JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2022.2101160

Taylor & Francis
Taylor & Francis Group

Development of a Scale to Measure Cybercrime-Awareness on Social Media

Ibrahim Arpaci and Omer Aslan

Bandirma Onyedi Eylul University, Balikesir, Turkey

ABSTRACT

This study developed a psychometric scale to measure users' cybercrime awareness level on social media. Psychometric properties of the **C**ybercrime **A**wareness on **S**ocial **M**edia **S**cale (CASM-S) were tested based on data collected from 1045 social media users. Exploratory factor analysis (EFA) with principal components analysis was used to identify the underlying factor structure of the scale (N = 545). The results revealed that the scale has a unidimensional factor structure. The scale was found to have a high internal reliability (α = .957). Confirmatory factor analysis (CFA) was conducted to verify factor structure of the CASM-S (N = 500). Results revealed that the one-factor model fits the data well (x^2/DF = 2.757, CFI = .939, SRMR = .0366, RMSEA = .059). Further, the study evaluated the concurrent validity of the scale (r = .855, p < .001). The findings revealed that the CASM-S is a reliable and valid tool to measure users' cybercrime awareness level on social media.

KEYWORDS
Cybercrime awareness; social media; Scale development

Introduction

Cybercrime is a criminal activity which is carried out in cyberspace by using computer-based systems. The computer-based systems including personal computers, tablets, smartphones, Internet of Things (IoT) can be used to commit a crime as well as become a victim of cybercrime.[1] Recently, the number and sophistication of cybercrimes have been increased globally.[2] The increased usage of digital environments motivated cybercriminals to commit crimes in cyberspace rather than the real world.[3] Cybercriminals can be anyone from script kiddies to hackers, from organized groups to some state governments.[4] The crimes committed online can vary including child pornography, cyber extortion, cyber espionage, crypto jacking, data breach, e-mail fraud, identity theft, illegal interception, illegal gambling, infringing copyright, and phishing.[5] The cybercrimes threaten the privacy of users, bank accounts, health-related data, social media accounts as well as big companies' availability, confidentiality, and integrity of the data.[3]

In the past, the cyberattacks were not as complicated as today's attacks and there were fewer computer-based systems to protect.[6] However, the rapid advancement of technology has made cybercrimes easier and more sophisticated.[7] The increased usage of smartphones, IoT devices, social media platforms, cloud platforms, and crypto mining also escalated the effects of cybercrimes.[8] As stated in several scientific research reports, cybercrimes cost a few trillion dollars to the world economy each year, and this cost is expected to increase every year.[9]

The history of cybercrimes over the decades can be seen in Table 1. The history of cybercrime is important to understand how crimes have been evaluated over the years. For example, phone phreaking began in the 1950s.[10] Phone phreaks were hijacking the protocols in phone systems to make free calls for long distances. The phone phreaking can be considered as the first cybercrime in the digital world. The computer vulnerabilities and hacking term emerged in the 1960s.[10] The foundation of cybersecurity began in the early 1970s with the project called "Advanced Research Projects Agency Network" (ARPANET).[10] This was the first packet-switched network before the Internet. The first virus was created in 1971 in ARPANET's network, and famous hacker Kevin Mitnick was arrested for the first cybercriminal behavior in 1979.[10] In the 1980s, numerous computer-related attacks have occurred.[11] In 1985, the USA (United States of America) Department of Defense (DoD) created computer security guidelines, called as Trusted Computer System Evaluation Criteria (TCSEC). The TCSEC was later named as "Orange Book."[11] In the 1990s, initially computer viruses and later computer worms became very popular. In the 2000s, the Internet has grown fast. The first organized hacker group emerged in the beginning of the 2000s. In this area, just opening the website was enough to get

CONTACT Ibrahim Arpaci iarpaci@bandirma.edu.tr Bandirma Onyedi Eylul University, Faculty of Engineering and Natural Sciences, Department of Software Engineering, 10200 Balıkesir, Turkey

Table 1. The history of cybercrimes over the decades.

Period	Cybercrimes
1950s	Phone phreaking started
1960s	Vulnerability and hacking terms emerged
1970s	Computer security term appeared
1980s	From ARPANET to the Internet
1990s	Computer virus and worms became popular
2000s	The usage of the internet excessively growth
2010s	Cybercriminals exploited several security breaches and cybercrimes became an industry
2020s	Social media related cybercrime increased

infected with a virus. In the 2010s, cybercriminals discovered several security breaches in computer network protocols as well as in software applications. Between 2010 and 2020, ransomware-related attacks became very popular. LockerGoga Ransomware blocked the infected systems and caused millions of dollars in damage.[12] In 2020, CovidLock Ransomware affected several Android devices by encrypting the data on devices which resulted in denying data access for legitimate users.[13]

These days (2020s), it is almost possible for cybercriminals and organized hackers to hack everything in cyberspace. Professional websites provide cybercrimes as a service to commit crimes on the digital platforms.[14] It is important to note that back in the early days, cybercriminals were using some simple techniques to launch digital attacks. However, currently, cyberattacks have been seen as a way of making millions of dollars which big corporations and organizations are behind.[6] Nowadays, cybercrimes which target the social media environments are becoming so popular.[15]

An excessive use of social media platforms have been reported especially during the COVID-19 pandemic.[16] Almost half of the world's population spend most of their time on social media platforms.[17] Social media companies store sensitive users' information such as name, surname, address, workplace, and important images and videos.[18] There are several cybercrimes committed in social media platforms including cyber bullying, hacking, fraud, selling illegal things, spreading disinformation, and promoting spams.[18] In addition, there is a tremendous increase in fake profiles in social media which are responsible for posting illegal content as well as spamming legitimate.[18] We can basically classify these crimes into three categories: Cybercrimes targeting social media users, facilitated on social media platforms, and advertised on social media platforms.[1] By the end of 2019, 9.6 billion social media records were compromised.[19] From 30% to 40% of the social media platforms are somehow responsible for hacking activities.[15] Malicious software (malware) can be easily spread on social media environments by hiding in attachments, links, and messages.[20] Further, the majority of the companies are worried about their network security because of the use of social media platforms by their employees.[21]

Awareness may have a positively significant effect on users' security and privacy knowledge.[22] Nevertheless, cybercrime awareness in social media platforms is not examined deeply by the researchers. The users are as important as software developers and social media content providers. This is because at the end of the day, users use social media platforms, if the users are not careful enough, the cybercriminal will be successful no matter how software applications are bugs-free. Furthermore, the social media platforms are distributed over the Internet globally and there is no proper control over these complex platforms. Without the proper security standards, policies, and regulations, it will be almost impossible to fight against the cybercriminals. Hence, there is an urgent requirement to develop training programs to raise the user's awareness on social media platforms.

In general, the social media users are the weakest chain in the protection of cybercrimes and they can be easily convinced by using social engineering attacks. The social media companies which provide the services to the users are also prone to cybercrimes. Both social media users as well as social media content providers must be educated with seminars, training programs, and conferences regularly to inform them about cybercrimes and their destructive consequences. Accordingly, the present study aimed to develop a new scale to measure cybercrime awareness level of the social media users. The study evaluated psychometric characteristics of the scale by following rigorous methodological standards.

In order to measure the cybercrime awareness on social media platforms, the well-defined policies, guidelines, and cybercrime awareness scale are needed. As far as we know, the proposed scale is the first scale which measures cybercrime awareness on social media platforms. The suggested scale is crucial since it determines the social media user's awareness level against cybercrimes. We think that the proposed scale can be used as a policy guideline for social media users to increase awareness while decreasing the possibility of compromise. In addition, the proposed scale will be one of the main sources for future researchers who want to measure and improve the cybercrime awareness level of users on social media platforms.

Literature review

There are a few scientific publications which are somehow related to cybercrime or emphasize the cybercrime awareness on social media environments.[23] These studies are crucial since we utilized the methods that were used in those studies when we built the proposed scale. The studies were discussed based upon the main idea, presented method, relevance of study area, and limitations of the proposed method. This study proposed a new scale for measuring cybercrime awareness on social media platforms and contributed to the field by reducing shortcomings of the existing studies.

Prior studies focused on combating with cybercrimes via outreach, prevention and users' awareness.[24] Criminals on online platforms have more knowledge when it comes to using high-tech facilities, therefore, in order to effectively fight against those criminals, organizations and law enforcement authorities should work together.[24] Further, comprehensive information security policy is needed to identify the cybercrime trends beforehand and prevent those trends of crimes.[25] It is important to note that awareness is the key to information security policy compliance.[26] Raising the users' awareness on all levels as well as continuous training of the vulnerable groups in protection against potential cybercrimes may reduce cyber risks globally.

Saridakis et al.[27] investigated how personal characteristics, user awareness, and user behavioral patterns are related to be a victim of cybercrime. They prepared questionnaire was tested on 700 individuals and a model used to examine the probability of an event. Their results showed that the explanatory variables can be ordinal, dichotomous, or continuous. According to their results, the users who shared less information on social media were less likely to become a target of cybercrime. If the users had a high awareness level, they were also exposed to less cybercrimes. Their results also demonstrated that social media usage had a significant impact on online victimization. However, the effects may change based on the type of social media usage. For instance, for Facebook and Google there was no connection between the usage and victimization, while for LinkedIn and Blogger there was a strong correlation between the usage and victimization.

Almansoori et al.[28] focused on the challenges of analyzing cybercrimes on social media platforms. They assumed that several social media users do not have enough knowledge about security concerns when performing actions on online platforms. Their research goal was to find out the characteristics of cybercrimes committed on social media platforms. They used Python scripting language for data analysis and the results indicated that poor and uneducated people committed more cybercrimes. In addition, the users aged between 20 and 25 committed more crimes as well.

Prior studied indicated that although the usage of social media enhanced the business opportunities, they also brought several security issues for individuals as well as organizations. For example, a systematic review evaluated 18 publications to explore the effect of social media platforms for OSINT (open-source intelligence) concept.[29] The results indicated that usage of social media increased social cohesion as well as enhanced the business opportunities. The social media data were used to identify the terrorist group communications by analyzing the collected crime data. Most of the reviewed studies showed that social engineering attacks increase the level of risks on social media platforms. However, the social engineering threats could be mitigated with increasing users' awareness level.

Social media platforms produce a high volume of diverse data and users are not careful when they share information on these platforms. This raises the privacy and security issues on social media platforms.[30] Soomro and Hussain[20] categorized the cybercrimes committed on social media and provided valuable recommendations to decrease the level of being a victim of cybercrimes. Cybercrimes which are carried on social media platforms can be categorized as malware, identity theft, social engineering, phishing, burglary, cyber-casing, and cyber-stalking.[20] Further, cyber intrusion, data breaches, credit card fraud, and disaster fraud crimes are rising on social media platforms. Therefore, social media users should be cautious about the information shared publicly, check authenticity of e-mail addresses, install up-to-date security tools, and be careful when clicking the links, images, and videos.[20]

Recently, the cybercrime awareness among students have been investigated. Ismailova et al.[31] investigated cybercrime risk awareness level among the students in Kazakhstan as well as Kyrgyzstan. A study group of 156 students was selected from both countries to measure cybercrime risk awareness by using 51 questions related to cybercrimes. A one-way analysis of variance was performed on the collected data to test whether independent variables have an impact on the cybercrime awareness level or not. Their results demonstrated that gender and age significantly affected the cybercrime awareness level in Kazakhstan, while gender and age had no significant effect on the awareness level in Kyrgyzstan. This difference may be due to computer literacy level and information security knowledge among the students of the two countries.

Another study investigated cybercrime awareness in Saudi Arabia.[32] The study tested awareness on security practices and incident reporting by using an online questionnaire applied to 1230 participants. The results indicated that 32.5% of the participants were not aware of phishing attacks, 31.7% of the participants used free Wi-Fi services in order to connect to the Internet, 51% participants utilized personal information when creating passwords, and 21.7% of the participants were a victim of cybercrimes. Likewise, a recent study has investigated information security awareness on social media among female secondary school students in Saudi Arabia.[33] Their results indicated that Instagram and Snapchat were the most used social media applications among the young female students in Saudi Arabia. The results showed that 48% of the participants had information security awareness to a certain degree on social engineering techniques as well as fake gates. However, awareness on hacking activities and updating passwords regularly was weak. The study emphasized that the awareness level of young female students was low and this awareness level needs to be increased with proper training programs. In a similar study, cybersecurity awareness among undergraduate students at Majmaah University in Saudi Arabia has been investigated by collecting data on forged ads, computer viruses, phishing, popup Windows, electronic e-mails, and supplementary outbreaks via questionnaires.[34] The findings implied that there is an urgent need to train users to raise cybercrime awareness level and consequently to be less threatened by cyberattacks.

Cybercrime awareness among the elderly people has been investigated by prior studies. For example, Alwanain[35] conducted an experimental study to evaluate the phishing awareness among elderly users in social media. The study assumed that old people were targeted by cybercriminals more due to their lack of knowledge about the cyber risks. The experiment was performed on WhatsApp by analyzing elderly users' daily communications. The results indicated that training elderly users for phishing awareness had a positive effect on the identification of phishing attacks. In a similar study, the correlation between victimization and cybercrime awareness was examined for people who were older than sixty (60) years old.[36] The predefined awareness questions were asked to 15 elderly people. They found that most of the participants were using Facebook frequently, but hey were not very familiar with other social media platforms like Instagram and Twitter. They pointed out that normal cybercrime awareness education was not always useful for the people who were older than certain ages since they were not familiar with several Internet terms, norms, and practices. On the other hand, Alwanain[37] examined security awareness on phishing attacks among children aged between 7 and 13. They performed two test cases to determine the security awareness levels by analyzing daily WhatsApp communications. The experiment results showed that training children on phishing awareness has a noticeable positive effect on the detection of the phishing messages.

Prior studies indicated that if users have higher security awareness, they are less likely to be a victim of cybercrimes. Most of the evaluated publications were restricted to certain age groups (children, students, elderly, etc.) and performed on restricted regions (universities, certain city or country) which cannot be generalized to a broader population. Besides, none of these studies were focused on cybercrime awareness on social media platforms. Accordingly, the present study aimed to develop a cybercrime awareness scale which would reliably measure the awareness level of social media users. This study may eliminate the shortcomings of prior studies and make significant contributions to the cybersecurity literature.

Method and findings

It is important to note that when developing a new scale evidence of internal consistency, content validity, and criterion validity should be provided.[38] All these together provide evidence of construct validity that is defined as "the extent to which the scale measures what it is purported to measure."[39] Construct validity establishes a link between psychometric measurement and theory and it is an essential step for the development of high-quality scales.[40,41] Each stage of the development process shown in Figure 1 will highly contribute to the construct validity of the proposed scale.

Scale development process was initiated with the generation of scale items. Then the item pool was evaluated by the expert panel for content validity. The researchers were collected the initial data by using the items that have survived from the expert panel evaluation. The EFA was employed to determine the underlying factor structure of the proposed scale. It is not recommended to use the same data both for development of the scale and for testing the psychometric properties of the new scale due to the concerns about common method variance.[42] Further, it was recommended that if any items are removed or added from a scale, then the updated scale should be administered to a different independent sample.[43] Accordingly, the researchers were collected the secondary data by using the refined items. The CFA was employed to verify factor structure of the scale resulting from the EFA. Concurrent validity, which is a type of criterion validity, was tested to discover how well the new scale compares to a well-established scale. Finally, an item discrimination analysis was conducted to test discriminating power of the proposed scale.

Study 1

Content validity

Researchers systematically reviewed the relevant literature and existing legislations on cybercrimes and their types for the development of a theoretical foundation for

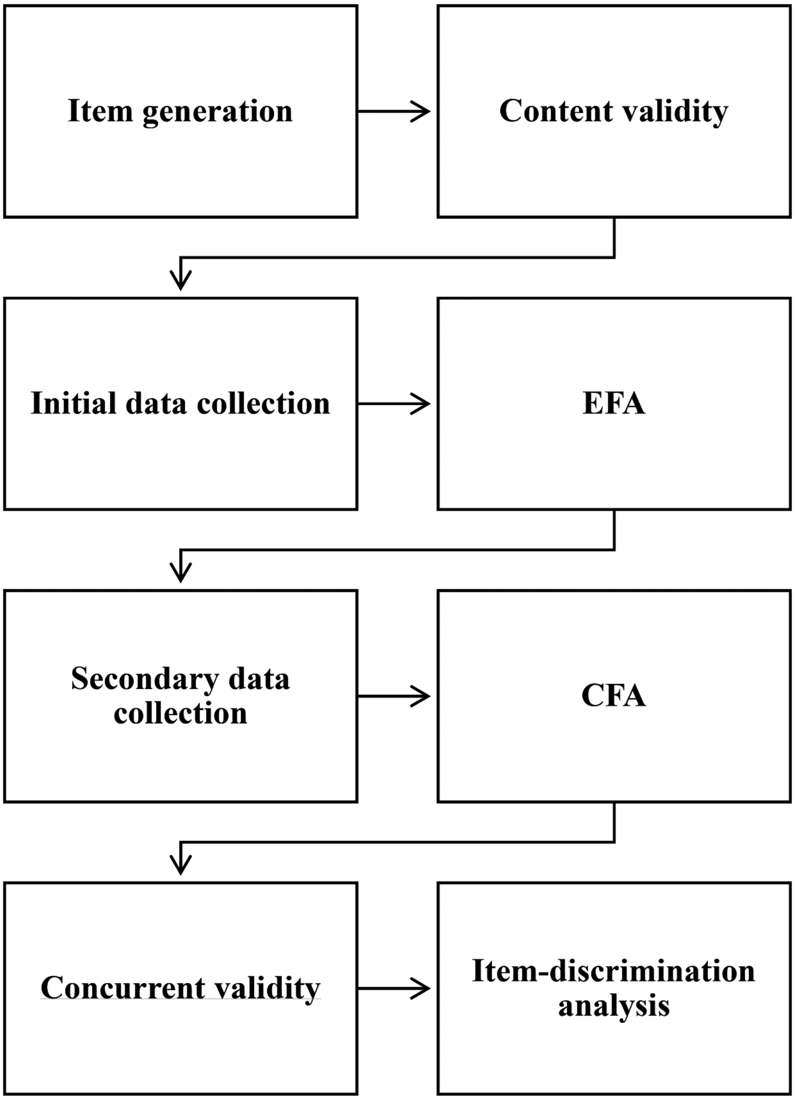

Figure 1. Scale development process.

the new scale. Prior research developed a tool measuring crime committed by using information systems.[4] The researchers enhanced and tailored existing tools by considering the existing legislations and panel codes and focusing on cybercrimes that can be committed on social media. The researchers aimed to develop sample items that adequately represent the construct under investigation to establish content validity. The researchers endeavored to generate short, simple, and easy to understand statements that measure only one concept at a time.

The initial items were evaluated by expert panel including three experts with a doctorate degree in measurement and evaluation, law, and cybersecurity. The experts panel assessed each item by labeling them as "should be removed, revised or appropriate." The implementation of the suggested modifications helped researchers reach the 25-item final form. The final form was written in both Turkish and English languages.

Participants and procedure

The "institutional review board" of the affiliated university approved this study (#2022-2). Data obtained from the participants with full informed consent. The study used a purposive sampling methodology and population of the study was active social media users. The first study consists of 545 social media users who have a mean age of 21.99 years ±6.71 (ranged between 14 and 58). In all, 55% of the participants were male (300 male and 245 female). 86.6% of the participants were students and their class levels were 42.9% freshmen, 23.3% sophomores, 9.5% were juniors, 7.9% were seniors, and 3% graduate students (master or doctorate). 20.7% of the respondents stated that they use social media 1–2 hours per day, while 42.8% of the respondents use social media 3–4 hours, 24.8% of the respondents use social media 5–6 hours, 6.4% of the respondents use social media 7–8 hours, and 4.4% of the

Table 2. Descriptive statistics of participants.

		Frequency	Percent (%)
Gender	Male	300	55
	Female	245	45
Class level	Freshmen	234	42.9
	Sophomores	127	23.3
	Juniors	52	9.5
	Seniors	43	7.9
	Graduate students	16	3
	Not a student	73	13.4
Social media usage	1–2 hours	113	20.7
	3–4 hours	233	42.8
	5–6 hours	135	24.8
	7–8 hours	35	6.4
	Over 8 hours	29	4.4

respondents use social media over 8 hours. The results showed that YouTube, Twitter, Instagram, and WhatsApp were the most used social media apps. Table 2 shows descriptive statistics for the demographic characteristics of the respondents.

Exploratory factor analysis

EFA with principal-components-analysis as factor extraction method was used to determine underlying factor structure of the new scale. After the third run, two items were eliminated since they failed to load significantly and one item was eliminated since it significantly loaded on two factors. The results of the principal-component-analysis with varimax-rotation indicated one-factor structure with 22 items, explaining 52.51% of the total variance. Scree plot shown in Figure 2 indicates the eigen value related to each principal component.

KMO (.973) and Bartlett's test results (χ^2 (DF = 231) = 7225.472, $p < .001$) revealed the items were suitable for a factor analysis. Loadings were ranged between .655 and .790, which were greater than the threshold of .40.[44] Moreover, communalities were ranged between .429 and .625, which were greater than the threshold of .30.[45] Internal consistency reliability of the scale was tested by conducting a reliability analysis. Cronbach's alpha of the scale was found as .957. The scale having a Cronbach's alpha over .70 indicated a good internal consistency reliability.[41] Further, skewness (SE = .105) and kurtosis (SE = .209) measures were ranged between +3 and −3, indicating that the data show a normal distribution.[44] Table 3 shows descriptive statistics along with factor analysis, reliability and normality results.

Study 2

Sample and procedure

The second study consisted of 500 participants (mean age = 21.99 SD = 6.97). The participants' age ranged from 14 to 60. In all, 56.2% of the participants were male (281 male and 219 female). Most of the participants were students (87%). Regarding their class level 36.6% of the respondents were freshmen, 23.4% were sophomores, 9.2% were juniors, 7.8% were seniors, and 3% were graduate students (13% were not a student). The participants declared that 21.2% of them spent less than 2 hours per day on social media, 42.8% of them spent more than 2 hours, 23.8% of them spent more than 4 hours, 6.8% of them spent more than 6 hours, and 5.4% of them spent more than 8 hours.

Instruments

"Cybercrime Awareness on Social Media Scale" (CASM-S)

The CASM-S was developed and tested in this study. The scale has 22 items rated on a five-point Likert scale ranging from "1 = strongly disagree" to "5 = strongly agree." Appendix shows scale items and scoring information.

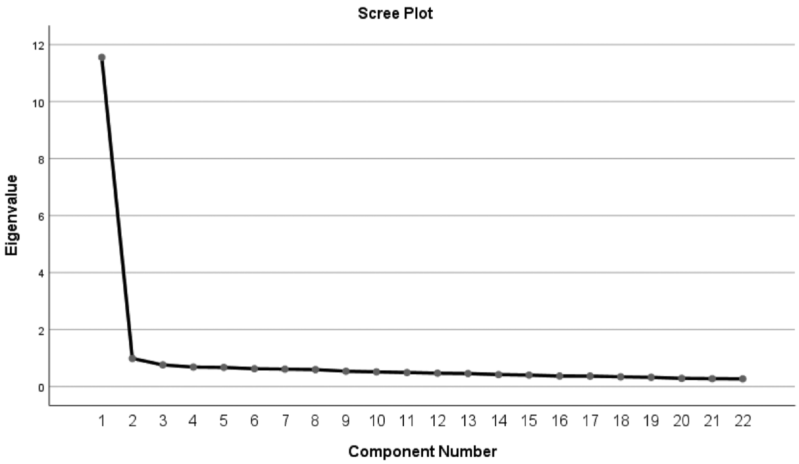

Figure 2. Scree plot.

Table 3. Pattern matrix and descriptive statistics.

Items	Mean	SD	Communality	Factor Loading	Alpha if Item Deleted	Skew.	Kurt.
Item1	4.15	1.08	.556	.746	.954	−1.117	.384
Item2	4.15	1.04	.543	.737	.954	−1.064	.405
Item3	4.08	1.04	.471	.686	.955	−.957	.152
Item4	4.11	1.07	.510	.714	.955	−1.126	.601
Item5	4.13	1.03	.599	.774	.954	−.969	.207
Item6	3.99	1.05	.429	.655	.955	−.790	−.145
Item7	4.08	1.09	.570	.755	.954	−.999	.113
Item8	4.09	1.07	.574	.758	.954	−.995	.232
Item9	4.02	1.09	.465	.682	.955	−.958	.172
Item10	3.99	1.07	.506	.711	.955	−.941	.247
Item11	4.06	1.04	.510	.714	.955	−.940	.169
Item12	3.98	1.09	.453	.673	.955	−.867	−.026
Item13	4.09	1.02	.556	.746	.954	−1.062	.630
Item14	4.09	1.00	.621	.788	.954	−.897	.115
Item15	4.20	1.04	.625	.790	.954	−1.200	.690
Item16	4.11	1.07	.554	.744	.954	−1.083	.366
Item17	4.10	1.07	.492	.702	.955	−1.122	.637
Item18	3.99	1.05	.461	.679	.955	−.830	.030
Item19	4.15	1.04	.563	.750	.954	−1.084	.492
Item20	4.13	1.05	.560	.748	.954	−1.059	.353
Item21	4.06	1.01	.499	.706	.955	−.974	.462
Item22	3.95	1.07	.434	.659	.955	−.833	.000

"Information Security Awareness Scale" (ISAS)

The ISAS consists five factors and 18 items.[46] The five-point scale was rated from "1 = strongly disagree" to "5 = strongly agree." Cronbach's alpha of the total scale was reported as .839. While Cronbach's alpha of the ISAS was calculated as .938 in the present study.

Factorability and reliability

Bartlett's test (χ^2(DF = 231) = 6129.443, $p < .001$) and "K-M-O measure of sampling adequacy" (.970) results confirmed factorability of the study data. Communalities were ranged between .444 and .632. Communalities higher than .30 were considered significant.45 Factor loadings were ranged between .624 and .778, which were greater than the minimum threshold of .40.[44] Cronbach's alpha value was calculated as .952 in the second study. This value is much greater than the threshold value of .70.[47]

Confirmatory factor analysis

CFA was conducted by using SPSS AMOS to test the measurement model. The results indicated a good fit between the study data and measurement model: [x^2 = 576.31, DF = 209, x^2/DF = 2.757, GFI = .900, AGFI = .878, TLI = .932, CFI = .939, IFI = .939, SRMR = .0366, RMSEA = .059 LO90 = .054, HI90 = .065, PCLOSE = .004]. The model-fit estimates were within thresholds proposed by Kline (2005). This indicated that one-factor structure was the optimal model.

Concurrent validity

Concurrent validity, which is a type of criterion-related validity, was evaluated by Pearson correlation analysis between the "Cybercrime Awareness on Social Media Scale" (CASM-S) and "Information Security Awareness Scale" (ISAS). The correlation between CASM-S and ISAS was statistically significant (r = .855, $p < .001$). The high correlation between these scales revealed that individuals with higher scores in CASM-S more likely to have a greater level of awareness on information security.

Item-discrimination analysis

An item-discrimination analysis was conducted by using the high-low-27-per-cent group method. An "independent sample t-test" was used to distinguish the 27% highest (M = 105.10, SD = 2.26) and 27% lowest (M = 66.9, SD = 13.4) group. The results indicated that the scale had a sufficient discriminating power t (270) = 38.206, $p < .001$.

The study further investigated gender differences in the total scores obtained by the proposed scale. Total scores in the scale ranged between 22 and 110 in which male (N = 281, M = 86.22, SD = 17.16) scored lower on the scale than did female (N = 219, M = 90.31, SD = 15.47). The "independent sample t-test" results revealed a statistically significant difference between female and male participants (t (498) = 2.754, p = .006. The results showed that females have a greater level of cybercrime awareness on social media.

Discussion and conclusion

Cybercrime is a type of crime committed by using electronic devices through Internet access against organizations or individuals.[48] Nzeakor et al.[49] reported that the amount of cybercrime victimization is much greater than the number of conventional crimes and cybercrime victimization rates of identity theft, online credit card fraud, phishing, and unauthorized access to accounts are increasing on daily basis. Prior findings indicated that cybercrime victimization rates are higher in undeveloped countries, highlighting the need for prevention interventions in those countries.[50]

Global cybersecurity agenda defined seven strategic goals toward curbing cybercrime scourge, including institutional/organizational, technical, legal, international cooperation, law enforcement/capacity building, public awareness strategies, and public–private partnership.[50] Hadlington[51] argued that there is a positive correlation between cybercrime awareness and cybercrime control and prevention. On the other hand, the review of the existing literature indicated that there was no scale available to measure users' cybercrime awareness level on social media platforms. Accordingly, this study focused on developing a scale for measuring the level of cybercrime awareness on social media.

The present study evaluated psychometric characteristics of the scale based on data obtained from 1045 social media users. The EFA was used to identify factor structure of the proposed scale. The results suggested that the scale has a one-factor structure and an adequate internal reliability ($\alpha = .957$). The factor structure of the CASM-S was confirmed by conducting a CFA. The results revealed the one-factor model fits the study data well ($x^2/DF = 2.757$, CFI = .939, SRMR = .0366, RMSEA = .059). Further, the study evaluated the concurrent validity of the scale by investigating correlation between the CASM-S and ISAS ($r = .855$, $p < .001$). The item discrimination analysis indicated that the proposed scale had a sufficient discriminating power. Finally, there was a statistically significant difference between male and female participants, where females have a greater level of cybercrime awareness on social media. This finding therefore calls for more effective cybercrime awareness campaign targeted at male users on social media.

Altogether, these findings revealed that CASM-S is a valid and reliable instrument to measure users' cybercrime awareness level on social media. The scale relies on 22 Likert items and total score can range between 22 to 110. The higher scores on the proposed scale reflect higher levels of cybercrime awareness on social media platforms. The scale has a unidimensional factor structure and there are no reverse-scored items. While using the proposed scale in a future study, the researchers should be careful about social desirability bias since the scale includes self-reported items to measure a sensitive topic.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Ibrahim Arpaci http://orcid.org/0000-0001-6513-4569
Omer Aslan http://orcid.org/0000-0003-0737-1966

References

1. Photon Research Team. Cybercrime and dark web research. How cybercriminals weaponize social media. [accessed 2022 July 5]. https://www.digitalshadows.com/blog-and-research/how-cybercriminals-weaponize-social-media.
2. Threat Post. Cybercrime getting more sophisticated: how to protect your business? [accessed 2022 July 5]. https://threatpost.com/cybercrime-more-sophisticated/179676.
3. Arpaci I, Sevinc K. Development of the cybersecurity scale (CS-S): evidence of validity and reliability. Inf Dev. 2022;38(2):218–26. doi:10.1177/0266666921997512.
4. Ateş E. Siber suç farkındalık ölçeği geliştirme: geçerlik ve güvenirlik çalışması [Master's thesis]. Tokat (TR): Gaziosmanpasa University; 2021.
5. Kaspersky. Tips on how to protect yourself against cybercrime. [accessed 2022 July 5]. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.
6. Aslan O, Samet R. A comprehensive review on malware detection approaches. IEEE Access. 2020;8:6249–71. doi:10.1109/access.2019.2963724.
7. Aslan Ö, Samet R, Tanrıöver ÖÖ. Using a subtractive center behavioral model to detect malware. Secur Commun Network. 2020;2020:1–17. doi:10.1155/2020/7501894.
8. Aslan O, Ozkan-Okay M, Gupta D. Intelligent behavior-based malware detection system on cloud computing environment. IEEE Access. 2021;9:83252–71. doi:10.1109/access.2021.3087316.
9. Morgan S. 2019/2020 Cybersecurity Almanac: 100 facts, figures, predictions and statistics. [accessed 2022 July 5]. https://cybersecurityventures.com/cybersecurity-almanac-2019.
10. Chadd K. The history of cybersecurity. [accessed 2022 July 5]. https://blog.avast.com/history-of-cybersecurity-avast.
11. Lehtinen R, and Gangemi GT Sr. Computer security basics: computer security. Chambersburg, PA. (US): O'Reilly Media; 2006.
12. Trend Micro. What you need to know about the LockerGoga ransomware. [accessed 2022 July 5]. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

13. Research and Analysis. CovidLock: android ransomware spreading amid COVID-19 epidemic; 2020 [accessed 2022 July 5]. https://cyware.com/research-and-analysis/covidlock-android-ransomware-spreading-amid-covid-19-epidemic-4a5b.
14. Manky D. Cybercrime as a service: a very modern business. Comput Fraud Secur. 2013;2013(6):9–13. doi:10.1016/s1361-3723(13)70053-8.
15. Zaharia A. 300+ terrifying cybercrime and cybersecurity statistics (2022 edition). Comparitech. [accessed 2022 July 5]. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.
16. Arpaci I, Karatas K, Kiran F, Kusci I, Topcu A. Mediating role of positivity in the relationship between state anxiety and problematic social media use during the COVID-19 pandemic. Death Stud. 2021:1–11. doi:10.1080/07481187.2021.1923588.
17. Mohsin M. 10 Facebook statistics every marketer should know in 2021. [accessed 2022 July 5]. https://www.oberlo.com/blog/facebook-statistics.
18. The Defence Works. How social media is used in cybercrimes. [accessed 2022 July 5]. https://thedefenceworks.com/services/cyber-and-security-awareness/guides/how-social-media-is-used-in-cybercrimes/ .
19. Lazic M. 39 worrying cyber crime statistics [updated for 2022]. LegalJobs. [accessed 2022 July 5]. https://legaljobs.io/blog/cyber-crime-statistics/.
20. Soomro TR, Hussain M. Social media-related cybercrimes and techniques for their prevention. Appl Comput Syst. 2019;24(1):9–17. doi:10.2478/acss-2019-0002.
21. Vanitha A, Balakrishnan N. A responsiveness model for privacy conservation against antagonist and fake user in cyber-physical and online social networks. J Phys Conf Ser. 2021;1767(1):012051. doi:10.1088/1742-6596/1767/1/012051.
22. Koohang A, Sargent CS, Nord JH, Paliszkiewicz J. Internet of Things (IoT): from awareness to continued use. Int J Inf Manage. 2022;62(102442):102442. doi:10.1016/j.ijinfomgt.2021.102442.
23. Koohang A, Floyd K, Yerby J, Paliszkiewicz J. Social media privacy concerns, security concerns, trust, and awareness: empirical validation of an instrument. Issues Inf Syst. 2021;22(2):133–45. doi:10.48009/2_iis_2021_136-149.
24. Buono L. Fighting cybercrime through prevention, outreach and awareness raising. ERA Forum. 2014;15(1):1–8. doi:10.1007/s12027-014-0333-4.
25. Koohang A, Anderson J, Nord JH, Paliszkiewicz J. Building an awareness-centered information security policy compliance model. Ind Manage Data Syst. 2019;120(1):231–47. doi:10.1108/imds-07-2019-0412.
26. Koohang A, Nowak A, Paliszkiewicz J, Nord JH. Information security policy compliance: leadership, trust, role values, and awareness. J Comput Inf Syst. 2020;60(1):1–8. doi:10.1080/08874417.2019.1668738.
27. Saridakis G, Benson V, Ezingeard JN, Tennakoon H. Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technol Forecast Soc Change. 2016;102:320–30. doi:10.1016/j.techfore.2015.08.012.
28. Almansoori A, Alshamsi M, Abdallah S, and Salloum SA. Analysis of cybercrime on social media platforms and its challenges. Proceedings of the international conference on artificial intelligence and computer vision (AICV2021). Advances in intelligent systems and computing. Settat, Morocco: Springer International Publishing; 2021. p. 615–25. doi:10.1007/978-3-030-76346-6_54.
29. Yeboah-Ofori A, Brimicombe A. The society of digital information and wireless communication. cyber intelligence and OSINT: developing mitigation techniques against cybercrime threats on social media. Int J Cyber-Secur Digit Forensics. 2018;7(1):87–98. doi:10.17781/p002378.
30. Arpaci I. What drives students' online self-disclosure behaviour on social media? A hybrid SEM and artificial intelligence approach. Int J Mob Commun. 2020;18(2):229. doi:10.1504/ijmc.2020.105847.
31. Ismailova R, Muhametjanova G, Medeni TD, Medeni IT, Soylu D, Dossymbekuly OA. Cybercrime risk awareness rate among students in Central Asia: a comparative study in Kyrgyzstan and Kazakhstan. Inf Secur J Glob Perspect. 2019;28(4–5):127–35. doi:10.1080/19393555.2019.1685142.
32. Alzubaidi A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon. 2021;7(1):e06016. doi:10.1016/j.heliyon.2021.e06016.
33. Gharieb ME. Knowing the level of information security awareness in the usage of social media among female secondary school students in Eastern Makkah Al-Mukarramah-Saudi Arabia. Int J Comput Netw Secur. 2021;21:360–68.
34. Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Big Data Cogn Comput. 2021;5(2):23. doi:10.3390/bdcc5020023.
35. Alwanain MI. Phishing awareness and elderly users in social media. Int J Comput Sci Netw Secur. 2020;20(9):114–19. doi:10.22937/IJCSNS.2020.20.09.14.
36. Karagiannopoulos DV, Kirby DA, Oftadeh-Moghadam SM, Sugiura DL. Cybercrime awareness and victimisation in individuals over 60 years: a Portsmouth case study. Comput Law Secur Rep. 2021;43(105615):105615. doi:10.1016/j.clsr.2021.105615.
37. Alwanain MI. How do children interact with phishing attacks? Int J Comput Sci Netw Secur. 2021;21(3):127–33. doi:10.22937/IJCSNS.2021.21.3.17.
38. American Educational Research Association, American Psychological Association, National Council on Measurement in Education. Standards for educational and psychological testing. Washington (DC): American Educational Research Association; 1999.
39. Hinkin TR. A brief tutorial on the development of measures for use in survey questionnaires. Organ Res Methods. 1998;1(1):104–21. doi:10.1177/109442819800100106.
40. Kerlinger FN, and Lee HB. Foundations of behavioral research. Orlonda, FL. (US): Wadsworth Publishing Company; 2008.
41. Nunnally JC, and Bernstein I. Psychometric Theory. New York, US: McGraw Hill Higher Education; 1993.
42. Campbell JR. Psychometric theory. In: Dunnette MD, editor. Handbook of industrial and organizational psychology. Chicago (US): Rand McNally. 1976. p. 185–222.
43. Anderson JC, Gerbing DW. Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. J Appl Psychol. 1991;76(5):732–40. doi:10.1037/0021-9010.76.5.732.

44. Hair JF, Black WC, Babin BJ, Anderson RE, and Tatham RL. Pearson new international edition. Multivariate data analysis. Seventh ed. Harlow, Essex (UK): Pearson Education Limited Harlow; 2014.
45. Child D. Essentials of Factor Analysis. London, UK: A&C Black; 2006.
46. Erdoğmuş A. Üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki etkilerinin analizi: afyon Kocatepe Üniversitesi örneği [Master's thesis]. Afyon (TR): Afyon Kocatepe University; 2017. [accessed 2022 July 5]. http://acikerisim.aku.edu.tr/xmlui/handle/11630/6277
47. Cronbach LJ. Coefficient alpha and the internal structure of tests. Psychometrika. 1951;16(3):297–334. doi:10.1007/bf02310555.
48. Halder D, Jaishankar K. Cyber crime and the victimization of women: laws, rights and regulations. Hershey (PA): IGI Global; 2011.
49. Nzeakor OF, Nwokeoma BN, Ezeh PJ. Pattern of cybercrime awareness in Imo state, Nigeria: an empirical assessment. Int J Cyber Criminol. 2020;14:283–99.
50. Malby S, Mace R, Holterhof A, Brown C, Kascherus S, Ignatuschtschenko E. Comprehensive study on cybercrime. United Nations Office on Drugs and Crime. [accessed 2022 July 5]. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
51. Hadlington LJ. Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom. Int J Cyber Criminol. 2018;12(1):262–74. doi:10.5281/zenodo.495776.

Appendix. Cybercrime Awareness on Social Media Scale (CASM-S)

(1) "It is a crime to break into someone else's social media account without permission."
(2) "It is a crime to share personal data with third parties without the user's knowledge."
(3) "There is a punishment for the violation of investigation confidentiality on social media."
(4) "It is a crime to promote the use of harmful substances on social media."
(5) "Posts that support terrorist organizations on social media constitute a crime."
(6) "Unfounded political and military posts on social media constitute a crime."
(7) "It is a crime to sell illegal (fake or stolen) products on social media."
(8) "It is a crime to direct individuals to illegal sites through links on social media."
(9) "Illegal betting/gambling on social media is a crime."
(10) "Sharing copyrighted works on social media is a crime."
(11) "I know that using insulting expressions on social media is a crime."
(12) "It is a crime to record video or audio on social media without permission."
(13) "It is a crime to reveal secrets related to confidential duties on social media."
(14) "I know that it is a crime to gain unfair advantage through illegal posts on social media."
(15) "I am aware that harassing another person on social media is a crime."
(16) "I am aware that cyberbullying on social media is a crime."
(17) "I am aware that sexual content will not be shared on social media."
(18) "Sharing violent images on social media is a crime."
(19) "I know that it is a crime to spread malicious software using social media."
(20) "It is necessary to file a criminal complaint against those who violate the privacy of individual life on social media."
(21) "I am aware that fake news spread on social media constitute a crime."
(22) "Share of unlicensed software on social media is a crime."

Scoring: The CASM-S has 22 items which rated on a "five-point Likert-type scale" ranging from "strongly disagree (1)" to "strongly agree (5)." The scale has a unidimensional factor structure and there are no reverse-scored items. Total scores can range between 22 to 110, a higher score shows a greater level of cybercrime awareness on social media.