes [17-19]. Regarding investigating knowledge in security awareness, there are scholarly works that have been carried out sparingly. In a study by Arachchilage and Love [20], the researchers proposed a game design framework specifically for the avoidance of attacks caused by phishing. Their idea was based on the fact that game-based education makes provision for learning to be undertaken in an environment that is natural. Therefore, with such backing, they carried out the research by offering a classification taxonomy for the training resources of cybersecurity in a university environment based on gamification.

Hamari, Koivisto [21] highlighted the role that gamification plays to be able to invoke the same psychological experiences as the game does generally. Gamification plays a very important role in awareness because it makes it more fun and engaging. Game-based education is gaining a lot of popularity in contemporary times. The reason is due to its provision of the chance to learn in a more naturalistic manner. Consequently, phishing precisely is an online identity theft, that attempts to steal private and quite delicate information which could comprise usernames, passwords, as well as online banking details from victims. To be able to avoid this, several studies have considered phishing awareness [14, 20, 22-25], however other aspects of cybersecurity are not been addressed adequately.

Moreover, Gonzalez, Llamas [26] of recent, informed that gamification has gained a lot of attention recently since it can achieve results that are positive most of the time. Therefore, with such backing, they carried out the research by offering a classification taxonomy for the training resources of cybersecurity in a university environment based on gamification. Cybersecurity is a growing as well as very important field known for making a great impact on society [27]. Contemporarily, society has begun to understand the criticality involved with the preservation of computer systems security as well as the Internet, with regards to the prevention of malicious attacks at several levels of governance, ranging from corporate to national [28]. Thus, it is important to educate the concept of cybersecurity among students in particular and the general populace [3, 29-31]. From the perspective of education, the approach of gamification- both as a tool for experimental learning as well as in imbibing learning experiences from research, helps in improving other horizontal skills. Some of these skills include self-efficacy, goal setting, and cooperation. More so, games have the ability to adapt to multiple learning theories as well as practical skills, some of which include, problem-solving and decision-making activities, even though there are concerns that could be raised with regard to their respective usage. One of the major concerns is linked to the lack of knowledge regarding the level of effectiveness of the features used in designing the game, to ensure game performance improvement. Consequently, there is a lack of studies associated with design game features perceived by students as most useful to detect their success self-perception.

This paper presents an explorative study that proposes the gamifying of cybersecurity knowledge to promote good online behaviour. The objective of this paper is to investigate cybersecurity knowledge and behaviour; propose the components for gamifying cybersecurity knowledge.

The remainder of the paper is divided into 4 sections: (II) Overview of literature, (III) Methodology, (IV) Results and Discussion, and (V) Conclusion.

II. Overview of Literature

A brief background study on related works in cybersecurity knowledge, behaviour, and gamification is discussed in this section.

A. *Cybersecurity Knowledge*

There is no specific definition of cybersecurity knowledge present in the literature, however, based on collaborative discussions some researchers agree with a particular definition. Cybersecurity knowledge refers to the know-how, familiarity, awareness or understanding, and experience, of persons regarding cybersecurity practices, alongside cyber threats, to ensure cybersecurity assurance [13, 14, 32]. It is appalling to state that small businesses using technology are at risk of cyberattacks and often do not have adequate cybersecurity knowledge, budgets, or dedicated security staff [13]. Hence, the need for cybersecurity knowledge to be acquired is of optimal necessity for cyber-users.

In a recent study by Olmstead and Smith [33] on what the public knows about cybersecurity, the authors conducted a survey consisting of 13 cybersecurity questions, which was used to test the knowledge of Americans regarding several cybersecurity issues. The research made use of an online survey with questions in form of multiple choice wherein the respondents could select appropriate answers based on their knowledge of cybersecurity and its related terminologies. Though cybersecurity is a very diversified and complicated area, however, the questions used as an instrument in this study covered a large aspect of the general concepts as well as the foundation stressed by cybersecurity experts to be seen as essential for users in protecting themselves in the cyberspace (internet). Their findings indicated that most adults could accurately identify simple cybersecurity issues such as identifying the strongest passwords, however, public cybersecurity knowledge was very low on some issues that are relatively technical [12, 33]. For example, a large proportion of cyber-users were not aware that utilizing the "private browsing mode" on their internet browsers could not make them and their activities invisible to the internet service providers (ISPs). Also, and very surprisingly, so many cyber adults were not aware of the meaning of "botnet", which is a group of networked computers used by hackers to extract data illegally or simply steal data.

Corroboratively, a study was conducted on phishing in a university community via experimental analysis [34]. In this research, the authors wanted to test the knowledge of the participants to see how well they understand phishing activities, thus, the use of phishing emails was sent unknowingly to the participants. Results indicated that students were more prone to phishing attacks compared to the faculty or staff, which indicates that experience could be a factor in victimizing an individual during social engineering attacks. The results also showed that there is no strong correlation between individuals' demographics and their susceptibility to phishing, in contrast to what has been hypothesized by other researchers over the years [35-37]. Nevertheless, predicting which users are more vulnerable to social engineering based on demographic factors needs further research. Consequently, education and increased awareness of cybercrimes among end-users is certainly needed. Results also reaffirmed the belief of the authors that the human aspects of phishing attacks are as important as the technological aspects [1, 6, 34, 38].

Summarily, results from these studies conform to the establishment of work routines that are focused on performance and normalcy as well as team foundation theories. This thus indicates the importance of team training in addressing contemporary critical cybersecurity issues. Furthermore, the collaboration of human as well as cybersecurity team leadership is of much significance in managing complicated technical systems as well as coordinating effective responses to present as well as novel cyber threats [39]. Essentially, there is a need to also leverage social sensing platforms for the enhancement of human measurement as well as to ensure validation and restructuring of theories related to human performance influencing factors and teamwork.

B. *Cybersecurity Behaviour*

The cybersecurity behaviour of users is a major area of concern for firms as well as general users of the internet. The reason is due to the drift by cyber-criminals from targeting technical systems to now attacking the system users directly. In lieu of the aforementioned, series of studies have tried in providing an understanding of cybersecurity behaviour among users. One of the advantages of comprehensively having a balanced knowledge about user behaviour is the knowledge application by both researchers as well as security practitioners [40]. Such knowledge can then be applied in the quest for changing behaviour to favour cybersecurity. A couple of studies have classified several cybersecurity behaviours, although there are variances across studies with regard to the naming conventions.

Cybersecurity Behaviour therefore can be defined according to the current research, as the actions of an individual, mannerisms, attitudes, reactions, as well as the way they conduct themselves generally in cyberspace [40]. The essence of studying the cybersecurity behaviour of users is to ensure that good cybersecurity behaviours are being promoted while at the same time mitigating bad or malicious cybersecurity behaviours. Several studies have discussed on cybersecurity behaviours of users from different perspectives, they are reviewed next.

Anwar, He [41], in a study on gender differences and employees' cybersecurity behaviours, tried to explore whether differences in cybersecurity beliefs and behaviours existed based on gender. Their findings produced a conclusion that gender is an important factor when it comes to cybersecurity behaviours among employees. Their results further showed that there are statistically significant gender-wise differences in terms of computer skills, prior experience, cues-to-action, security self-efficacy, and self-reported cybersecurity behaviour [41]. Furthermore, it was revealed in another study that students are more vulnerable to risks. Students' scores of exposure to crime were similarly higher than the other groups [42]. According to their results, the more the respondents perceive threats, their behaviour becomes protective. One of the most significant findings of their study which is also in line with findings from other studies [7, 43] was that the higher the education level, the more their information security awareness is, hereby stating that educational level had some impact on the security awareness of the participants.

Summarily, the literature is extant with works regarding cybersecurity behaviours as reviewed. However, the majority of the studies focused on singular facets of cybersecurity without really addressing other cybersecurity behavioural factors deeply. Also, the lack of a large sample for investigation in some of the studies affected generalizability, hence the current study will consider a larger sample size for investigation. There is no study so far that addressed the link between cybersecurity behaviour and cybersecurity knowledge empirically, which this research is aimed at achieving as part of its core objectives. Finally, no study has been able to establish how gamification can be introduced based on the relationships between cybersecurity behaviour and cybersecurity knowledge as discussed earlier. As the individual believes they are more protected in the workplace they may be inclined to take more risks, circumvent accepted protocols and engage in poorer cybersecurity behaviours. This proposition is couched very much in a tentative way, and there is a need to explore this in more detail through further research. The cyber security community should continue to progress and develop but it must not forget its roots and the obvious statistics that indicate we have not yet addressed the risks associated with the one consistent element of cyber security, the human error [7, 16, 27, 44].

C. Cybersecurity Gamification

Game-based education is gaining a lot of popularity in contemporary times. The reason is due to its provision of the chance to learn in a more naturalistic manner. Consequently, phishing precisely is an online identity theft, that attempts to steal private and quite delicate information which could comprise a username, passwords, as well as online banking details from victims [23, 45]. To be able to avoid this, there is a need to consider phishing awareness. The bulk of research focusing on gamification of cybersecurity dwells more on phishing threat avoidance, however, there are many more aspects of cybersecurity that could be incorporated into gamification to enhance cybersecurity knowledge among users.

Gamification is the process of improving services with affordances that are motivational to invoke gamely experiences and additional behavioural outcomes [17-19]. In one of the interesting studies regarding gamification and security, Arachchilage and Love [20] designed a game framework for avoiding phishing attacks. The authors developed a Technology Threat Avoidance Theory (TTAT) based theoretical model and utilized it in the game design framework [46]. More so, they conducted a survey study on about 150 regular computer users to gather feedback via a questionnaire. Findings revealed that the elements of perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and perceived susceptibility should be addressed when designing a computer user game framework for avoiding phishing attacks [3, 27, 28]. The researchers also made some arguments regarding the possibility of using such game design framework for other malicious IT attacks preventions, such as viruses, malware, botnets, and spyware, and not just for preventing phishing attacks.

Recently, a study by Ros, González [27], analysed students' self-perception of success and learning effectiveness via gamification in an online cybersecurity course. Interestingly, the authors designed a cybersecurity game anchored on the cognitive constructivism learning theory. The game scenes were built via metaphors used in presenting the major cybersecurity content to the students. Moreover, the game was delivered in a regular course with dual objectives, the first was to find essential design factors affecting the success and self-perception of students. Furthermore, the authors proposed a structural equation model to discover the most significantly impactful elements on the success self-perception of the students. From their results, it was discovered that there was no notable influence attached to the game contextualization and the design of the realistic game. Both were examples of best game design practices used in evaluating the game's learning effectiveness. Moreover, their results provide suggestions of a high correlation existing between success in the course and gameplay. Consequently, the authors stated that the performance chronological analysis revealed that the intent to play the game is likely a predictor of a simple dropout. Thus, the introduction of these games into the educational curricula could help in improving the engagement of students as well as consolidating their cybersecurity knowledge [3, 27].

The game's effectiveness in this study was analysed via comparisons between the dual group academic results for the term. Thus, since there was no randomness across the first groups, the study can be considered a quasi-experimental design, and assertions can only infer the existence of a correlation between gameplay and grades obtained. Future work could conduct more empirical studies with other well-established cybersecurity theoretical constructs as well as gamification constructs that focus mainly on relevant cybersecurity issues. Another study focusing on cybersecurity education via gamification from another perspective called CTF (Capture the Flag) revealed interesting submissions [47]. The paper provides a summary of contemporary popular gamification technologies as well as discusses the practice of using CTF (Capture the Flag) and projects competitions for classroom teaching. The research followed an exploratory approach. It employed the CTF competition to bring many teams across the globe in competing among themselves on cybersecurity challenges. It was informed that based on cyber awareness at elementary levels, the majority of occurring security breaches are a result of not being aware, thus the need for cyber education to be incorporated into the academic curriculum [19, 48, 49].

A very recent study by van Steen and Deeleman [3], on the successful gamification of cybersecurity training, designed a cybersecurity serious game that could be applied in cybersecurity training. The game's effectiveness was tested experimentally over a non-cyber security game that contained/did not contain information related to cybersecurity, via measures of the theory of planned behaviour. From the findings, it was revealed that the cybersecurity game attained higher self-reported scores on factors such as attitudes, perceived behavioural control, intentions, and behaviour as compared to non-cyber security games.

Thus, their study further revealed that a cybersecurity theory-informed serious game has the potential of having a significant effect on the self-reported theory of planned behaviour scores and behaviour. Though, serious games are known to positively affect intentions and attitudes in previous research [50-53]. This study provided additional findings by showing that perceived behavioural control, as well as subjective norms, could also get influenced in the same way. Additionally, the study also shows that just mere provision of information is not enough to yield significant changes as compared to a controlled condition. This supports the idea that to create change, it is not enough to just inform people of best practices alone.

Summarily, the reviewed studies have focused on the gamification of cybersecurity to address specific issues relating to cybersecurity. However, there are still limitations with regard to the development of a gamification approach that can cover a balanced portion of cybersecurity to instil long-lasting knowledge of cybersecurity among the users. Furthermore, cybersecurity topics are quite extensive, yet studies need to be able to conceptualise and concise the cybersecurity information into a package without losing the impacting strength for the users. Most of the studies also tried to design games in the real sense of gameplay, however, there is a need for serious games in the cybersecurity field, and perhaps a gamification integration could help promote the educative goal of developing cybersecurity knowledge games.

Precisely, no study has conceptualised these gamification designs based on statistical models as this study intends to do first to have a proper understanding of how the gamification can be developed more appropriately. Corroboratively, this study will also empirically conduct investigations on cybersecurity knowledge, behaviours, and how they are related as well as carry out inferential analysis on the components of gamifying cybersecurity knowledge among students in tertiary institutions. There is a wide gap for the current research and future studies to address regarding designing more intelligent cybersecurity games built on well-developed cybersecurity gamification models such as the one promised by this current study.

The next section shall discuss the proposed methodological approach to conduct the study.

III. METHODOLOGY

A. Research Approach

The research proposes to employ a mixed research approach, which would involve both quantitative and experimental techniques. The reason for the probable mix is to be able to obtain qualitative data to back up the quantitative data, thus comparing results from both approaches to be able to provide viable assertions as well as make strong conclusions.

B. Participants

Participants of the research shall be students in tertiary institutions across Klang Valley, in Malaysia. Students in this context refer to both undergraduates and postgraduates. The targeted students are active students currently studying in tertiary institutions within Klang Valley, Malaysia. Tertiary institutions consist of universities, colleges, as well as other higher educational institutes. This research is exploring the impact of cybersecurity knowledge on the cybersecurity behaviour of computer/internet users, as well as proposes a gamification technique to enhance cybersecurity knowledge among the users. Thus, tertiary institution students are appropriate participants for this study as they make use of the internet regularly due to the nature of their daily academic activities, and research, as well as catching up with family and friends via social media, especially during the period of the Covid 19 pandemic as of the time this research is being conducted.

C. Constructs

This research is grounded on three established theories from literature. The study shall make use of three theories, Protection Motivation Theory [54], the Actor-network theory, known as ANT [55], and the Technology Threat Avoidance Theory (TTAT) [56]. The first theory is a behavioral theory, while the second is more of a familiarity theory, used in representing the knowledge component, and the third theory is for the gamification component respectively.

The Protection Motivation Theory is used majorly for explaining the intentions of users to employ security technologies, as well as the means and time a user can adopt either adaptive or maladaptive behaviors when being informed of a threatening security incident. Constructs of Security Self Efficacy and Prior Experience with Security Practices, will be extracted from this theory as they are more related with Cybersecurity Experiences.

The Actor-network theory (ANT), helps in explaining the reactions to arising challenges and barriers when trying to comprehend a lot of security-associated behavior and engagement, such as past experiences, attributes of users as well as technological affordability. ANT is "a very crude method of learning from actors without imposing the priori definition of their work-building capacities" [57]. This theory basically is a useful approach in understanding the relationship between online behaviors and threat familiarity (that is, what shapes online engagement and internet experience, in this case cybersecurity knowledge).

The current study holds its grip on the Technology Threat Avoidance Theory (TTAT), as it gives explanations on the reason and manner in which users are able to avoid cyberthreats voluntarily [56]. TTAT was developed by Liang and Xue to synthesize literature across diverse areas comprising psychology, health care, Internet security as well as risk analysis. Thus, its basic premise is that when a cyberthreat is being perceived by IT users, there is a motivation to avoid such threats actively via using certain safeguard measures if they perceive the avoidance of that threat by the prescribed measure of safeguard, after which they might as well avoid the threat passively via emotion focused coping performances. Furthermore, the process and factors influencing the threat avoidance behavior of cyber-users is being delineated by TTAT [58]. Thus, it postulates that the behavior of threat avoidance could be illustrated as a cybernetic process whereby the aim of users is the enlargement of the distance amidst their present state of security as well as the end state that is not deemed safe [6, 46, 59].

First of all, users appraise the existence as well as the cyber threat level being faced and afterwards assess possible actions in avoiding such threats [60, 61]. On the basis of the aforementioned appraisals, decisions are being made as to which measure of safeguarding could help in mitigating the threat faster. Several key factors are identified in reflecting user perceptions, motivations as well as behaviors in the course of this process. In accordance to TTAT, a malicious threat would be avoided by users if they believe it is truly a threat and that it can be avoided via applying necessary safeguards. When being incorporated into a risk analysis research [62, 63] as well as health psychology [54, 64, 65], TTAT suggests that the determination of threat perception by users is via the threat occurrence perceived probability as well as the threat negative consequence perceived severity. Thus, being advised by previous health protective behavior researches [54, 66-68] as well as self-efficacy [1, 41, 43, 69], there is a submission by TTAT, stating that users put three factors into consideration when evaluating the manner in which threat can be avoided, in the course of taking a measure of safeguard. These include: the safeguard effectiveness, safeguard costs, and the user self-efficacy in applying such safeguards.

Other constructs of this research such as Cybersecurity Awareness and Cybersecurity Knowledge shall be adapted from related Cybersecurity Awareness empirical studies. Thus, the research shall make use of 5 independent constructs representing Cybersecurity Knowledge namely: Cybersecurity Awareness (CSA), Cybersecurity Knowledge (CSK), Familiarity with Cyber Threats (FCT), Prior Experience with Computer Security Practices (PE), and Cybersecurity Compliance (CSC). Corroboratively, another 8 constructs would be used in measuring the Cybersecurity Gamification component namely; Safeguard Effectiveness (SGE), Safeguard Cost (SGC), Security Self-Efficacy (SE), Perceived Severity (PS), Avoidance Motivation (AM), Avoidance Behavior (AB), Perceived Threat (PT), and Perceived Susceptibility (PSB), respectively. The Dependent Variable shall be Cybersecurity Behavior (CSB). All resulting to a gamification model to create awareness, enhance cybersecurity knowledge and promote good cybersecurity behavior among tertiary institution students.

D. Data Collection

This research shall employ the use of an online survey to collect data, and if the researcher experiences any delay, an alternative means of collecting data through the use of a paper questionnaire shall be made available. The online survey shall be sent via the university mailing systems, as well as social media platforms to the general student population. Prior to data collection, consent shall be obtained from the participants, as well as permission granted from the relevant research ethics committee of the anchoring university. For the qualitative part of the research, data shall be collected via structured interviews with selected experts across the cybersecurity/IT field.

E. Data Analysis

Data analysis shall be achieved via Structural Equation Modelling Techniques. The primary tool for data analysis will be the Statistical Package for Social Sciences (SPSS).

F. Software Development

For cybersecurity gamification development, UNITY software will be used. This game will be developed based on the components from the research model as well as cover hot cybersecurity contemporary topics.

G. Research Design

Figure 1 illustrates the research design flow, clearly elucidating the steps in which the research will be conducted.

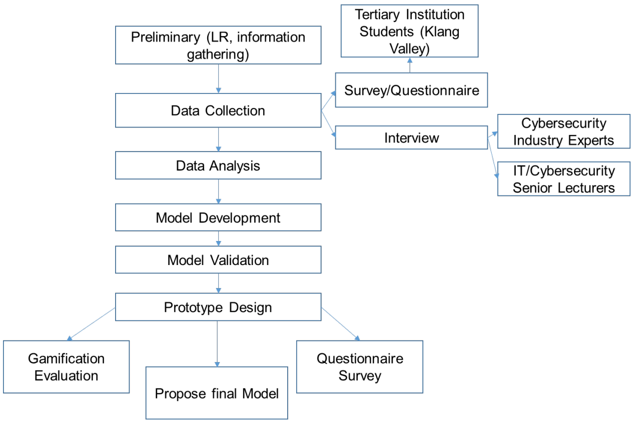

Figure 1. Research Design

IV. RESULT & DISCUSSION

In this section, the components of the research model will be discussed as this is ongoing research work. Specifically, constructs used in this research comprise three sections: Cybersecurity Knowledge; Cybersecurity Behaviours; and Cybersecurity Gamification Components. The cybersecurity knowledge and cybersecurity gamification constructs are independent variables while cybersecurity behaviour is the dependent variable for this research. Based on an extensive literature review, the components of the constructs have been derived to best suit the aim of this research. For measuring cybersecurity knowledge, five (5) constructs will be used, namely: Cybersecurity Awareness, Cybersecurity Knowledge, Familiarity with Cyber-threat, Prior Experiences with Computer Security Practices, and Cybersecurity Compliance. Consequently, to measure cybersecurity gamification, eight (8) constructs will be used, namely: Safeguard Effectiveness, Safeguard Cost, Self-Efficacy, Perceived Severity, Avoidance Motivation, Avoidance Behaviour, Perceived Threat, and Perceived Susceptibility. The dependent variable in this research is Cybersecurity Behaviour. The measures/constructs for this research are explained briefly in the next subsections.

A. Cybersecurity Awareness

The Cybersecurity Awareness scale is the first among five (5) scales used in measuring the cybersecurity knowledge component of this research. Cybersecurity Awareness is used to measure the overall awareness of cybersecurity terms amongst the participants. The questions would consist of different aspects of cybersecurity and how participants are fully aware of those aspects. A 7-point Likert scale in reversed order will be used to gather responses from items under this scale.

B. Cybersecurity Knowledge

Unlike Cybersecurity Awareness, the Cybersecurity Knowledge scale will be used in measuring the specific cybersecurity knowledge of the participants. It will also deeply investigate how the participants gain knowledge or learn about these various cybersecurity constituents instead of just their overall awareness levels. A 7-point Likert scale is proposed in reverse order to gather responses under this scale.

C. Familiarity with Cyber-threat

This scale will be used in measuring the level of familiarity with common cyber-threats. The goal is to discover if the participants understand what these cyber-threats are and the consequences of falling for them. Also, it will find out how much the participants know about the cyber-threats and if they know how to avoid them in the first place. A 7-point Likert scale will be used in reverse order to gather responses for this scale.

D. Prior Experience with Computer Security Practices

This scale will be used in measuring the level of experience among participants in good cybersecurity practices. The idea is to find out issues such as training, reading security newsletters, and having hands-on experience with practical cybersecurity practices either personally or at their work stations/via institutions. A 7-point Likert scale will be used in reverse order to gather the responses.

E. Cybersecurity Compliance

The cybersecurity compliance scale is used in measuring how and if participants meet up with various controls (usually enacted via regulatory authority, the industry groups, or the law), all aimed at ensuring the protection of data confidentiality, integrity, and availability, respectively. The responses shall be gathered via a 7- point Likert scale in reverse order.

F. Safeguard Effectiveness

Safeguard effectiveness is crucial to minimizing daily errors and failures. In this study, safeguard effectiveness is one of the scales used in measuring the cybersecurity gamification components. Specifically, it will be used in measuring how participants perceive the proposed gamification approach as useful in enhancing cybersecurity knowledge as well as how it can help protect them from falling for cyber-attacks. The responses shall be gathered via a 7-point Likert scale in reverse order.

G. Safeguard Cost

Safeguard cost refers to the payback for safeguard effectiveness. It also constitutes the physical as well as cognitive efforts, such as time, money, inconvenience, and comprehension required by using the safeguard measures. In this research, Safeguard Cost will be used in measuring if participants are willing to sacrifice certain efforts, such as time, money, inconvenience, and comprehension to be able to achieve safeguard effectiveness with regards to cybersecurity knowledge they receive from the gamification approach. The responses shall be gathered via a 7-point Likert scale.

H. Self - Efficacy

Self-efficacy refers to a person's confidence in adopting a safeguard measure. In this case, the self-efficacy scale is used to measure the participant's confidence levels and perceptions towards making use of a gamification tool in enhancing their cybersecurity knowledge to further improve their cybersecurity behaviour. To gather non-biased responses from the participants, a 7- point Likert scale will be used.

I. Perceived Severity

Perceived severity refers to negative consequences associated with an individual as regards an event or outcome. In this case, it refers to the negative circumstances' participants associate with the event or outcome of cybersecurity gamification in helping to boost their knowledge on cybersecurity threats as well as to measure how the participants take cybersecurity issues seriously. To achieve a non-biased result, a 7-point Likert scale will be used.

J. Avoidance Motivation

Avoidance motivation is an aspect of human nature wherein individuals learn ways of avoiding negative stimuli based on social, psychological, and physiological rationales. It is of utmost advantage, particularly in threatening circumstances; however, it can be also disadvantageous when it has to deal with task avoidance requiring completion. In this study, the avoidance motivation scale will be used to find out what motivates participants in accepting the cybersecurity gamification tool to boost cybersecurity knowledge. A 7-point Likert scale will be used in gathering the responses.

K. Avoidance Behaviour

The avoidance behaviour scale will be used to find out behavioural aspects of participants regarding why and how they would want to use the cybersecurity gamification tool in avoiding cyber-attacks. A 7-point Likert scale will be used in gathering the data.

L. Perceived Threat

Perceived threat refers to the extent to which an individual perceives a malicious cyber threat as dangerous or harmful. Here, the gamification tool is expected to help users detect the danger level of several cyber-attacks or threats. A 7-point Likert scale will be used to gather data in this respect.

M. Perceived Susceptibility

Perceived susceptibility refers to the subjective probability of an individual as to if a malicious cyber-attack will have a negative impact on them. In this research, the perceived susceptibility scale will find out if the cybersecurity gamification tool can be able to help individuals detect the negative impact of a cyber-attack. The responses shall be gathered via a 7-point Likert scale.

N. Cybersecurity Behaviour

Cybersecurity behaviour is the dependent variable used in this study and it will be the base variable on all the other components of cybersecurity knowledge and cybersecurity gamification will be tested. The cybersecurity behaviour scale will be used in measuring the actual cybersecurity behaviours of the participants with respect to recent cybersecurity issues and how users are to behave when surfing the internet or when faced with cybersecurity challenges. A 7-point Likert scale will be used in gathering the data.

Figure 2 presents the conceptual framework for the ongoing research.

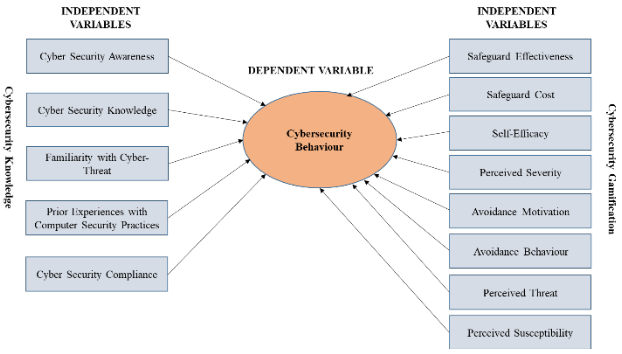

Figure 2. Research Conceptual Framework

V. CONCLUSION

A. Study Limitations

The first limitation of this research is that currently, there is no quantitative study to verify the components of the gamification tool. However, this is justified as the research is ongoing and the components for the quantitative analysis are already being studied. In the future, the researcher will present the quantitative analysis findings to find out the mindset of the users regarding their acceptability of the cybersecurity gamification model and if their knowledge was enhanced by the proposed cybersecurity game.

B. Contributions

This research shall contribute in diverse ways such as: firstly, in identifying factors that can be used in assessing cybersecurity knowledge of students in tertiary institutions; secondly, it will contribute to establishing the relationships between cybersecurity knowledge and cybersecurity behaviour of students in the tertiary institutions. Finally, the research would use an assessment result to propose a gamification model that can be replicated by other researchers in the cybersecurity behavioural domains. Practically, this research will help in providing assertions that can be of use to the cybersecurity units of tertiary institutions, to enable them to maintain good cybersecurity practices for better cybersecurity assurance of the students, as well as other cyber users in the institutions.

C. Future Work

In the future, the researchers tend to complete the quantitative and experimental aspects of the research, by first investigating the level of cybersecurity knowledge from users as well as testing their knowledge via the developed cybersecurity gamification prototype. Afterward, a post-analysis will be conducted to examine the level of satisfaction as well as knowledge enhancement by the users regarding cybersecurity issues. Moreso, the developed game can be integrated into general platforms such for the common users to constantly get awareness about cybersecurity issues and how to avoid cyber-attacks efficiently.

Security technologies are increasingly being developed with a user-centric approach. Part of the challenge of user-centred security is that people interacting with security systems possess tremendously different levels of computer and security knowledge and even different levels of basic literacy.

The present research intends to assess the impact of cybersecurity knowledge on the cybersecurity behaviour of students in tertiary institutions via an empirical quantitative approach with the inclusion of gamification ideation for enhancing cybersecurity knowledge, which would result in a cybersecurity gamification model. Specifically, the research aims at investigating cybersecurity knowledge as well as finding out the impact it has on the cybersecurity behaviour of students in tertiary institutions. More so, the research is proposing a gamification model for the impact of cybersecurity knowledge on the cybersecurity behaviour of tertiary institution students. Finally, this research will validate the gamification model via a prototype to find the impact of cybersecurity knowledge on the cybersecurity behaviour of students in tertiary institutions.

ACKNOWLEDGMENT

Special thanks to all authors of the work for their selfless contributions accordingly.

REFERENCES

[1] Blythe JM, Coventry L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior. 2018;87:87-97.

[2] Caulkins B, Marlowe T, Reardon A. Cybersecurity Skills to Address Today’s Threats. Advances in Intelligent Systems and Computing2019. p. 187-92.

[3] Van Steen T, Deeleman JR. Successful Gamification of Cybersecurity Training. Cyberpsychology, Behavior, and Social Networking. 2021;24(9):593-8.

[4] Hadlington L. The "human factor" in cybersecurity: Exploring the accidental insider. Psychological and Behavioral Examinations in Cyber Security2018. p. 46-63.

[5] Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Computers and Security. 2018;73:345-58.

[6] Addae JH, Brown M, Sun X, Towey D, Radenkovic M. Measuring attitude towards personal data for adaptive cybersecurity. Information and Computer Security. 2017;25(5):560-79.

[7] Evans M, Maglaras LA, He Y, Janicke H. Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks. 2016;9(17):4667-79.

[8] Faith FB, Suraya H, Azah N. The Development of a Conceptual University Student Cybersecurity Behavioural Model (C-Uscb) based on the Impact of Multiple Factors and Constructs of Self-Reported Cybersecurity Behaviours. Data Science Research Symposium 2018; Malaysia: umexpert; 2018.

[9] Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017;3(7):e00346.

[10] Halevi T, Memon N, Lewis J, Kumaraguru P, Arora S, Dagar N, et al. Cultural and psychological factors in cyber-security. Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services; Singapore, Singapore. 3011165: ACM; 2016. p. 318-24.

[11] Dodel M, Mesch G. Cyber-victimization preventive behavior: A health belief model approach. Computers in Human Behavior. 2017;68:359-67.

[12] Yan Z, Robertson T, Yan R, Park SY, Bordoff S, Chen Q, et al. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior. 2018;84:375-82.

[13] Raineri EM, Fudge T. Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs. Journal of Higher Education Theory & Practice. 2019;19(4).

[14] Wang PA, editor Assessment of cybersecurity knowledge and behavior: an anti-phishing scenario. International Conference on Internet Monitoring and Protection (ICIMP); 2013.

[15] Rajivan P, Moriano P, Kelley T, Camp LJ. Factors in an end user security expertise instrument. Information and Computer Security. 2017;25(2):190-205.

[16] Zukarnain ZA, Hashim MZ, Muhammad N, Mansor FA, Azib WNHW. Impact of training on cybersecurity awareness. Gading Journal of Science and Technology (e-ISSN: 2637-0018). 2020;3(01):114-20.

[17] Hamari J. Transforming homo economicus into homo ludens: A field experiment on gamification in a utilitarian peer-to-peer trading service. Electronic commerce research and applications. 2013;12(4):236-45.

[18] Huotari K, Hamari J, editors. Defining gamification: a service marketing perspective. Proceeding of the 16th international academic MindTrek conference; 2012: ACM.

[19] Gonzalez H, Llamas R, Ordaz F. Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. Res Comput Sci. 2017;146:35-43.

[20] Arachchilage NAG, Love S. A game design framework for avoiding phishing attacks. Computers in Human Behavior. 2013;29(3):706-14.

[21] Hamari J, Koivisto J, Sarsa H, editors. Does gamification work?--a literature review of empirical studies on gamification. 2014 47th Hawaii international conference on system sciences (HICSS); 2014: IEEE.

[22] Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: A survey. Computers & Security. 2017;68:160-96.

[23] Arachchilage NAG, Love S, Beznosov K. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior. 2016;60:185-97.

[24] Canova G, Volkamer M, Bergmann C, Borza R, Reinheimer B, Stockhardt S, et al., editors. Learn to spot phishing URLs with the Android NoPhish app. IFIP World Conference on Information Security Education; 2015: Springer.

[25] Rocha Flores W, Holm H, Svensson G, Ericsson G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management & Computer Security. 2014;22(4):393-406.

[26] Gonzalez H, Llamas R, Ordaz F. Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. Research in Computing Science. 2017;146:35-43.

[27] Ros S, González S, Robles A, Tobarra L, Caminero A, Cano J. Analyzing Students’ Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. IEEE Access. 2020;8:97718-28.

[28] Wolfenden B. Gamification as a winning cyber security strategy. Computer Fraud & Security. 2019;2019(5):9-12.

[29] Paschoal F, Ebecken NFF, Ribeiro GVS, Daquer LMdA, Mauro RC, Ogasawara ES, editors. FitRank — Social app to combat physical inactivity study of the use of fitness social apps on Facebook's users profiles. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI); 2017 21-24 June 2017.

[30] Ros S, Gonzalez S, Robles A, Tobarra L, Caminero A, Cano J. Analyzing students’ self-perception of success and learning effectiveness using gamification in an online cybersecurity course. IEEE Access. 2020;8:97718-28.

[31] Scholefield S, Shepherd LA. Gamification Techniques for Raising Cyber Security Awareness. arXiv preprint arXiv:190308454. 2019.

[32] Jia Y, Qi Y, Shang H, Jiang R, Li A. A Practical Approach to Constructing a Knowledge Graph for Cybersecurity. Engineering. 2018;4(1):53-60.

[33] Olmstead K, Smith A. What the public knows about cybersecurity. Pew Research Center. 2017;22.

[34] Mohebzada J, El Zarka A, BHojani AH, Darwish A, editors. Phishing in a university community: Two large scale phishing experiments. Innovations in Information Technology (IIT), 2012 International Conference on; 2012: IEEE.

[35] Sawyer BD, Hancock PA. Hacking the Human: The Prevalence Paradox in Cybersecurity. Human Factors. 2018;60(5):597-609.

[36] Sharma K. Impact of framing and priming on users' behavior in cybersecurity: Missouri University of Science and Technology; 2017.

[37] Tirumala SS, Sarrafzadeh A, Pang P, editors. A survey on Internet usage and cybersecurity awareness in students. 2016 14th Annual Conference on Privacy, Security and Trust (PST); 2016: IEEE.

[38] Adams M, Makramalla M. Cybersecurity skills training: An attacker-centric gamified approach. Technology Innovation Management Review. 2015;5(1).

[39] Buchler N, Rajivan P, Marusich LR, Lightner L, Gonzalez C. Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. Computers & Security. 2018;73:114-36.

[40] Mashiane T, Kritzinger E, editors. Cybersecurity behaviour: a conceptual taxonomy. IFIP International Conference on Information Security Theory and Practice; 2018: Springer.

[41] Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior. 2017;69:437-43.

[42] Ogutcu G, Tastik OM, Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security. 2016;56:83-93.

[43] Fatokun FB, Hamid S, Norman A, Fatokun JO. The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. Journal of Physics: Conference Series. 2019;1339:012098.

[44] Nicholson J, Morrison B, Dixon M, Holt J, Coventry L, McGlasson J, editors. Training and Embedding Cybersecurity Guardians in Older Communities. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems; 2021.

[45] Kelley T, Amon MJ, Bertenthal BI. Statistical models for predicting threat detection from human behavior. Frontiers in Psychology. 2018;9(APR).

[46] Arachchilage NAG, Love S. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 2014;38:304-12.

[47] Li C, Kulkarni R, editors. Survey of cybersecurity education through gamification. 2016 ASEE Annual Conference & Exposition; 2016.

[48] Coull N, Donald I, Ferguson I, Keane E, Mitchell T, Smith OV, et al., editors. The gamification of cybersecurity training. International Conference on Technologies for E-Learning and Digital Entertainment; 2017: Springer.

[49] Fink G, Best D, Manz D, Popovsky V, Endicott-Popovsky B, editors. Gamification for measuring cyber security situational awareness. International Conference on Augmented Cognition; 2013: Springer.

[50] Garcia JA, Sundara N, Tabor G, Gay VC, Leong TW, editors. Solitaire Fitness: Design of an asynchronous exergame for the elderly to enhance cognitive and physical ability. 2019 IEEE 7th International Conference on Serious Games and Applications for Health (SeGAH); 2019 5-7 Aug. 2019.

[51] Yasin A, Liu L, Li T, Wang J, Zowghi D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). Information and Software Technology. 2018;95:179-200.

[52] Hendrix M, Al-Sherbaz A, Victoria B. Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games. 2016;3(1):53-61.

[53] Le Compte A, Elizondo D, Watson T, editors. A renewed approach to serious games for cyber security. Cyber conflict: Architectures in cyberspace (CyCon), 2015 7th international conference on; 2015: IEEE.

[54] Maddux JE, Rogers RW. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology. 1983;19(5):469-79.

[55] Latour B. Science in action: How to follow scientists and engineers through society: Harvard university press; 1987.

[56] Liang H, Xue YL. Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the association for information systems. 2010;11(7):1.

[57] Latour B. On Recalling Ant. The Sociological Review. 1999;47(1_suppl):15-25.

[58] Mihelič A, Vrhovec S. A model of self-protection in the cyberspace. Elektrotehniski Vestnik/Electrotechnical Review. 2018;85(1-2):13-22.

[59] Solic K, Velki T, Galba T. Empirical study on ICT system's users' risky behavior and security awareness. Biljanovic P, Butkovic Z, Skala K, Mikac B, Cicin-Sain M, Sruk V, et al., editors2015. 1356-9 p.

[60] Bitton R, Finkelshtein A, Sidi L, Puzis R, Rokach L, Shabtai A. Taxonomy of mobile users' security awareness. Computers & Security. 2018;73:266-93.

[61] Li W, Yigitcanlar T, Erol I, Liu A. Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. Energy Research & Social Science. 2021;80:102211.

[62] Liebana-Cabanillas F, Munoz-Leiva F, Sanchez-Fernandez J. A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment. Service Business. 2018;12(1):25-64.

[63] van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P. Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior. 2017;75:547-59.

[64] Yen HY. Smart wearable devices as a psychological intervention for healthy lifestyle and quality of life: a randomized controlled trial. Qual Life Res. 2021;30(3):791-802.

[65] Li WY, Chiu FC, Zeng JK, Li YW, Huang SH, Yeh HC, et al. Mobile Health App With Social Media to Support Self-Management for Patients With Chronic Kidney Disease: Prospective Randomized Controlled Study. J Med Internet Res. 2020;22(12):e19452.

[66] Villani GQ, Villani A, Zanni A, Sticozzi C, Maceda DP, Rossi L, et al. Mobile health and implantable cardiac devices: Patients' expectations. Eur J Prev Cardiol. 2019;26(9):920-7.

[67] Chen CK, Tsai TH, Lin YC, Lin CC, Hsu SC, Chung CY, et al. Acceptance of different design exergames in elders. PLoS One. 2018;13(7):e0200185.

[68] Valenzuela JF, Monterola C, Tong VJC, Ng TP, Larbi A. Health and disease phenotyping in old age using a cluster network analysis. Sci Rep. 2017;7(1):15608.

[69] Chandler J, Sox L, Kellam K, Feder L, Nemeth L, Treiber F. Impact of a Culturally Tailored mHealth Medication Regimen Self-Management Program upon Blood Pressure among Hypertensive Hispanic Adults. Int J Environ Res Public Health. 2019;16(7).