DEVELOPMENT AND VALIDATION OF SCAM VICTIMISATION RISK INVENTORY (SVR-I) AMONG MALAYSIAN POPULATION

Wan Shahrazad Wan Sulaiman, Universiti Kebangsaan Malaysia
Fatin Adha Murad, Universiti Kebangsaan Malaysia
Geshina Ayu Mat Saat, Universiti Sains Malaysia, Malaysia
Rozainee Khairudin, Universiti Kebangsaan Malaysia
Daniella Maryam Mohamed Mokhtar, Universiti Kebangsaan Malaysia
Saralah Mariamdaran, Universiti Utara Malaysia
Azianura Hani Shaari, Universiti Kebangsaan Malaysia
Mohammad Rahim Kamaluddin, Universiti Kebangsaan Malaysia

ABSTRACT

An increasing number of people have fallen victim to scam resulting in loss of money and psychological trauma. This in turn affects the financial sustainability of the person. A number of studies have shown that the tendency to become victims of scams is related to lack of knowledge and awareness of cyber security as well as psychological predispositions. Therefore, this study aims to identify what are the risks involved among scam victims in Malaysia and hence, develop a Scam Victimisation Risk Inventory (SVR-I). This study was conducted using a cross-sectional survey in a two-phase study. Phase 1 was the pilot study and Phase II was the validation of the scale study. A total of 150 respondents participated in Phase I and another 150 respondents were involved in Phase II. The data were analysed using an Exploratory Factor Analysis (EFA) for Phase I and Confirmatory Factor Analysis (CFA) in Phase II. Results from EFA extracted three factors with satisfactory Eigen values and factor loadings. Further analyses with CFA validated the three-factor structure of the Scam Victimisation Risk Inventory (SVR-I). This study implies the importance of identifying dimensions of hasty-urgency, trustful of inaccurate information and risk-seeking as the risks for commercial scam victims. SVR-I is concluded as a valid and reliable measure to assess scam victimisation risk.

Keywords: Scam, Validation, Victimisation Risk, Scam Victimisation Risk Inventory, Financial Sustainability.

INTRODUCTION

In recent years, the extent and nature of scams can be viewed as perplexing and the prevalence is at an alarming rate. Scam victimisation is perceived as a constant threat to the public trust, confidence and has potential to erode the well-being of financial sustainability of an individual. Despite proactive efforts by government agencies and organizations to warn people

Citation Information: Sulaiman, W.S.W., Murad, F.A., Saat, G.A.M., Khairudin, R., Mokhtar, D.M.M., Mariamdaran, S., Shaari, A.H., & Kamaluddin, M.R. (2022). Development and validation of Scam Victimisation Risk Inventory (SVR-I) among Malaysian population. *Journal of Legal, Ethical and Regulatory Issues, 25*(S5), 1-15.

of the risks of being too trusting, incidents of scam victimisation continue to rise. Official statistics, news coverage and anecdotal accounts on social media depict the increasing prevalence of scam victimisation. Availability and accessibility to online commerce and relationship sites makes it increasingly easy for scammers to deceive individuals. Anonymity options, site design and products that appear to be legitimate, and user information disclosure; may also have contributed to the prolificacy of scam victimization.

Victimology and psychology researches have been applied to a range of behavioural issues including provocation and responses to violence and criminal victimisation. Models derived from victimology, psychology, or both together; provide mechanisms to explain pathways or engagement processes which underlie victimisation behaviours (Gainsbury, 2019; Mouton et al., 2016; Norris & Brookes, 2021; Williams et al., 2017). Other fields of study, for example criminology, information security, sociology, and economics have also explored the links between human agents and scam activities.

The available literatures provide some evidence for specific behaviours (for example impulsivity, negligence, gullibility, irresponsibility, too trusting), specific emotions (for example greed, desire, loneliness, attachment) and specific cognitions (for example failure to recognize deception cues, heuristics, low need for cognition) are more likely to be present in scam victimisation; despite awareness on the existence and extensiveness of such scams. Often, victims do not believe that they are vulnerable or susceptible until they experience victimisation. In many cases, victims underestimate their vulnerability to scams (Williams et al., 2017). According to Norris & Brookes (2021), the inability to detect fraudulent communications may be a factor underlying the victimisation experience itself.

Utilizing low self-control theory (Gottfredson & Hirschi, 1990) and Routine Activities Theory Mesch & Dodel (2018) opined that individuals with low self-control together with routine online activities; get involved in risk-taking behaviours that expose them to motivated cybercriminals, subsequently increasing their likelihood of victimisation. Mesch & Dodel (2018) further proposed that self-disclosure of personal information is another facet of victim culpability. Research on online self-disclosure of personal information is gaining popularity with research linking self-disclosure to gullibility (George et al., 2020; Mercier, 2017), anonymity (Clark-Gordon et al., 2019); social networking (Hallam & Zanella, 2017) and disinhibition (Green et al., 2016).

The psychology of a person could very much contribute to the susceptibility towards scam victimisation. As a person, the various traits or level of processing does provide a significant level of contribution to how far can the person be influenced by fraudsters. For instance, Murad et al. (2020) in their review found that personality traits such as neuroticism, openness, and agreeableness are prone to social influence. This is also affected by the amount of knowledge possessed by an individual, especially people of old age where a lack of knowledge regarding the risk factors in the financial exploitation of older people increases propensity for fraud (Jackson, 2017). The lack of adequate information would lead to compromised consideration that could inhibit cognitive decision-making processes. A report by the UK National Fraud Authority points out the victims for frauds being selected, their approach strategies and the details and profiles of the victims involved. The report highlights a few articles that signify the targeting of individual susceptibility being the key feature of many internet frauds (Button et al., 2014). An example would be the use of respond mechanisms with time limits to inhibit conscious processing. Other factors like risk taking and low self-control are additional personality traits that adds up to the general build of fraud victims (Deliema et al., 2020; Whitty, 2018).

Other than the victims' own actions, the available literature reports on outcomes of scam victimisation. Cross et al. (2016) provided some psychological distress experienced by research participants (80 face to face interviews) as a result of scam victimisation. Of those interviewed, victimisation experiences were described as *"devastating, soul-destroying, an event that changed [their] attitude to life"* (Cross et al., 2016). The range of negative emotional outcomes experienced persisted some time post-victimisation, and for some respondents, long-term trauma in the form of depression, attempted suicide, and negative coping mechanisms; were described (Cross et al., 2016). More recent research, for example Williams et al. (2017) and Gainsbury (2019); reinforce Cross et al. (2016) findings. Not only that, the consequence of becoming scam victims also lead to a decline in financial well-being which is associated with an increased probability of experiencing material hardship and struggling to make ends meet. This inevitably will impact on their sustainable development in terms of reducing poverty and hunger and ensuring good health and well-being.

With recent advancement in technology, online scam appears to have become the most common form of scams (Mesch & Dodel, 2018). Losses in terms of money and emotional trauma have been cited amongst victims (Cross et al., 2016; George et al., 2020; Pouryousefi & Frooman, 2019), yet continued rises of incidents have been reported; indicating the susceptibility of internet users and the lucrativeness of scams. A large number of studies have been devoted to study on various aspects of scam. For instance, the scope of studies on online scam victimisation within the last five years include: victim vulnerability and characteristics (Gainsbury, 2019; Norris & Brookes, 2021; Williams et al., 2017), online scamming techniques (Pouryousefi & Frooman, 2019; Wood et al., 2018; Chiluwa et al., 2017), instruments to measure experiences of online scams (George et al., 2020; Hamby et al., 2018; Mesch & Dodel, 2018; Whitty, 2019), and online scam detection systems (Chiluwa et al., 2017; Kharraz et al., 2018; Vinayakumar et al., 2018).

Cognizant of the worsening rates of crime victimisation and monetary loss, several researchers have developed instruments to measure risks and experiences of scams. Such instruments seek to better understand vulnerability issues, victim characteristics, evaluate risks, and determine scammer modus operandi; as ways to prevent future incidents. In the past five years, several instruments were developed and validated for meas-urement of risk. For example, Digital Online and Privacy Survey (Digital-OPS) by Hamby et al. (2018), Gullibility Scale (George et al., 2020), Susceptibility to Cyber-fraud Victimhood (Whitty, 2019), Susceptibility to Persuasion II (StP-II) (Modic et al., 2018), and Predicting susceptibility to cyber-fraud victimhood (Whitty, 2019). Yet whilst many have developed tools, there is no clear and specific tool to measure risk of scam victimisation in general. Such tools are vital for the purpose of monitoring, self-assessment and to relate with psychological factors that increases such risk of victimisation. Screening tendency to become scam victim using SVR-I is also highly recommended to ensure financial sustainability. Having said this, the present study aims to develop and validate a specific inventory to measure scam victimisation (henceforth, SVR-I) among Malaysian sample.

MATERIALS AND METHODS

A thoroughly validated protocols were employed in this current study in order to produce a valid and reliable measure of SVR-I. The items of SVR-I were developed based on interviews among selected sample of scam victims. Important aspects were extracted and were made it as a reference to develop items. All the items were content validated by three independent experts. An item-rating form and items of SVR-I were distributed to these experts to assess the relevance and representativeness in measuring risk of scam victimization. Based on their feedbacks, several amendments were made to items. Finally, the improved version of SVR-I were dis-tributed to a random sample of 30 Malaysian adults for the purpose of face validation. Here, the face validation was performed to identify language suitability and also wanted to know whether the questionnaire was easy to read, interpret and understand by the test takers.

Following this, validation study was commenced. This validation study was conducted using a quantitative cross-sectional survey in a two-phase study. Phase 1 was the pilot study and Phase II was the validation of the scale study. The Scam Victimisation Risk Inventory (SVR-I) was developed based on the in-depth interviews with scam victims (n = 14). The scale initially consists 38 items and employs a 5-point Likert from 1=Strongly Disagree, 2=Disagree, 3=Uncertain, 4=Agree and 5=Strongly Agree. Items such as I give my money to anyone who needs it (Q9) or People say I can be very naïve (Q24) were constructed to see how far hastiness and urgency element affects people to become victim. On the other hand, examples of items to measure trusting in false information are I am easily influenced by suspicious phone calls (Q31) and I usually give some time to hear to any threats or persuasion from unknown people (Q37). The inventory also measure financial risk-taking behaviour with items I do not miss out on discount opportunities when shopping online (Q5) and I usually assume people have good intentions in general (Q16). A higher score of the inventory indicates a higher risk of scam. A total of 150 respondents participated in Phase I and another 150 respondents were involved in Phase II. The data were analysed using Exploratory Factor Analysis (EFA) for Phase I and Confirmatory Factor Analysis (CFA) in Phase II. IBM SPSS 23.0 was used to analyse data in Phase I and Phase II.

RESULT

Exploratory Factor Analysis (EFA)

The data were analysed using Exploratory Factor Analysis (EFA) to explore the factor structure of the scale. Exploratory factor analysis is suitable to be used when there are no previous studies showing construct validity of a scale in the local context which is different than the culture in which the scale was developed (Pallant, 2007). A total of 38 items in the scale were analysed using Principal Component Analysis (PCA) with Varimax rotation. When PCA was conducted, the suitability of the data for analysis was first evaluated to determine that it fulfilled the requirements of factor analysis. Examination on the correlation matrix showed that all items have coefficient values of 0.30 and above (Pallant, 2007). So was the value of Kaiser-Meyer-Olkin (KMO) which was 0.851, exceeding the recommended value of 0.60 and Bartlett Test of

Citation Information: Sulaiman, W.S.W., Murad, F.A., Saat, G.A.M., Khairudin, R., Mokhtar, D.M.M., Mariamdaran, S., Shaari, A.H., & Kamaluddin, M.R. (2022). Development and validation of Scam Victimisation Risk Inventory (SVR-I) among Malaysian population. *Journal of Legal, Ethical and Regulatory Issues, 25*(S5), 1-15.

Sphericity was also significant (p<0.000), which supported the presence of factors in the correlation matrices (Dharmalingam et al., 2016).

However, the results of the first factor analysis did not extract a good factor structure because nine factors were extracted with 65.2 percentage of variance (PVE). Six of these factors were not distinct as the Eigen values and scree plot did not show unique factors. Next, communalities were examined to determine that items showed clarity to samples by ensuring that all values were above 0.30 (Pallant, 2007). After examining the communalities values, all items showed satisfactory values which were above 0.50. Therefore, the re-searchers conducted the second PCA with varimax rotation by fixing the extraction method to a fixed number of factors, which was fixing the factors into three factors as suggested by the Eigen values and scree plot.

The results of the revised EFA model showed findings with correlation matrix of all items having coefficient values of 0.30 and above (Pallant, 2007). So was the value of Kaiser-Meyer-Olkin (KMO) which was 0.868, exceeding the recommended value of 0.60 and Bartlett Test of Sphericity was also significant (p<0.000), which supported the presence of factors in the correlation matrices.

PCA has extracted three factors with good Eigen values which were 7.70 for Factor 1, 5.06 for Factor 2, and 3.48 for Factor 3. The percentage of variance explained (PVE) for the three factors also showed good results with PVE 21.99% for Factor 1, 14.46% for Factor 2, and 9.94% for Factor 3 with a total percentage of the variance of 46.39%. The values of factor loading for each item were checked to ensure that they fulfilled the minimum requirement of 0.30. All items were found to have good loadings. Factor loading for each item was then analysed to determine which factor it belongs to with factor loading values exceeding 0.30 as shown in Table 1. The analysis showed that Factor 1 consisted of 18 items, Factor 2 has 6 items, and Factor 3 has 10 items. Four items (Q2, Q14, Q20 and Q32) were eliminated due to poor factor loadings. According to the requirement of factor analysis, a factor can only be accepted if it consists of at least 3 items. Hence, these three factors can be accepted as each factor consists of sufficient items.

Table 1
RESULTS OF FACTOR ANALYSIS

Item	**Factor Loading**		
	11	**22**	**33**
Factor 1=Hasty-urgency; Eigen value=7.70; PVE=21.99%			
Q1 I make financial decisions based on my intentions.	0.476		
Q4 I have been told that I am a gullible person.	0.612		
Q6 I will act quickly so that I do not miss any opportunities.	0.532		
Q7 I am attracted to offers, gifts or discounts given by others.	0.511		
Q9 I give my money to anyone who needs it.	0.571		
Q10 I am easily manipulated.	0.731		
Q11 I am hasty when making decisions regarding money or finances.	0.578		
Q12 I cannot think clearly when under pressure.	0.647		
Q13 I am easily influenced by others.	0.763		
Q15 I do not like to ask many questions.	0.637		
Q17 I am easily deceived by praises.	0.556		
Q18 My decision-making process is influenced by others.	0.696		
Q19 People can easily control my actions.	0.756		

Citation Information: Sulaiman, W.S.W., Murad, F.A., Saat, G.A.M., Khairudin, R., Mokhtar, D.M.M., Mariamdaran, S., Shaari, A.H., & Kamaluddin, M.R. (2022). Development and validation of Scam Victimisation Risk Inventory (SVR-I) among Malaysian population. *Journal of Legal, Ethical and Regulatory Issues, 25*(S5), 1-15.

Q22 I give my money to others without questioning much.	0.659		
Q23 I perceive asking too many questions as rude.	0.672		
Q24 People say I can be very naïve.	0.511		
Q26 I do not take a long time to make a decision.	0.469		
Q30 I am easily deceived by others.	0.624		
Factor 2=Trustful in inaccurate information; Eigen value=5.06; PVE=14.46%			
Q31 I am easily influenced by suspicious phone calls.		0.765	
Q33 I am influenced by fake official calls.		0.745	
Q34 I am easily influenced by messages regarding transactions and funds transfer.		0.786	
Q35 I provide personal information to unknown people.		0.766	
Q36 I easily believe personal information provided by unknown people.		0.748	
Q37 I usually give some time to hear to any threats or persuasion from unknown people.		0.471	
Factor 3=Risk seeking; Eigen value=3.48; PVE=9.94%			
Q3 I panic after receiving unexpected news.			0.504
Q5 I do not miss out on discount opportunities when shopping online.			0.484
Q8 I usually take risks in financial decisions.			0.463
Q16 I usually assume people have good intentions in general.			0.363
Q21 I have trouble refusing when someone wishes to borrow my money			0.397
Q25 I get excited with new things.			0.751
Q27 I am willing to do anything during financial shortage.			0.370
Q28 I am always willing to try new things in my life.			0.679
Q29 I desire to become rich fast.			0.728
Q38 I am excited to do things that profit me.			0.389

Confirmatory Factor Analysis (CFA)

Confirmatory factor analysis (CFA) was employed to test how well the measured variables represent the constructs. With CFA, the researcher must specify both the number of factors that exist within a set of variables and which factor each variable will load highly on before results can be computed. The goodness of fit of the measurement models was evaluated using six indices, which reflected the overall model fit: (1) the chi-square statistic; (2) the minimum value of the discrepancy between the observed data and the hypothesized model divided by degrees of freedom (CMIN/DF); (3) the goodness-of-fit index (GFI); and (6) the root mean-square error of approximation (RMSEA). Arbuckle and Wothke (1999) stated that first, the CMIN/df with a value of less than 5 is considered acceptable. Second, the possible values of GFI range from 0 to 1, with values close to 1 demonstrating a good fit. Finally, a value of RMSEA of 0.08 or less shows a reasonable error of estimation.

Results of the assessment of normality for SVR-I showed no violations of normality. The distribution of scores for all 34 items in the inventory showed acceptable skewness within |3.0| and kurtosis in the range of |10.0|. The results (Figure 1) showed that the model $\chi^2(524)=1080.88$, $p<0.0001$, indicating poor fit. The χ^2 statistic is the most conventional indicator which represents the size of the discrepancy between the sample and the model with a non-significant χ^2 value indicating good fit. However, the value of CMIN/df was 2.06 was considered acceptable. The values of other goodness-of-fit indices also showed unacceptable values which were below 0.90. In addition, the value of RMSEA was 0.084 also did not fulfil the recommended value. Therefore, this showed that the SVR-I has poor fit between the model and the data. Therefore, this measurement model needed to be revised.

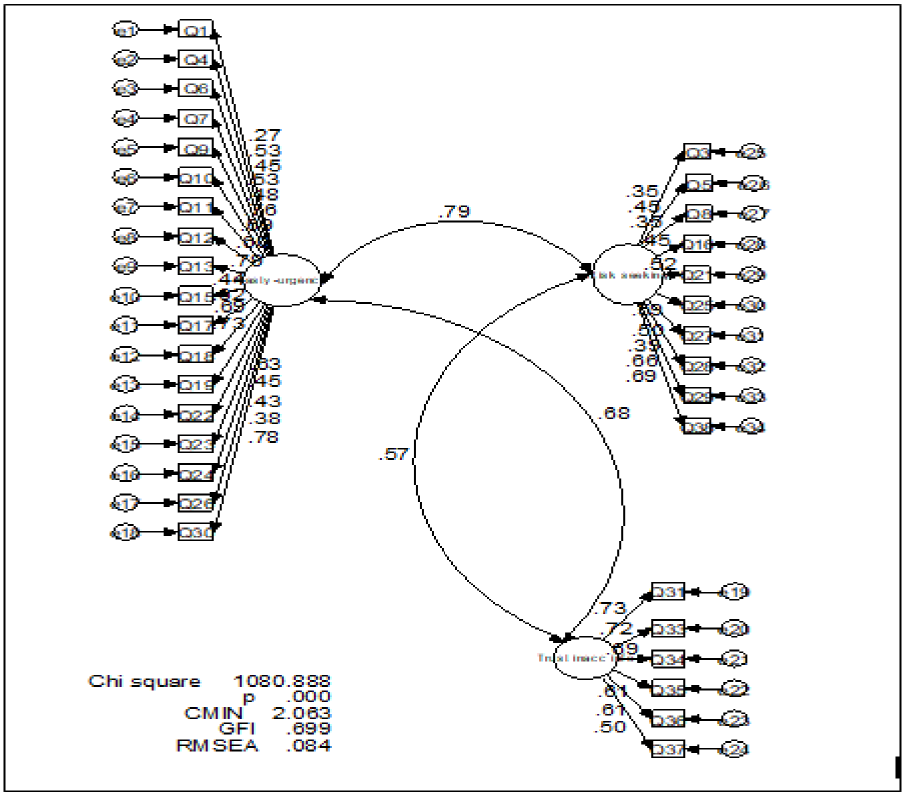

FIGURE 1
MEASUREMENT MODEL OF SVR-I

The measurement model was revised by examining the modification indices. Apart from that, it is suggested that all factor loadings should have values of 0.30 and above and statistically significant. Using modification indices and factor loading values, 20 items were eliminated to achieve a good fit model. A total of six items were retained for Hasty-urgency dimension which were Q11, Q12, Q17, Q22, Q24 and Q30. Dimension 2 which was Trustful of inaccurate information consisted of four items which were Q33, Q34, Q36 and Q37. The last dimension, Risk-seeking on the other hand consisted of four items which were Q5, Q16, Q25 and Q27. The model was analysed again using 14 items.

The results of the revised model (Figure 2) showed that the model χ^2 (72)=11.07, p< 0.001. However, looking at other indices showed that the RCFV-I has acceptable goodness-of-fit between the model and the data. The model has adequate fit indices of a good model according to CMIN/df=1.61. The goodness-of-fit indices showed acceptable values of GFI=0.90. The value of RMSEA was 0.065 which also fulfilled the conventional standard of a good fit. In addition, the correlation between the three dimensions showed moderate correlations indicating subscales measuring three different dimensions. In addition, alpha Cronbach of the 14-item RCFV-I yielded acceptable reliability of 0.797 for Hasty-urgency dimension, 0.744 for Trustful with inaccurate information, 0.474 for Risk Seeking and 0.846 for the total items.

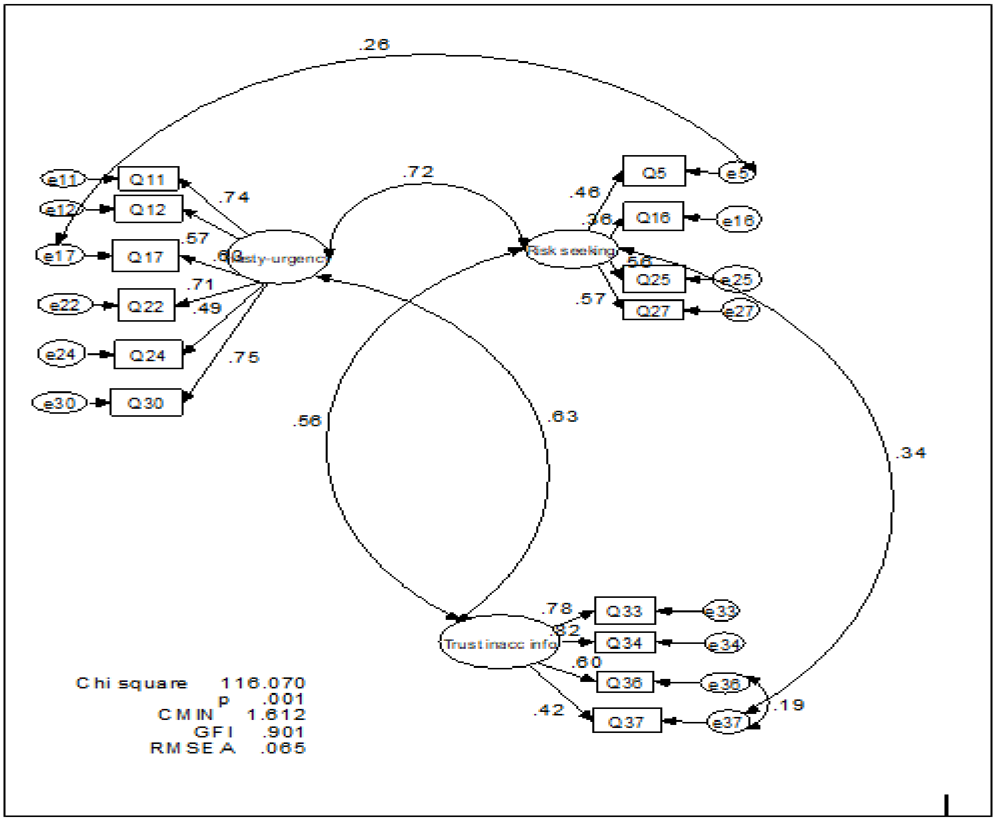

FIGURE 2
REVISED MEASUREMENT MODEL OF RCFV-I

DISCUSSION

Series of interview with participants who had been victims in various types of scams. Based on the interview, the researchers developed items that make up the inventory. Overall, the goodness of fit of SVR-I was acceptable. From the confirmatory factor analysis conducted, three factors to measure scam risk victimisation were identified: hastiness-urgency, trustful in inaccurate in-formation and risk-seeking behaviour. The Cronbach alphas of each of the factors make a good reliability, ranging between 0.47 and 0.79.

An extension of past literature show that scam risk victimisation could vary from individuals' sociodemographic background such as age, gender or education (Beals et al., 2017; Saad & Abdullah, 2018; Whitty & Buchanan, 2012). However, Button et al. (2014) explains that lack of knowledge and awareness could be one of many reasons why people fall victims. On the other hand, Cross & Kelly (2016) stressed that prevention through education and awareness are not always effective as person who are aware of the crime can also be deceived by criminals. It is because the messages that are used by the criminals are more important to be highlighted and considered in prevention steps. Following this, current research found three factors to explain why people are deceived by scams.

Fraudulent activities have been on the rise, with criminals using different methods to gain their victims from time to time. Since the dawn of the internet and technology, criminals are able to gain victims without going out and meeting them such in online romance scam or Macau scam. The evolvement of the internet has been a great asset to scammers who depend on social networking sites (Facebook, Instagram, Twitter, Whatsapp, etc.) to commit acts of fraud (Blanton, 2012). These scammers are generally anonymous and difficult to identify and recognise as they constantly alter their disguises. Tan, et al. (2017) state that users undertake false identities to engage in deceptive communication due to the anonymity provided by the Internet. They usually crack into individuals’ bank, credit card or other accounts through a certain procedure and use the account holders’ money to carry out transactions or even invest without their authority. In general, victims of commercial crimes such as scams lost large amounts of money. However, they are also silently suffering from psychological damages that are not highlighted by media reports. While Whitty & Buchanan (2012) stated that non-financial victims, too, were affected by online romance scam, Cross (2018) also found out that victims tend to develop cognitive distortion and blame themselves for being victims. Victims also may experience prolonged psychological distress and some may develop cognitive distortion such as self-blaming, hopelessness, helplessness and preoccupation with danger (Zamani et al., 2014). In a study, findings also showed that scam victims experienced negative emotional effects and this occurs in high frequency among social media users. In some extreme degree, victims consider suicide as the scam caused them to lose their savings, jobs and homes and they are ashamed and sad (Button et al., 2009). These are circumstances in which victims do not have sustainability in maintaining their mental health and financial well-being which is strongly related to the level of poverty in a society (Griggs, 2013) as well as to the economic growth of a society.

The reasons to how scams could occur are highly subjective but in general, most scam victims are found to be generally gullible, hasty, and heedless or reckless. It is often perceived that the elderly people are more susceptible to scam or fraud due to their lack of general awareness and their tendency to believe anything plausible. An article by the Citizens Advice Scotland (2014) however states that scam victimisation is for every person and not only the elderly. This is consistent with Button et al. (2009) study who concluded that “*the profiles of victims cover almost everybody; hence almost anyone could become the victim of a scam*”. The article revealed that adults of 30-40 years of age are more prone to scams in general but people under the age of 25 are also potential victims to online scams which have become a norm in recent times. This study was conducted to identify the potential risks of victimisation among scam victims. There are many tools and systems that measure the causes of scams, and how are victims formed. However, this study aims to concentrate on victims as a whole and evaluate them based on their traits. The tool created would be able to analyse and evaluate victims based on how susceptible they are to scams, and the perk of this study is that victims could self-evaluate themselves to be extra cautious in possible encounters thereafter.

Based on this study, the inventory created for analysing the risk of victimisation focuses on three main factors on why people are prone to be victims of scams. These factors were determined from a preliminary interview of 14 scam victims, and later on affirmed through a cross-sectional survey in a two-phase study. Hastiness or urgency is a common factor that leads to scam victimisation due to the lack of time spent for proper analysis and consideration. Usually, people who are hasty and reckless when making decisions are prone to phishing, a scam involving a scammer impersonating a trustworthy third party that creates a vague situation for users. According to Naidoo (2015), phishing uses influence cues such as hastiness and urgency to encourage increased information processing. This is achieved by short circuiting a targeted user's comprehension, his/her mental resources and preventing that person from picking out the minor detail that separates the impersonator from the true party, thus leading to deception.

As for urgency, scammers take advantage of the psychological nature of people who have an obsessive compulsion to not miss out on limited opportunities. The advancement of technology has established the compulsory use of mobile and handheld devices which created the general expectation that users should be more active in responding to emails (Vacek, 2014). He also stated in his study that 37.5% of users attempt to check and reply their emails immediately and 56% try to at least reply on the same day. According to a psychological reactance theory, people usually want things that are limited, scarce or rare and serve their competitive needs (Cialdini, 2001; Workman, 2007). Scammers profit from this psychological flaw, where a phishing email is constructed to create a pressured situation for users with a time limit or deadline. Phishing designs are capable of arousing strong emotions based on the principle of scarcity where people tend to be motivated more by the idea of something slipping away rather than gaining something equal in value (Cialdini, 2001).

Scammers would use emotion-inducing in their messages to get attention from their potential victims. For example, messages laced with fear often state the consequences if their victims unable to comply (e.g. losing money, legal action and deadlines) (Norris & Brookes, 2021). Some scammers go an extra mile by mentioning penalties or losses if the user does not respond to the email or link within a certain time period. The whole purpose of this gesture is to scare or intimidate the user into acting promptly instead of carefully contemplating and evaluating the content of the email received (Naidoo, 2015). Fraudulent activities through email are further encouraged when marketers from companies use email as a medium to increase their sales, thus causing information overload (Andersson et al., 2014). Scammers would do well to camouflage among these emails and users would not be able to tell the difference in desperate or rushed circumstances. Targeted users are usually people or companies that have extended working hours, or a lot on their plate which prevents them from spending a lot of time reading and understanding emails. Scammers use these flaws to their advantage and add elements of attraction to further speed up the process. A common example is rewards, intensives or promotions. These programs habituate customers into the need for upgrading their perceived status as according to them, it is an essential investment that provides tangible financial benefits or any privilege (Naidoo, 2015). From an overall perspective, it could be clearly stated that hastiness and urgency are a significant factor in promoting scam victimisation.

Another factor that causes scam victimisation is trusting false resources or in shorter terms, blind trust. Just like urgency and hastiness, blindly trusting any resource could also lead to scam victimisation. The ever-expanding trait of technology has led scammers to be greatly innovative in contrasting tactics that trap more users. The likeliness to spot a difference between scam and verified emails/messages/links is very low given the creativity of scammers who continuously improve and update themselves with newer tactics. Despite the numerous efforts initiated to curb scams victimisation, unsuspecting customers are repeatedly deceived with similar schemes due to the failure of realizing and identifying infinitely creative scammers, all who make users, believe in new, lucrative and unique offers (Blanton, 2012). Norris et al. (2019) described how users are constantly drawn to the persuasive influence of scam messages sent by fraudsters. The trust builds from situations where users are desperate or in a situation that require immediate solutions. Scammers use this as an advantage when they position themselves as someone from an organization or agency and offer a solution, product or opportunity that would solve that particular problem, or in some cases even bring profit (Blanton, 2012).

This is supported by several studies that showed the most common strategy employed is by disguising as a person of authority to deceive their victim (Button et al., 2014; Shaari et al., 2019; Williams et al., 2017). Deb & Segupta (2020) also found that perpetrators appeared to be as someone who can be trusted or pretend to be someone of authority such as police officer or custom officer before they take advantage on their victims. Victims of pyramid scheme who lack education and live in poverty often become their targets after believing that their investment would bring higher returns. Emotionality also plays a part in this situation. Being gullible, stemmed with higher emotionality (i.e. anxiety, fearfulness, and emotional reactivity) explains why a person would fall a victim (George et al., 2020).

Any user in general is more likely to interact and respond frequently with bank or financial experts and hence build trust and identify strongly with the bank and personal financial services over time (Vishwanath et al., 2011). In cases of making decisions regarding the bank, users tend to overlook minute details and rely on heuristics to make them, and due to a dependence on past experience and affiliation, these users are easy targets to fraudsters who impersonate as legitimate bank officers. Although detectable through thorough observations, scam is still a large problem due to fraudsters who spend a lot of time building their identities by using suitable phrases and words that establish a form of trust within users. Trust language, or words opted to convey a sense of mutual reliance between a user and the scammer is very capable of captivating the thoughts of scam victims (Rich, 2018). An article by Consumers International (2019) stated that scammers are very likely to aim or focus on specific demographic groups to increase the probability of their success. A good instance would be the UK Trading Standards reporting young men being the most likely to be scammed with products involving steroids and middle-aged women are more susceptible to ones involving diet pills. Although trusting suspicious or malicious emails, links or messages are less likely in situations where users are less hasty, the innovations made to strengthen fraudulent activities make it possible for even careful, observant users to be targets of scams.

The third factor identified in this study is risk seeking. The internet has made is possible for users to have almost everything at their fingertips. Users could seek for information, shop, and communicate in a really short time and this feature carries a truckload of advantages, especially when it comes to saving time. However, with the incredibly short time required to carry out these activities compared to doing it in real time, comes the immense risk of being susceptible to fraudulent activities. Many users overlook the risk of facing potential, fraudulent activities when dealing with online activities such as shopping and other forms of transaction. This occurs more frequently among the elderly as they lack the sufficient information regarding scams and frauds (Toms, 2015). Large companies or investors are often open to risks when constructing models or synthesising methods for further profit. The lack of adequate consideration which leads to taking up unnecessary risks is a large contributing factor to scam victimisation. In addition, Deliema et al. (2020) identify that males are more likely to take risk in investment. This is probably due to the motivation to get higher profit return without realising that they have been duped. An article by Dhami & Mandel (2012) found that risk taking behaviour is very much connected to a limited rationality perspective where it is associated with a person's focus on the perceived benefits of being involved in risky actions or behaviours. This trait could be associated with scam victimisation as targeted users usually lack enough perspective to identify the severity of consequences from scams, thus proceeding without caution.

The ability of a person to comprehend the idea behind online dealership rests on rationality. In the process of identifying and evaluating risks, a person's rationality plays the key role in considering the pros and cons of a decision, and it that case, rationality in general is influenced by external limitations such as time constraints, available information and resources, and internal limitations such as a limited ability of cognitive processing abilities (Dhami & Mandel, 2012). Fraudsters are smart enough to identify methods that could trigger a sense of interest, hastiness and desperation. Obvious scam techniques are outdated and today, users susceptible to scams are not even aware of the risks they took. Scam victims are reported to engage in various online activities compared to non-victims, clicking on pop-up ads, opening and acting on emails from unknown resources, buying and selling merchandise online, signing up for trials and offers, downloading apps and replying to random strangers. Though not entirely or necessarily cause victimisation, these activities create an increased exposure to scammers, thus increasing the chances of becoming a victim (Shadel et al., 2014). A risk in victimisation is highly probable but subjective and depends on other factors such as hastiness and limitations. However, prior to making a decision, one should remember to consider the consequences at stake prior to making decisions, especially when it involves activities online.

CONCLUSION

Scam victimisation is a highly subjective matter given the endless possibility of how a person could be labelled susceptible to being a victim. In this study, a few possibilities are reviewed and analysed based on Confirmatory Factor Analysis and three factors that cause scam victimisation are hastiness or urgency, blind trust for false resources and people's tendency to take risks. Though these factors could be prevented from thorough analysis, observation and careful contemplation and consideration prior to making decisions, recent advancements have made it marginally impossible to completely eliminate the possibility of a user being prone to even a small scam. The unlimited access to technology not only provides opportunities for modernization, but also opens the door to unethical acts which could be executed through easier methods with more to absolute anonymity. As a user, consumer or a general person in an era of rapid technological advancement, understanding the factors that lead up to scam victimisation is very important.

With the seriousness of scams in mind, the researchers realised that it is important to have an instrument that can predict its victimisation. Past works of literature show how commercial crimes (scams) operated, who their victims are, how much are the loss and why people from different background can be victims. However, instruments that are capable to measure risk victimisation are still limited. Thus, the inventory was developed and tested. Three main factors were found that underlies within the inventory which hopefully would shed light to understand why people can fall victims. It is important to understand the victimisation factors so that relevant interventions or prevention steps can be taken in order to fight commercial crimes like scams. Findings of the study show that SVR-I am valid and reliable using samples of subjects in Malaysia thus can be used within Malaysian population. SVR-I hopefully would become a pioneer for future researches regarding to scams.

Previous studies have highlighted these factors but have not provided optimum solutions to how a person could self-evaluate to prevent them from indulging into fraudulent activities or scams without them knowing. This study aimed to allow users to analyse themselves based on three factors that were determined to be the cause for scam victimisation, and after that, users would identify their traits and hence, could be more conscious of their actions and act accordingly. Therefore, through this study, users would prepare themselves to face any possible fraudulent activity and reduce their susceptibility to being victims of scams.

FUNDING

This present study was funded by Fundamental Research Grant Scheme (FRGS) by The Ministry of Education (Malaysia) [code: FRGS/1/2018/SS06/UKM/02/1].

REFERENCES

Andersson, M., Fredriksson, M., & Berndt, A. (2014). Open or delete: Decision-makers' attitudes toward e-mail marketing messages. *Advances in Social Sciences Research Journal*, *1*(3), 133-144.

Arbuckle, J.L., & Wothke, W. (1999). *Amos 4.0 user's guide, small waters corporation.* Chicago, IL.

Beals, M.E., Carr, D.C., Mottola, G.R., Deevy, M.J., & Carstensen, L.L. (2017). How does survey context impact self-reported fraud victimization? *The Gerontologist*, *57*(2), 329-340.

Blanton, K. (2012). *The rise of financial fraud: Scams never change but disguises do*. Center for Retirement Research working paper.

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud*. National Fraud Authority: London.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391-408.

Chiluwa, I.M., Chiluwa, I., & Ajiboye, E. (2017). *Online deception: A discourse study of email business scams*.

Cialdini, R.B. (2001). *Influence: Science and practice*. Massachusetts: Pearson Education.

Clark-Gordon, C.V., Bowman, N.D., Goodboy, A.K., & Wright, A. (2019). Anonymity and online self-disclosure: A meta-analysis. *Communication Reports, 32*(2), 98-111.

Consumers International. (2019). *Social media scams: Understanding the consumer experience to create a safer digital world.*

Cross, C. (2018). (Mis) Understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, *13*(6), 757-776.

Cross, C., & Kelly, M. (2016). The problem of white noise: Examining current prevention approaches to online fraud. *Journal of Financial Crime*, *23*(4), 806-818.

Cross, C., Richards, K., & Smith, R.G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *5*(18), 1-14.

Deb, S., & Sengupta, S. (2020). What makes the base of the pyramid susceptible to investment fraud. *Journal of Financial Crime, 27*(1), 143-154.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research, 46*(5), 904-914.

Dhami, M.K., & Mandel, D.R. (2012). Crime as risk taking. *Psychology, Crime & Law*, *18*(4), 389-403.

Citation Information: Sulaiman, W.S.W., Murad, F.A., Saat, G.A.M., Khairudin, R., Mokhtar, D.M.M., Mariamdaran, S., Shaari, A.H., & Kamaluddin, M.R. (2022). Development and validation of Scam Victimisation Risk Inventory (SVR-I) among Malaysian population. *Journal of Legal, Ethical and Regulatory Issues, 25*(S5), 1-15.

Dharmalingam, T. K., Kamaluddin, M. R., & Hassan, S. K. (2016). Factorial validation and psychometric properties establishment of Malay version critical care family need inventory. *IIUM Medical Journal Malaysia*, *15*(1), 1-9.

Gainsbury, S.M. (2019). Identifying risky internet use: Linking negative internet experiences to specific online behaviour. *New Media and Society*, *21*(6), 12-32.

George, M.S., Teunisse, A.K., & Case, T.I. (2020). Gotcha! Behavioural validation of the gullibility scale. *Personality and Individual Differences*, *162*(1), 110-134.

Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Green, T., Wilhelmsen, T., Wilmots, E., Dodd, B., & Quinn, S. (2016). Social anxiety attributes of online communication and self-disclosure across private and public Facebook communication. *Computers in Human Behavior*, *58*(1), 206-213.

Griggs, D. (2013). Sustainable development goals for people and planet. *Nature*, *495*(2), 305–307.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*(2), 217-227.

Hamby, S., Taylor, E., Jones, L., Mitchell, K.J., Turner, H.A., & Newlin, C. (2018). From poly-victimization to poly-strengths: Understanding the web of violence can transform research on youth violence and illuminate the path to prevention and resilience. *Journal of Interpersonal Violence*, *33*(5), 719-739.

Jackson, S.L. (2017). Senate special committee on aging hearings and GAO reports. *Elder abuse: research, practice, and policy. Springer, New York*, 595-613.

Kharraz, A., Robertson, W., & Kirda, E. (2018). Protecting against ransom ware: A new line of research or restating classic ideas?. *IEEE Security & Privacy*, *16*(3), 103-107.

Mercier, H. (2017). How gullible are we? A review of the evidence from psychology and social science. *Review of General Psychology*, *21*(2), 103-122.

Mesch, G.S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356-1371.

Modic, D., Anderson, R., & Palomäki, J. (2018). We will make you like our research: The development of a susceptibility-to-persuasion scale. *PloS one*, *13*(3), 194-219.

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*(2), 186-209.

Murad, F.A., Kamaluddin, M.R., Sulaiman, W.S.W., & Khairudin, A.H.S. (2020). Personality and low self-control as contributing factors for scam victimization: A concept paper. *International Journal of Psychosocial Rehabilitation*, *24*(2), 4448–4461.

Naidoo, R. (2015). Analysing urgency and trust cues exploited in phishing scam designs. In *10th International Conference on Cyber Warfare and Security*.

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, *169*(1), 109-847.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Pallant, J. (2007). *SPSS survival manual - A step by step guide to data analysis using SPSS for windows*. Open University Press: Maidenhead.

Pouryousefi, S., & Frooman, J. (2019). The consumer scam: an agency-theoretic approach. *Journal of Business Ethics*, *154*(1), 1-12.

Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, *31*(1), 208-225.

Saad, M.E., & Abdullah, S.N.H.S. (2018). Victimization analysis based on routine activity theory for cyber-love scam in Malaysia. In *2018 Cyber Resilience Conference (CRC)*.

Scotland, C.A. (2014). *The impact of fraudsters: Scammed and dangerous.*

Shaari, A. H., Kamaluddin, M. R., Paizi, W. F., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1), 1-9.

Shadel, D., Pak, K., & Sauer, J. (2014). *Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim.*

Toms, S. (2015). Fraud and financial scandals: A historical analysis of opportunity and impediment. *Leeds University Business School Working Paper*.

Vacek, M. (2014). How to survive email. In *2014 IEEE 9th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI)*.

Vinayakumar, R., Poornachandran, P., & Soman, K. P. (2018). Scalable framework for cyber threat situational awareness based on domain name systems data analysis. In *Big data in engineering applications*. Springer, Singapore.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, *21*(2), 105-109.

Whitty, M.T. (2019). Who can spot an online romance scam? *Journal of Financial Crime*, *26*(2), 623-633.

Whitty, M.T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*(1), 412-421.

Wood, S., Liu, P. J., Hanoch, Y., Xi, P. M., & Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied*, *24*(2), 196-210.

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

Zamani, Z. A., Nasir, R., Desa, A., Khairudin, R., & Yusooff, F. (2014). Family functioning, cognitive distortion and resilience among clients under treatment in drug rehabilitation centres in Malaysia. *Procedia-Social and Behavioral Sciences*, *140*(2), 150-154.

Received: 06-Oct-2021, Manuscript No. JLERI-21-8715; **Editor assigned:** 08-Oct-2021, PreQC No. JLERI-21-8715(PQ); **Reviewed:** 22-Oct-2021, QC No. JLERI-21-8715; **Revised:** 22-Feb-2022, Manuscript No. JLERI-21-8630(R); **Published:** 01-Mar-2022