Copyright © 2022 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2022. Vol. 16(1): 40–53. DOI: 10.5281/zenodo.4766555
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

This is a Diamond Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cybercrime Risk Fear Among University Students' Social Networking Sites: Validity and Reliability

Abdulnaser A. Fakhrou[1], Taha Rabie Adawi[2]
Qatar University

Mahmoud Ali Moussa[3]
Suez Cannel University

Abstract

Social networking sites and other media applications have been admitted as compulsive communication outlets. Their vulnerability and various risks involved, these social media platforms are easy sources to commit cybercrimes. The main purpose of this study was to test the structure of fear of cybercrime among users of social networks. The sample consisted of 612 university students who used social networking sites. The snowball sampling technique was used to drive sample of the study. The study utilized a descriptive approach. An electronic Google form comprising 15 items with a focus on fear of crime was administered after taking students' informed consent. MPLUS and IBM SPSS were used to analyze data. The study tested three models of scale structure including the exploratory factor analysis to generate models. These models were then verified by confirmatory factor analysis. The three-factor model excelled exploratory and confirmatory in terms of goodness-of-fit indicators. The study recommends applying the scale with caution in future because of the low variance explained by using the scale, which reached 30.7%.

Keywords: cybercrime fears; Cybercrime anxiety.

Introduction

Social media and various networking applications have penetrated into human lives so deeply that they often act as compulsive communication outlets. Owing to their vulnerability and various risks involved, however, these social media platforms are also subjected to cyber threats like cyberbullying, malware, phishing attacks, identity theft, and scams. As a result, there is an overwhelming fear of social media among masses that they always correlate internet application and other websites as sites of crime and every individual as a hacker (Covington & Taylor, 1991; Intravia et

[1] Qatar University – afakhrou@qu.edu.qa
[2] Corresponding: Qatar University – tadawi@qu.edu.qa
[3] Suez Cannel University - mahmoud_muhanna@edu.suez.edu.eg

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

al., 2017). In the recent times, social networking sites although provide the user with the pleasure and satisfaction of various cognitive, emotional, and inspiration motives. It was the justification for the use of social networking sites seekers with low levels of ego to satisfy confined passions, discharge emotional strength resulting from constraint and frustrations in the achievement of dreams and ambitions.

The increasing demand on the Internet and communication networks explains the suspense and excitement that saturates users and satisfies their psychological, emotional, and social needs. It is considered an outlet for their emotions, which is difficult for them to show or to satisfy in the authentic context because of the social restrictions and norms. In such a state, users cannot withdraw or violate their harmony and control so as not to be stigmatized as an exception. Due to the melting of the spatial, temporal, and cultural barriers between all societies, it was desirable for those common interests and professional, psychological, and emotional interests to communicate in any available authentic context. This integration occurs by joining into groups or through their stories and frequent times log on their pages. Thus, the individual has feedback considering the integration of cultures over time.

Due to the previous features achieved, social networks can increase long periods of usage, negatively affecting the family, social, academic, and professional aspects. The individual becomes victim to the negative symptoms that result from overuse. The individual turns to restricted use in response to depression and psychological loneliness to which he is exposed. The individual seeks mood compensation and tries to get freed of psychological conflict situations.

There is scientific evidence confirming that Internet addiction may be a cause of cybercrime. Oskenbay et al. (2015) and Suler (2004) have shown that usage as chat rooms, news and internet searches, also scientific research does not exceed 2%, and the remaining percentage was between different sites. The social media addiction phenomenon gives rise to new behavior species as cyber-behaviors, Cyber extortion, Cyber-blackmail, Cyber-harassment, Cyber-smearing, Cyberstalking, and Cyber-teasing. Gambling addiction, cybersex or pornography addiction, and cyber-relationships addiction help us draw the motivation classification that manifests a comprehensive solution to reduce cybercrime (Aiken, 2017; Mishra et al., 2014). It is also feared that dwelling too much on cyber behaviors in some directions generates narcissism, ego expansion, self-image enhancement, and even the individual's tendency to self-absorption.

Owing to the increased use of social media and the paranoia that emanates on users fearing their being victimized by cybercrime, it was necessary to examine what builds this structure of fear of cybercrime among users of social networking sites and what models can be designed to build a structure. The current research, therefore, attempted to assess the fear of criminal victimization due to social media by adopting an integrated risk interpretation model on a sample of 612 male and female university students of Arab background. The study also accounted for various other factors of traditional fear of cybercrime victimization and attempted the construction of a cybercrime fear scale for the social network users. With the help of three exploratory models: the general factor model, the two factors model, and the three factors model, this study used verified its findings with exploratory models using CFA.

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Theoretical framework

The study chiefly attempted to build a risk interpretation model to evaluate the current state of crime fear interpretation that combines both the individual and community characteristics. This risk interpretation model considered that individuals perceived the risk of deception based on their personal and societal characteristics as well as basic determinants of fear of crime (Lee et al., 2019). The model indicates that individual factors of cybercrime are related to routine activities or lifestyle characteristics. These factors involve individuals in dangerous activities, excluding them from their home without shelter, carrying valuables, or photographing them in prohibited places (Wilcox, Quisenberry, & Jones, 2003). The model includes community-level effects on social cohesion, social and religious turmoil, and the nature of adolescent education.

Lee et al. (2019) assert that a major risk arises from the measure indicating fear of the environmental factors of security aspects and special education programs such as developing the context of the surrounding area. The victim's experiences and social disruption factors in the social context increases the risk of deception victimization, which increases fear of crime Ferguson and Mindel (2007) also believed that sex, age, and previous victimization experiences do not affect fear of the crime. The distress to which society and the community are exposed directly or indirectly affects the fear of crime. The higher the level of awareness associates with less level of perceived risk and fear. Conversely, strong ethnicity may be associated with loneliness within a group and suspicion of strangers. Thus, it may enhance perceived danger and fear (Rojas, 2020).

The risk interpretation model became the basic foundation of this study which aimed at determining the dimensions of the phenomenon of awareness of cybercrime, cybercrime anxiety, and fear of cybercrime. This model was assisted by two other models: General factor model and two factor structure model. The General factor model, as postulated in Bouchard and Morselli (2014), confirms the existence of such general factor items that could be considered as the anxious immersion of electronic texts on payment systems and social contexts. These items are referred as emotions that catch the individual's paranoia and fear of being victimized to internet application. Similarly, Yaghoobi et al. (2016) found that anxious attachment pattern is a positive predictor of fear cybercrime. Alshalan and Al-Khalifa (2020) also supported the general factor in fear of cybercrime and classified cybercrimes as internet extortion, loss of security, and hacking.

The second model, two factor structure model, comprises awareness and experience as two different aspects to examine cybercrimes. The awareness factor is the behavior of the individual towards online payments after hearing news of fraud, theft, and electronic cheating, while experience is associated with external factors like commercial blackmail, allurement, or polarization, or the exploitation of some information for fraud (Behl, Pal, & Tiwari, 2019). Experience may indicate exposure to abuse by exploiting information to misuse an individual's social status (Virtanen, 2017).

During the pandemic, the fear and irrational behavior exacerbated these factors. Luring victims became one psychological principle on which cybercriminals relied on, as anxiety motivated people to look for various new sources of information to catch up important news. People felt more unwilling to feel safe to open a phishing email or press an unsafe link. Cybercriminals, since the emergence of Covid-19, are therefore launching newer and more innovative fraud campaigns taking advantage of people’s fears.

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

The current research contributes the existing literature in terms of the cultural context of the individuals. Most scales, questionnaires and inventories designed are appropriate for individualistic culture, compatible to European countries and the United States, however, in the middle East, where there is more a collectivist culture, it is necessary to identify a different scale. However, little research has been conducted in the Arab region to investigate fears of cybercrime risk and fear of victimization, from the psychological perspective. There is also no research, till date, that might have explored the validation of a scale to measure this phenomenon in the Arab region. Accordingly, the study fills this gap as it seeks an answer to the following question: What is the factorial structure around which the fear of cybercrime risk and fear of victimization organized?

Literature review

- *Cybercrime phenomenon and classification*

Böhme and Moore (2012) define cybercrime as a kind of violation of the privacy of individuals, their ability to express themselves on social media sites, civil society organizations, or public institutions. It may be a way to manage conflict against governments, parliaments, other public institutions, and state infrastructure. Stephenson and Walter (2011) describe it as a threat to democratic stability and the use of technology and means of communication for other purposes or to subscribe to extremism or exploitation. Cybercrimes can be classified in terms of the degree of aggression; method of performance; generation of crime; data crimes, harmful outcomes of cybercrime, and the type of physical abuse inflicted on individuals and companies.

The classification in terms of the degree of aggression comprises four types (Stephenson & Walter, 2011): (a) Power assertive crimes: These are crimes in which the individual imposes coercion and aggression to impose limitation over the victim and chase her actions that call for pride through anonymous websites, social networks. The number of offenders of these narcissistic crimes and intimidation of the offering has increased manifold; (b) Power Reassurance Crimes: It is very similar to aggressive crime, except that the difference is the amount of imagination the offender brings to reality. It is one of the unorganized crimes. It depends primarily on age. It focuses on challenging the victim physically and mentally and exploiting him financially, morally, or sexually due to the victim's lack of self-confidence. It depends on persuasion between the offender and the victim and the extent of the less structured relationship than the crime category. These crimes are the simplest to commit because it depends on the amount of information available through the victim's social media accounts. (c) Anger Retaliatory crimes: This crime represents the offender of complete hostility to one or more persons or organizations. The representatives of these crimes are not interested in holding meetings in the real world, as the offender behavior is stirred according to an ideology. These crimes are represented by the recruiting of young men and girls to implement plans that may amount him to terrorism. (d) Anger excitation crimes: The offender is characterized by sadism and the focus of his activity on terrorizing the victim.

The second classification in terms of method of performance (Saini, Rao, & Panda, 2012) can be explained in terms of evidence and content as (a) Computer-Related

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Forgery and Fraud crimes: This type is done in cash transactions and providing manifest procedures. Usually, the individual needs an intermediary gathering to implement this crime, such as falsifying electronic certificates. (b) Content-Related Crimes: These include cyber-punk or sex, unsolicited commercial communications, and cyber defamation.

The third classification in terms of generation of crime (Choo & Smith, 2008) divides crimes in terms of digital development into two generations: (a) first, which relies on electronically produced crimes that disrupt data and then break personal computers on server data; (b) second, which have arisen because of the emergence of Web 2.0 technologies. These crimes contain impersonation and research plagiarism. Social networks, wikis, and other interactive sites are crime tools for this generation. Example of crimes include anonymity and borrowing content, pictures, or anything else.

The fourth classification of data crimes depend on network hackers to obtain data and employ or destroy it. These crimes pose a greater challenge to the cyber police as there is a drastic change in the method used in executing crime, where it is difficult to track the crime offender in the cyberspace (Jeffries & Apeh, 2020). The data crimes can be further classified as sniffing and social engineering crimes: (a) The sniffing type of crime happens in such networks where cyber criminals are involved in sniffing everything that goes on between personal computers through a method called wiretapping (Prasad & Rohokale, 2020). This type of crime occurs in one of two ways: cyber espionage or cyber warfare. The cyber espionage refers to intruding on confidential information of a user or an institution without permission or stealing information and exploiting it for sabotage or economic espionage. The cyber warfare aims to disrupt the infrastructure by causing a general defect in the digital information sources, which leads to a disorder or disruption in the provision of public services to the state or financial and civil institutions. (b) The social engineering crimes are committed through an imitation technique that provides a hacker to obtain information needed for the break-in. The person who discusses every data is satisfied that the hacker is a friend or something similar, or one of the individuals who have the right to obtain the information. This behavior prompts the victim to reveal the information which he needs.

Next, there is the classification of crimes based on the harmful outcomes of cybercrime. This type of cybercrimes depends on the type of psychological harm inflicted on individuals. The appearance of this crime leads to the occurrence of psychological abuse to individuals, and it subdivided into two types: as cyberstalking crime or cyber pornography crimes. Cyberstalking crime means the use of cyberspace to control, harass, or terrorize a target to the point of fear of death either for himself or for others who live around him. Cyber pornography type can be used to possess, create, publish, and distribute pornographic material, and it usually occurs with children. Carvalho et al. (2020) believe that these crimes involve the fraudulent exploitation of children and the negotiation of illegal content. The crime outcomes lack evidence due to inadequate identification and location of the offender. Besides, victims cannot be specified unless they report the abuse that happened to them (Jeffries & Apeh, 2020). Consequently, law enforcement malfunctions in the absence of reliable information (Carvalho et al., 2020).

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Finally, the crimes that depend on the type of physical abuse are usually inflicted on companies rather than individuals. It can be executed through non-violating technologies. This type of crime includes any crimes far from political and controversial motives such as: cyber vigilantism crime, which includes the convergence between different organizations and the cyberspace through which they broadcast rumors; or cyber-hacktivism crime, which means that a few perpetrators create prominent linkages with the cyber pirates or develop such skills themselves in order to strengthen their communities and self-interests.

- *Factors contributing to the cybercrime context*

The factors contributing to cybercrime can be studied into four categories, namely: Electronic and technical factors, Personality factors, factors concerning social characteristics, and factors concerning individual motivation. The first category of electronic and technical factors refers to identity theft electronically by stealing a person's credentials and embezzling bank accounts and manipulating other personalized details. Often this crime is committed through personal computers and smartphones by reaching into individual's tax files, social security numbers and PIN numbers of credit cards and like (Roberts, Indermaur, & Spiranovic, 2013). The personality factors are the qualities inherent in the psychological makeup of the individual, which causes falling victim to electronic crimes (Saroha, 2014). The factors concerning social characteristics are associated with the characteristics of social control and the problem of the mind of the criminal intelligence of the individual following their social skills and their self-confidence and beliefs of ideology (Saroha, 2014). Finally, factors concerning individual motivation, relates to the sense of inferiority or demolition and sabotage for the offender of a crime, or by pleasing his ego, or a cure for the lack of content in the trading networks, banking, and shopping.

The fear actor or the fear of victimization can potentially make a negative impact on individuals' mental health and overall personality by creating anxiety and distrust (Ferraro, 1995; Lewis & Salem, 2017; Park & Vieraitis, 2021). Such fears have increased since the increase in the usage of the Internet, because most cybercrime activities are committed online with the help of the internet. People are now afraid to use the internet for the fear of online victimization (Choi, 2010), with identify theft as the most feared cybercrime. Other crimes affiliated to the online cybercrimes include cyberbullying, harassment, or stalking (Choi, 2010). Reinhart (2017) found that in US, internet users are more fearful of Internet crimes than traditional crimes; resulting in cyber-victimization (Morgan, 2017). Various factors have been identified as causes behind such fears and models to resolve these issues are based on users' vulnerability, users' victimization, the problems of disorder and social integration, and risk interpretation (Cohen, Kluegel, & Land, 1981; Ferraro, 1995; Meier & Miethe, 1993; Rountree & Land, 1996). Despite, a heavily researched domain, there is very little empirical research existing on the fear factors of cyberspace risks and being victimized as a result of that (Henson, Reyns, & Fisher, 2013).

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Method

- *Research Design and Participants:*

An exploratory cross-sectional method was applied for participants from various universities contacted through the Arab user's Facebook groups and an electronic survey using the Google form link: https://forms.gle/2QgzK9oVyMkqc3ef7. The participants included university students with the Arab background and were identified using the snowballing sampling technique. It means that when the survey links were sent to the participants, they were asked to forward the links to their fellow students. The final sample numbered 612 students, 120 (19.6%) males and 492 (80.4%) females, with an average age of 20.41 years and a standard deviation of 3.54. The marital status of the sample showed 547 (89.7%) as single and only 30 (4.9%) as married, 27 (4.4%) as divorced, and 6 (1%) as widowed.

- *Measures: Cybercrime risk fear Scale:*

A cybercrime risk fear questionnaire with 15 items was used for this study to collect the data. The scale responses were formulated on a five-point Likert scale. The scale was based on previous studies that have interpreted cybercrime fears from different factors such as psychological factor (Yu, 2014), who studied the cybercrime four-factor model of fear and anxiety such as Internet fraud, digital piracy, Internet viruses, and cyberbullying. Bernik, Dobovšek, and Markelj (2013) examined the context of anxiety and fears with exploratory factor analysis (EFA); Park and Vieraitis (2021) treated the fear of cybercrime as a general factor model; Riek, Bohme, and Moore (2015); Riek, Böhme, and Moore (2014) found some dimensions as factors including the perceived threats of cybercrime, intent to avoid, awareness, and cybercrime experience. Some other scales such as (Lee, Jackson, & Ellis, 2020; Rader, 2004) have focused on feelings, thoughts, and perceived threat behaviors; finally, Lee et al. (2020) have addressed physiological responses to threat, recurrent thoughts associated with anticipating future liability, and more prevalent low emotions.

- *Procedures and Data analysis:*

The questionnaire was distributed through social networking sites, especially WhatsApp and Facebook, through an electronic link on Google form. The period ranged between August 2021 to January 2022. Respondents were informed about the confidentiality of data and analysis and that the data would be used only for scientific purposes. The subscales measured the anxiety manifestations in individuals during social networking sites interactions and the fear of falling as a victim of cybercrime considering the ongoing pandemic. The data was first stored in MS-Excel, and then converted into SPSS file. The IBM SPSS v26 and MPLUS v7 software were used to analyze data. Subscale's consistency stability was tested by Cronbach's Alpha coefficient. The general-factor, two-factor, and three-factor models were generated using exploratory factor analysis using a maximum likelihood approach. Geomin orthogonal rotation was selected for extracting data. Confirmatory factor analysis by the Maximum Likelihood method verified the model's fit. The accepted model depended on the chi-squared statistic, RMSEA, TLI, and CFI indices.

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Results

Right at the outset, an exploratory factor analysis was conducted for the cybercrime fear scale. The maximum likelihood method and Geomin orthogonal rotation were selected to perform the analysis. The resulting model-fit indicators were poor, X2=443.21, P=.000, RMSEA= .080, CFI= .707, TLI= .658, SRMR= .071. The SRMR was acceptable as it was close to zero, which meant that the model was poorly defined in explaining the phenomenon. The saturation levels on first-order exploratory general factor model were as follows (Table 1):

Table 1. The first-order exploratory general factor model.

	Factor loading (Estimated)	Standard error (SE)	t-value (Estimated/SE)
1	0.553	0.041	13.59
2	0.505	0.037	13.78
3	0.475	0.039	12.11
4	0.063	0.047	1.35
5	0.369	0.046	8.11
6	0.394	0.044	9.05
7	0.526	0.043	12.22
8	0.071	0.053	1.34
9	0.573	0.035	16.43
10	0.059	0.052	1.14
11	0.578	0.035	16.70
12	0.530	0.035	15.18
13	0.476	0.041	11.61
14	0.403	0.043	9.28
15	0.389	0.047	8.36

The item factor loadings on the latent general factor ranged between 0.059 to 0.578. Items 4, 8 and 10 were excluded as they were not statistically significant. The Cronbach's alpha was 0.78.

The exploratory two-factor was measured using the Geomin orthogonal rotation and Maximum likelihood approach selected to conduct the model. The goodness of fit indices was poorly fitted, X^2=443.21, P=.000, CFI= .707, TLI= .658; while RMSEA= .080 indicator was the best value. The SRMR= .071 was acceptable as it was close to zero, which meant that the model was poorly defined in describing the phenomenon. Table 2. presents the item factor loadings in exploratory two-factor model.

Table 2. Exploratory two-factor model item factor loadings.

	Factor 1	Factor 2
1	0.550	
2	0.502	
3	0.473	
4		0.310
5	0.378	
6	0.386	
7	0.533	
8		0.572
9	0.566	
10		0.725
11	0.583	
12	0.522	
13	0.477	
14	0.416	
15	0.408	

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

The first-dimension factor loadings ranged from 0.378 to 0.583. A total of 12 items saturated on this dimension. The factor loadings for the second factor ranged from 0.310 to 0.725, and 3 items saturated on it. According to the internal consistency of the dimensions using the alpha coefficient its value was 0.78 and 0.53.

The exploratory three-factor model was studied through the orthogonal rotation by Geomin, which was used to extract the model items. The goodness of fit was poor in X2=183.81, P=.000 which p-value was significant. The indicators RMSEA= .056, CFI= .900 were accepted. The TLI= .833 has a bad fit. The SRMR= .037 was well fitted. The SRMR and CFI were acceptable as they approached zero. The item factor loadings are presented in Table 3.

Table 3. Three-factor model loading.

	Factor 1	Factor 2	Factor 3
1	0.672		
2	0.572		
3	0.561		
4		0.321	
5			0.334
6			0.364
7	0.537		
8		0.558	
9	0.570		
10		0.745	
11	0.549		
12	0.449		
13			0.443
14			0.575
15			0.635

The first-dimension loadings were ranged from 0.449 to 0.672, and it had 7 items. The second dimension had 3 items, and its factor loadings ranged from 0.321 to 0.745. Finally, the third dimension had 5 items, and its item saturations were ranged from 0.334 to 0.635. The internal consistency of the dimensions was computed using the alpha coefficient and its value was 0.78, 0.53, and 0.65.

It was noted from the exploratory models that there was an agreement in the same items that were excluded from the general factor model, as it was one of the factors in the two-factor and the three-factor models. It was also noted that the item loadings in the second dimension of the three-factor model inflated their values more than in the two factors model, which signifies the explanatory accuracy of the factor. The first dimension in the two-factor model decayed into two dimensions in the three-factor model.

Next, a confirmatory factor analysis of the previous exploratory competitive models was conducted to explain the phenomenon of fear of cybercrime models. The models fit were compared with exploratory analysis and confirmatory analysis. the confirmatory analysis was performed using the MLR method. The results are presented in Table 4.

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Table 4. Competitive models goodness of fit indices.

Model	Model fit indices							
	X^2 (P)	X^2/df	SRMR	CFI	TLI	RMSEA [90%CI]	AIC	BIC
General factor CFA	537.61 P=.0000	5.97	0.071	0.698	0.647	0.090 [0.083 - 0.098]	28916.40	29115
General factor EFA	443.21 P=.000	4.92	0.071	0.707	0.658	0.080 [0.073 - 0.088]	28916.40	29115
Two-factor EFA	297.04 P=.0000	3.91	0.053	0.817	0.747	0.069 [.061 - 0.077]	28762.59	29022.98
Two-factor CFA	281.66 P=.0000	3.27	0.050	0.868	0.839	0.061 [0.053 - 0.069]	28668.44	28884.70
Three-factor EFA	183.81 P=.0000	2.92	0.037	0.900	0.833	0.056 [0.047 - 0.066]	28644.53	28962.30
Three-factor CFA	202.27 P=.0000	2.41	0.042	0.920	0.900	0.048 [0.040 - 0.057]	28593.05	28818.13

The results reveal that confirmatory models suffered from misidentification of the model, except for the three-factor model, for which the fit indices were acceptable and compatible with the sampled data. The results agreed on the superiority of the three-factor model, exploratory and confirmatory, and this meant that the construction reflected the fear of cybercrime risks. The goodness of fit indicators was acceptable for the exploratory and confirmatory two-factor model according to indicators X^2/df and acceptable SRMR; whereas all indices of the two-factor model had a poor fit, which may reflect as misidentification of the model.

Discussion

The current study aimed to verify the construction of the cybercrime fear scale on social network users. The factor analysis approach was used to study the phenomenon. The factor analysis resulted in three exploratory models: the general factor model, the two factors model, and the three factors model. The study verified the exploratory models using CFA. Previous studies have confirmed that the cybercrime fear construction differs according to the perspective of its study. From the perspective of the technical sciences, for instance, it is studied as the field of crime in its essence, and examples are studied (Yu, 2014); while in terms of psychological perspective, it was divided into emotional factors (avoidance of harm, experience), personal factors (cognitive beliefs, ideas, and individual reference frameworks), behavioral aspects (physiological responses, and the intention to avoid interactions), and it is consistent with Lee et al. (2020); Rader (2004); Riek et al. (2015).

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

The results of the present study contrast in their psychometric nature with studies of general factor construction using EFA and CFA (Park & Vieraitis, 2021). The current study also agrees on the three-factor construction with Bernik et al. (2013); Lee et al. (2020); Rader (2004); Riek et al. (2015); where the corresponding indicators were acceptable. The findings suggest that poor fitting of the one-factor model using exploratory and confirmatory factor analysis may be due to many factors including:

1. Misunderstanding by the individual of his abilities, thoughts and feelings, and the difficulty of expressing them.
2. Social approval is the individual's refusal to express his behavior even if he has had a previous experience as a victim. It may suggest that the individual refuses to express his feelings.
3. The general factor construction includes rejection of the unknown and avoidance of harm. It may be self-evident that the individual adheres to during interactions with others.
4. The general factor is the first factor in the two- and three-model construction, which indicates that it is more stable and is a requirement for explaining the emotions and behaviors related to the experience of being a victim of cybercrime.

The IBM SPSS software was also used to perform the total explained variance of the general factor model, which was 19%. The differences between the subscale's eigenvalues did not exceed the value of one while the two-factor model measured a variance of 25.7%; and the three-factor model explained the total variance of 30.7%. The exploratory three-factor model was simple (parsimonious criteria verified), as each item was loaded on a single factor. It was also noted that the factor loadings saturations with the first factor were inflated from their value in the two other models.

The study recommends the necessity of verifying the validity of the construction on larger samples. The study had some determinants for generalizing the results of the scale because the variance explained by the three factors was very small i.e., 30.7%, which may not be a defect in the sample data, while it is due to the individual's refusal to feel helpless or awareness of the role of the victim or fear of the unknown that may only occur in the areas of rare.

Conclusion

Overall, the findings of the study suggest that a structural causal model comprising two or three factor models pertaining to fear of crime may be acceptable. However, due to some factors like the impact of fear of victimization and fear of cyber fraud, the risk interpretation model suggested in this study would not work. This finding occurs because of the fact that most social networking sites are vulnerable and are subjected to fear of victimization and fear of Internet fraud. While considering the two or three factor models in the current research, particular attention needs to be drawn to the contextual aspects of the social networking sites to cope up with the fear of victimization. It is recommended that public awareness campaign should be conducted and experiences of internet victims must be shared on public platforms and social media. Since most cyber predators make use of the social media as a venue for cybercrime, such dissemination of cyber fraud stories and awareness camps could lead to avoidance of these crimes.

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

- **Acknowledgement:** Dr. Abdulnaser contributed in the idea, literature review, application and discussion. Dr. Mahmoud contributed in methodology, statistics and discussion. Dr. Adawi contributed to the idea, literature review and discussion.
- **Conflict of Interest**: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.
- **Informed Consent**: All procedures followed were in accordance with the ethical standards of the responsible committee on human experimentation (institutional and national) and with the Helsinki Declaration of 1975, as revised in 2000 (5). Informed consent was obtained from all participants for being included in the study

References

Aiken, M. (2017). *The Cyber Effect: An Expert in Cyberpsychology Explains How Technology Is Shaping Our Children, Our Behavior, and Our Values--and What We Can Do About It*. Random House Publishing Group. https://books.google.com.pk/books?id=ZIclDwAAQBAJ

Alshalan, R., & Al-Khalifa, H. (2020). A deep learning approach for automatic hate speech detection in the saudi twittersphere. *Applied Sciences, 10*(23), 8614. https://doi.org/10.3390/app10238614

Behl, A., Pal, A., & Tiwari, C. (2019). Analysis of effect of perceived cybercrime risk on mobile app payments. *International Journal of Public Sector Performance Management, 5*(3-4), 415-432. https://doi.org/10.1504/IJPSPM.2019.101062

Bernik, I., Dobovšek, B., & Markelj, B. (2013). To fear or not to fear on cybercrime. *Innovative Issues and Approaches in Social Sciences, 6*(3), 1-17. http://www.iiass.com/pdf/IIASS-volume6-number3-article1.pdf

Böhme, R., & Moore, T. (2012). How do consumers react to cybercrime? In *2012 eCrime researchers summit* (pp. 1-12). IEEE. https://doi.org/10.1109/eCrime.2012.6489519

Bouchard, M., & Morselli, C. (2014). Opportunistic structures of organized crime. In L. Paoli (Ed.), *The Oxford Handbook of Organized Crime* (pp. 288-302). Oxford / New York: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199730445.013.015

Carvalho, J. V., Rocha, Á., Abreu, A., & Victor, A. (2020). Portuguese Concerns and Experience of Specific Cybercrimes: A Benchmarking with European Citizens. In *Developments and Advances in Defense and Security* (pp. 39-50). Springer. https://doi.org/10.1007/978-981-13-9155-2_4

Choi, K.-S. (2010). *Risk factors in computer-crime victimization*. LFB Scholarly Pub. https://www.ojp.gov/ncjrs/virtual-library/abstracts/risk-factors-computer-crime-victimization

Choo, K.-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology, 3*(1), 37-59. https://doi.org/10.1007/s11417-007-9035-y

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American sociological review*, 505-524. https://doi.org/10.2307/2094935

Covington, J., & Taylor, R. B. (1991). Fear of crime in urban residential neighborhoods: Implications of between-and within-neighborhood sources for current models. *The Sociological Quarterly, 32*(2), 231-249. https://doi.org/10.1111/j.1533-8525.1991.tb00355.x

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Ferguson, K. M., & Mindel, C. H. (2007). Modeling fear of crime in Dallas neighborhoods: A test of social capital theory. *Crime & Delinquency, 53*(2), 322-349. https://doi.org/10.1177/0011128705285039

Ferraro, K. F. (1995). *Fear of Crime: Interpreting Victimization Risk*. State University of New York Press. https://books.google.com.pk/books?id=98Mq8xQy0cAC

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497. https://doi.org/10.1177/1043986213507403

Intravia, J., Wolff, K. T., Paez, R., & Gibbs, B. R. (2017). Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. *Computers in Human Behavior, 77*, 158-168. https://doi.org/10.1016/j.chb.2017.08.047

Jeffries, S., & Apeh, E. (2020). Standard operating procedures for cybercrime investigations: a systematic literature review. In *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 145-162). Elsevier. https://doi.org/10.1016/B978-0-12-816203-3.00007-1

Lee, M., Jackson, J., & Ellis, J. R. (2020). Functional and dysfunctional fear of crime in inner Sydney: Findings from the quantitative component of a mixed-methods study. *Australian & New Zealand Journal of Criminology, 53*(3), 311-332. https://doi.org/10.1177/0004865820911994

Lee, S.-S., Choi, K.-s., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 5-22. https://www.doi.org/10.52306/02020219SVZL9707

Lewis, D. A., & Salem, G. W. (2017). *Fear of crime: Incivility and the production of a social problem*. Routledge. https://doi.org/10.4324/9780203792032

Meier, R. F., & Miethe, T. D. (1993). Understanding theories of criminal victimization. *Crime and justice, 17*, 459-499. https://www.journals.uchicago.edu/doi/abs/10.1086/449218?cookieSet=1

Mishra, S., Draus, P., Goreva, N., Leone, G., & Caputo, D. (2014). The Impact of Internet Addiction On University Students and Its Effect on Subsequent Academic Success: A Survey Based Study. *Issues in Information Systems, 15*(1). https://doi.org/10.48009/1_iis_2014_344-352

Morgan, S. (2017). *Cybercrime report, 2017*. HerjavecGroup.com. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Oskenbay, F., Kalymbetova, E., Tolegenova, A., Kabakova, M., Bakiyeva, S., & Nugmanova, S. (2015). Addictive behavior among adolescents. *Procedia-Social and Behavioral Sciences, 171*, 406-411. https://doi.org/10.1016/j.sbspro.2015.01.140

Park, Y., & Vieraitis, L. M. (2021). Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experiences. *International Journal of Cybersecurity Intelligence & Cybercrime, 4*(2), 38-52. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1105&context=ijcic

Prasad, R., & Rohokale, V. (2020). *Cyber security: the lifeline of information and communication technology*. Springer. https://doi.org/10.1007/978-3-030-31703-4

Rader, N. E. (2004). The threat of victimization: A theoretical reconceptualization of fear of crime. *Sociological Spectrum, 24*(6), 689-704. https://doi.org/10.1080/02732170490467936

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Reinhart, R. (2017). Cybercrime tops Americans' crime worries. *Gallop News*. https://news.gallup.com/poll/221270/cybercrime-tops-americans-crime-worries.aspx

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273. https://ieeexplore.ieee.org/abstract/document/7056466

Riek, M., Böhme, R., & Moore, T. (2014). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. In *13th Workshop on the Economics of Information Security* (pp. 1-35). https://econinfosec.org/archive/weis2014/papers/RiekBoehmeMoore-WEIS2014.pdf

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law, 20*(3), 315-328. https://doi.org/10.1080/13218719.2012.672275

Rojas, M. (2020). Crime, Violence and Well-Being. In *Well-Being in Latin America* (pp. 141-153). Springer. https://doi.org/10.1007/978-3-030-33498-7_10

Rountree, P. W., & Land, K. C. (1996). Burglary victimization, perceptions of crime risk, and routine activities: A multilevel analysis across Seattle neighborhoods and census tracts. *Journal of research in crime and delinquency, 33*(2), 147-180. https://doi.org/10.1177/0022427896033002001

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209. https://www.researchgate.net/profile/Hemraj-Saini/publication/241689554_Cyber-

Saroha, R. (2014). Profiling a Cyber Criminal. *International Journal of Information and Computation Technology, 4*(3), 253-258. https://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

Stephenson, P. R., & Walter, R. D. (2011). Toward cyber crime assessment: cyberstalking. In *6th Annual symposium on information assurance (ASIA'11)* (pp. 7-8). Citeseer. https://www.albany.edu/iasymposium/proceedings/2011/5-StephensonReview.pdf

Suler, J. (2004). Computer and cyberspace "addiction". *International Journal of Applied Psychoanalytic Studies, 1*(4), 359-362. https://pep-web.org/browse/document/IJAPS.001.0359A?index=40

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. https://doi.org/10.1080/13218719.2017.1315785

Wilcox, P., Quisenberry, N., & Jones, S. (2003). The built environment and community crime risk interpretation. *Journal of Research in crime and delinquency, 40*(3), 322-345. https://doi.org/10.1177/0022427803253801

Yaghoobi, A., Mohammadzade, S., Chegini, A. A., Vasel, M. Y., & Paidar, M. R. Z. (2016). The relationship between attachment styles, self-monitoring and cybercrime in social network users. *International Journal of High Risk Behaviors & Addiction, 5*(3). https://doi.org/10.5812%2Fijhrba.27785

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1), 36. https://www.cybercrimejournal.com/pdf/yuijcc2014vol8issue1.pdf

© 2022 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License