# Development of the cybercrime awareness scale (CAS): a validity and reliability study in a Turkish sample

Ibrahim Arpaci
*Software Engineering, Faculty of Engineering and Natural Sciences, Bandirma Onyedi Eylul University, Balikesir, Turkey, and*
Ersin Ateş
*Computer Education and Instructional Technology, Faculty of Education, Tokat Gaziosmanpasa University, Tokat, Turkey*

Received 25 January 2022
Revised 18 June 2022
3 August 2022
Accepted 23 August 2022

## Abstract

**Purpose** – Cybercrimes increase day by day in parallel to cyber-attacks and cyber-threats. Due to such an increase, required cybersecurity precautions against all kinds of cyber-attacks and cyber-threats should be taken by both organizations and individuals. This study aims to develop a reliable and valid measurement tool to measure cybercrime awareness levels of individuals.

**Design/methodology/approach** – In this study, a scale named as Cybercrime Awareness Scale (CAS) has been developed and psychometric properties of the scale have been tested by two separate studies.

**Findings** – The first study included a total of 500 respondents (294 female and 206 male). In the first study, factor structure of the proposed scale has been determined through an exploratory factor analysis. The results revealed a three-factor structure (i.e. information systems crimes, personal data crimes, and privacy and security). Cronbach's alpha reliability coefficients for the subdimensions were 0.95, 0.92, and 0.90, respectively. The sample of the second study consisted of 494 respondents (281 female and 213 male). The confirmatory-factor-analysis results revealed that three-factor structure is valid and optimal model. Further, the proposed scale demonstrated moderate concurrent validity results in relation to the Digital Data Security Awareness Scale.

**Originality/value** – Findings indicated that the CAS is a valid and reliable measurement tool to measure individuals' cybercrime awareness level. This study makes a novel contribution to the existing cybersecurity literature by providing the CAS, which is developed by following rigorous methodological standards.

**Peer review** – The peer review history for this article is available at: https://publons.com/publon/10.1108/OIR-01-2022-0023/

**Keywords** Awareness, Cybercrime, Cybercrime awareness scale, CAS, Scale development

**Paper type** Research paper

## Introduction

Cybercrimes target the security of an information system and related user data (Arpaci and Sevinc, 2022). The most basic feature that distinguishes cybercrimes from other crimes is that they cannot be committed without an information system (Ates, 2021). Therefore, this type of crime is also called as computer and Internet crimes (EGM, 2022). Information systems affect the structure and functioning of organizations, change characteristics of the products purchased and affect the entire nature of doing business (Arpaci and Aslan, 2022). Technological developments and diffusion of new technologies created new opportunities, but also emerged new threats and security incidents (Abbas *et al.*, 2022).

It is worthwhile to note that cybercrimes vary more than other crimes and types of cybercrimes constantly update themselves. It is argued that the rapid action in the legal

This study is based on a master's thesis presented to the "Department of Computer Education and Instructional Technology" at "Tokat Gaziosmanpasa University" on October 2021.

Online Information Review

1468-4527
DOI 10.1108/OIR-01-2022-0023

regulation studies is related to the level of development of the countries (Budak, 2015). The severity of cybercrimes has been understood by developing countries much later and legal arrangements that need to be made in relation to cybercrimes have started to be made by the developing countries, but they are still insufficient.

Crimes such as copyright violations, obscenity, insults, interactive fraud, theft of personal data, blocking of communication, and seizure of bank/card information are among the most common types of cybercrimes (İlbaş and Köksal, 2011). In order not to be exposed to these crimes, it is necessary to develop robust policies on information systems and information security at both individual and institutional levels (Whitman and Mattord, 2012). Most of crimes such as theft, fraud, cyberbullying, violation of privacy, and seizure of personal information have become possible without the need to be in the same place as the victim. Further, information systems have increased the communication opportunities of criminal groups or terrorist organizations and facilitated their propaganda opportunities.

In order to deal with the Internet-related security incidents, one must first be aware of potential cybersecurity crimes. Training individuals on this issue and increasing their awareness level of cybercrime will enable them to take precautions against cybercrimes and threats. Accordingly, this study aims to develop a new scale named as "Cybercrime Awareness Scale" (CAS) to measure individuals' cybercrime awareness level.

## Related studies

In the literature, there are some other tools that measure cybercrime awareness level of individuals. For example, Rajasekar (2011) proposed a tool to measure cybercrime awareness with 21 positive and 15 negative items. It is argued that the higher the total score obtained when the negative items are reversed, the higher the cybercrime awareness will be. It is important to note that Rajasekar's scale (2011) measured the participants' awareness about cybercrime terms such as spamming, assault by threat, social engineering, sniffing, corporate espionage, email spoofing, cracking, spoofing, cheating, fraud, cyber-defamation, cyber-harassment, cyber-terrorism, cyber-pornography, cyber-stalking, cyber-trespass, cyber-warfare, cyber-squatting, cyber-extortion, cyber-vandalism, and web-jacking.

Abuda *et al.* (2020) developed another tool to measure cybercrime awareness level of high school students in Philippines and validated the tool in a sample of 200 students. The tool consists of 18 items and it has a four-factor structure named as "awareness on phishing, awareness on spamming, perceived effectiveness of antivirus software, and bullying on the web." The tool includes general statements such as "I know some of the cyber laws; I protect myself from cybercrime; I think that antiviruses are enough to protect me from a cybercrime; I trust any website that asks me to enter my bank account detail." Similarly, Tibi *et al.* (2019) developed a tool to measure cybercrime awareness level and validated this tool in a sample of 73 Arab college students. The tool consists of 23 items and it has a single-factor structure. They include general statements such as "I know what cybercrime is; I heard about phishing; I know some cyber laws."

Some exploratory studies were conducted to evaluate the current cybercrime awareness and threats in different countries. For example, Mesko and Bernik (2011) investigated knowledge, awareness, and fear of cybercrime in Slovenia. They developed an online questionnaire consisted of 28 closed-ended questions and two-parts ("awareness and knowledge of cybercrimes" and "fear of cybercrimes"). Respondents were 277 individuals aged between 19 and 48 years. Their results showed that respondents are quite aware of various types of cybercrimes and threats in cyberspace. Further, they found that more educated and older respondents are less afraid of cybercrimes. In another study, Nzeakor *et al.* (2020) investigated public awareness of cybercrime in Nigeria. They collected data from 1,031 individuals by using a questionnaire and interviews. They found that older and more

educated respondents have a higher level of awareness on cybercrimes. Finally, Zayid *et al.* (2017) investigated cybercrime awareness and risks in Saudi Arabia based on data collected from 135 male university students whose ages ranged between 18 and 25 years. Their results indicated that a cybercrime may come from financial, political, sexual, and cultural reasons. They found that awareness level of the respondents about cybercrimes and threats is quite weak.

## Method

### *Content validity*

This study is a scale development study aimed at determining individuals' cybercrime awareness level. In the first place, an item pool consisting of 90 items was generated by the study researchers by taking into account the cybercrime legislations and the cybercrime types in the Turkish penal code. The scale items were developed in Turkish language but later on translated into English by a translation-back translation procedure. The item pool was evaluated by three field experts who has a PhD in forensic informatics, information systems, and measurement and evaluation, respectively. The expert panel scored the items from 1 to 10. Davis (1992) proposed that researchers should consider 80% agreement or higher among judges for a new instrument. If the Content Validity Index (CVI) for an item is between 70 and 79%, it should be revised. If the CVI is less than 70%, the item should be eliminated. Accordingly, 47 items were eliminated and 15 items were revised. After the first revision, the item pool was sent to the field experts for a second revision and the final 43-item form was obtained with a consensus.

### *Procedure*

The final draft of the scale was applied to the first sample group of 500 participants via Google Forms. Then an "Exploratory Factor Analysis" (EFA) was performed by using SPSS software. The revised scale having three subdimensions was applied to a different sample group consisting of 494 respondents. The "Confirmatory Factor Analysis" (CFA) was performed by using AMOS software. Finally, the concurrent validity of the proposed scale was tested.

All research procedures comply with ethical standards and the research was approved by the Research-Ethics Committee of the affiliated university (17/11/2020-E.51622). Participants were informed about the purpose of the study and voluntary participation consent was obtained from all participants in the online form.

### *Measures*

Demographic information questionnaire (e.g. gender, age, Internet usage), "Digital Data Security Awareness Scale", and the CAS were used as measurement tools. The CAS has a five-point Likert-type (See Appendix). The degree of agreement of the scale was determined as "strongly disagree (1), disagree (2), neither agree nor disagree (3), disagree (4) and strongly agree (5)."

Digital Data Security Awareness Scale is a reliable and valid scale consisting of 32 items in five-point Likert type (Yılmaz, 2015). The EFA and CFA were performed with 529 and 335 teachers, respectively. The scale has a single factor structure where factor loads vary between 0.506 and 0.689. The internal consistency reliability coefficient ($\alpha$) was reported as 945. Sample items for the scale include "I am careful to create passwords that others cannot guess; I know the importance of using antivirus software; I have knowledge of firewall software; I am aware that files can be password-protected to prevent unauthorized use; I am aware that unlicensed software can create security vulnerabilities."

## Results

*Study I*

*Sample*. Sample of the first study consists of 500 university students. Participants were selected by using a convenience sampling technique. There were 294 female (58.8%) and 206 male (41.2%) participants with a mean age of 24.80 (SD = 2.60, between 17–48 years). The results showed that most of the participants (92.8%) use mobile Internet, 71.4% of the participants use e-commerce, and 74.6% of them use e-government services. The results further indicated that only 11.8% of the participants have received a training related to cybercrimes and 14% of them have been subjected to a cyber-attack.

**Table 1.** Rotated component matrix

| Items | Communalities | Factor 1 | Factor 2 | Factor 3 |
|---|---|---|---|---|
| Item-20 | 0.603 | 0.542 | | |
| Item-21 | 0.559 | 0.599 | | |
| Item-22 | 0.549 | 0.467 | | |
| Item-23 | 0.657 | 0.658 | | |
| Item-26 | 0.663 | 0.584 | | |
| Item-27 | 0.496 | 0.553 | | |
| Item-28 | 0.669 | 0.748 | | |
| Item-29 | 0.680 | 0.750 | | |
| Item-30 | 0.746 | 0.782 | | |
| Item-31 | 0.410 | 0.459 | | |
| Item-32 | 0.560 | 0.695 | | |
| Item-33 | 0.546 | 0.629 | | |
| Item-34 | 0.633 | 0.713 | | |
| Item-36 | 0.620 | 0.605 | | |
| Item-40 | 0.635 | 0.673 | | |
| Item-41 | 0.475 | 0.426 | | |
| Item-1 | 0.570 | | 0.732 | |
| Item-2 | 0.573 | | 0.685 | |
| Item-3 | 0.505 | | 0.639 | |
| Item-4 | 0.373 | | 0.461 | |
| Item-5 | 0.706 | | 0.741 | |
| Item-6 | 0.402 | | 0.517 | |
| Item-7 | 0.572 | | 0.672 | |
| Item-8 | 0.681 | | 0.674 | |
| Item-9 | 0.606 | | 0.643 | |
| Item-10 | 0.634 | | 0.641 | |
| Item-11 | 0.690 | | 0.640 | |
| Item-13 | 0.498 | | 0.446 | |
| Item-14 | 0.715 | | 0.661 | |
| Item-17 | 0.692 | | 0.620 | |
| Item-19 | 0.559 | | 0.459 | |
| Item-24 | 0.663 | | 0.540 | |
| Item-35 | 0.546 | | 0.509 | |
| Item-12 | 0.385 | | | 0.442 |
| Item-15 | 0.350 | | | 0.522 |
| Item-16 | 0.499 | | | 0.634 |
| Item-18 | 0.487 | | | 0.646 |
| Item-25 | 0.452 | | | 0.496 |
| Item-37 | 0.493 | | | 0.552 |
| Item-38 | 0.544 | | | 0.516 |
| Item-39 | 0.572 | | | 0.463 |
| Eigenvalue | | 19.501 | 2.168 | 1.426 |
| Explained variance | | 45.352 | 5.041 | 3.316 |
| Total variance explained | | | | 53.709 |

*Exploratory factor analysis.* The EFA was carried out to determine factor structure and psychometric properties of the proposed scale. The Kaiser–Meyer–Olkin indices of sampling adequacy were 0.957 and Bartlett's sphericity test results were significant ($x^2$(DF = 903) = 15,408.501). The results showed that the data are suitable for the factor analysis. In the first run, two items with a factor load below 0.30 were removed (Seçer, 2013). In the later runs, factor loads as a result of varimax rotation varied between 0.426 and 0.782. In the final run, a three-factor structure was obtained and 41 items were remained. Eigenvalue of the three factors were greater than one. Results showed the first factor explains 45.35% of the variance and it has an eigenvalue of 19.5. The second factor explains an additional 5.04%

| Substances | Mean | S.D. | Corrected item-total correlation | Cronbach's alpha if item deleted | *t* |
|---|---|---|---|---|---|
| Item 1 | 4.92 | 0.452 | 0.558 | 0.967 | 3.867*** |
| Item 2 | 4.87 | 0.505 | 0.645 | 0.966 | 5.473*** |
| Item 3 | 4.85 | 0.544 | 0.587 | 0.966 | 5.831*** |
| Item 4 | 4.71 | 0.700 | 0.554 | 0.967 | 8.375*** |
| Item 5 | 4.87 | 0.496 | 0.737 | 0.966 | 5.998*** |
| Item 6 | 4.77 | 0.678 | 0.566 | 0.967 | 7.277*** |
| Item 7 | 4.83 | 0.583 | 0.654 | 0.966 | 6.140*** |
| Item 8 | 4.84 | 0.581 | 0.759 | 0.966 | 6.922*** |
| Item 9 | 4.85 | 0.515 | 0.700 | 0.966 | 6.192*** |
| Item 10 | 4.87 | 0.510 | 0.741 | 0.966 | 5.824*** |
| Item 11 | 4.87 | 0.473 | 0.781 | 0.966 | 6.368*** |
| Item 12 | 4.50 | 1.000 | 0.388 | 0.969 | 9.758*** |
| Item 13 | 4.78 | 0.690 | 0.689 | 0.966 | 7.301*** |
| Item 14 | 4.88 | 0.487 | 0.800 | 0.966 | 5.793*** |
| Item 15 | 4.64 | 0.731 | 0.477 | 0.967 | 8.642*** |
| Item 16 | 4.65 | 0.781 | 0.557 | 0.967 | 10.213*** |
| Item 17 | 4.82 | 0.559 | 0.786 | 0.966 | 7.519*** |
| Item 18 | 4.63 | 0.798 | 0.521 | 0.967 | 9.222*** |
| Item 19 | 4.78 | 0.605 | 0.726 | 0.966 | 8.040*** |
| Item 20 | 4.85 | 0.503 | 0.738 | 0.966 | 6.991*** |
| Item 21 | 4.86 | 0.505 | 0.765 | 0.966 | 6.389*** |
| Item 22 | 4.87 | 0.459 | 0.712 | 0.966 | 6.268*** |
| Item 23 | 4.86 | 0.491 | 0.692 | 0.966 | 6.734*** |
| Item 24 | 4.87 | 0.497 | 0.771 | 0.966 | 6.255*** |
| Item 25 | 4.56 | 0.853 | 0.586 | 0.967 | 12.415*** |
| Item 26 | 4.85 | 0.501 | 0.660 | 0.966 | 7.100*** |
| Item 27 | 4.79 | 0.591 | 0.657 | 0.966 | 8.509*** |
| Item 28 | 4.85 | 0.506 | 0.676 | 0.966 | 7.337*** |
| Item 29 | 4.83 | 0.562 | 0.710 | 0.966 | 7.420*** |
| Item 30 | 4.84 | 0.556 | 0.645 | 0.966 | 6.877*** |
| Item 31 | 4.76 | 0.654 | 0.497 | 0.967 | 8.719*** |
| Item 32 | 4.77 | 0.598 | 0.632 | 0.966 | 10.373*** |
| Item 33 | 4.63 | 0.720 | 0.599 | 0.966 | 10.674*** |
| Item 34 | 4.84 | 0.532 | 0.676 | 0.966 | 7.117*** |
| Item 35 | 4.86 | 0.512 | 0.749 | 0.966 | 6.395*** |
| Item 36 | 4.80 | 0.577 | 0.714 | 0.966 | 8.448*** |
| Item 37 | 4.79 | 0.582 | 0.627 | 0.966 | 8.960*** |
| Item 38 | 4.78 | 0.567 | 0.653 | 0.966 | 8.887*** |
| Item 39 | 4.82 | 0.534 | 0.726 | 0.966 | 8.321*** |
| Item 40 | 4.86 | 0.469 | 0.722 | 0.966 | 7.715*** |
| Item 41 | 4.77 | 0.635 | 0.669 | 0.966 | 8.172*** |

**Note(s):** *** $p < 0.001$

**Table 2.**
Reliability and item analysis results

of the variance (eigenvalue of 2.168), and the third factor explains 3.32% of the variance (eigenvalue of 1.426). The total variance explained was calculated as 53.709%. Table 1 shows the rotated component matrix with varimax rotation.

*Reliability*. Cronbach's alpha ($\alpha$) was calculated to check the internal consistency reliability coefficient of the scale. Reliability coefficient for the total scale was computed as 0.967. Besides that, reliability coefficients for the subdimensions were 0.947, 0.923, and 0.896, respectively. This indicated that the reliability coefficients for the internal consistency of the total scale and subdimensions were adequate. Further, Table 2 shows that the differences between the 27% upper and lower group means were statistically significant ($p < 0.001$). The item analysis results indicated that 41 items can significantly distinguish the respondents in the 27% upper and lower groups (Büyüköztürk, 2004).

*Study II*

*Sample*. The second study consisted of 494 university students (213 males and 281 females) with a mean age of 26.30 (SD = 2.42, 18–47 years). Results indicated that majority of the participants (88.3%) use the Internet more than four hours a day. Further, 81.4% of the participants reported that they use e-government services and 62.1% of them use e-commerce. Finally, 15% of the participants reported that they have received a training related to cybercrimes and 13.6% of them were subjected to a cyber-attack.

*Confirmatory factor analysis*. In the second study, a CFA was conducted to validate the measurement model with SPSS AMOS (v.25). Given the threshold values proposed by Kline (2005), model-fit indices for the measurement model were sufficient: [$\chi^2$/DF = 2.87, AGFI = 0.86, GFI = 0.92, CFI = 0.92, IFI = 0.93, TLI = 0.94, RMSEA = 0.05]. These results suggested that three-factor model (i.e. information systems crimes, personal data crimes, and privacy and security) fits the data well. Table 3 shows model-fit indices for the measurement model shown in Figure 1.

*Concurrent validity*. The correlation between the "Cybercrime Awareness Scale" and "Digital Data Security Awareness Scale" was tested by performing Pearson's correlation analysis. The results indicated that there is a positive and significant correlation between the scales ($p < 0.001$). The result also showed that the correlation between the two scales was moderate ($r = 0.53$).

## Discussion and conclusion

Nowadays, critical data about persons and strategic institutions such as banks, hospitals, and companies are stored in the cyberspace. Therefore, information systems should be protected against cyber-attacks and cybercrimes (Gökçearslan *et al.*, 2020). Both individuals and institutions should pay attention to the cybercrimes and related risks (Arpaci *et al.*, 2015).

**Table 3.** Model-fit indices

| Compatibility indices | Measurement model | Thresholds |
|---|---|---|
| $\chi^2$ | 289.472 | |
| $p$ value | <0.001 | |
| $\chi^2$ /df | 2.872 | <3 |
| GFI | 0.924 | ≥0.90 |
| AGFI | 0.865 | ≥0.80 |
| NFI | 0.914 | ≥0.90 |
| TLI | 0.948 | ≥0.90 |
| CFI | 0.929 | ≥0.90 |
| IFI | 0.935 | ≥0.90 |
| RMSEA | 0.057 | ≤0.08 |
| SRMR | 0.048 | ≤0.08 |

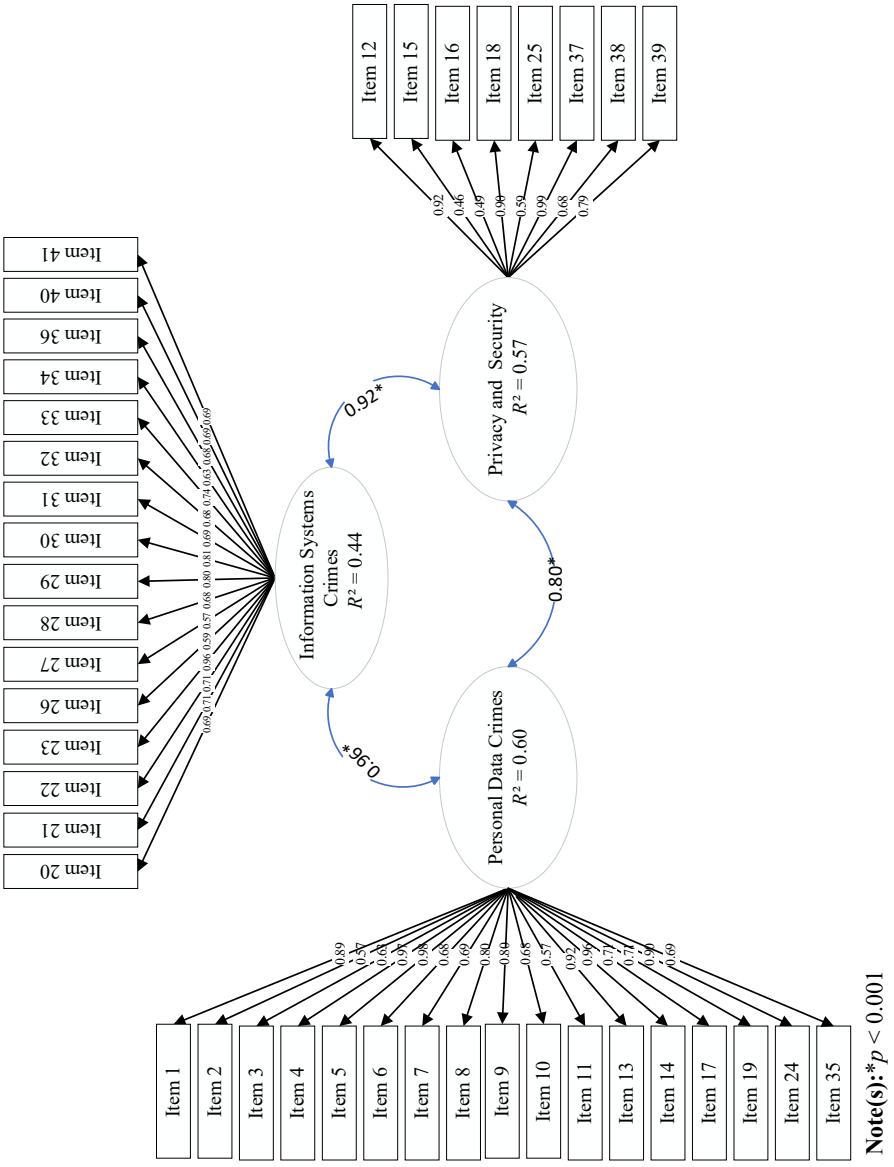


**Figure 1.**
Measurement model

Accordingly, this study aimed to develop a reliable and valid scale that can be used to measure individuals' cybercrime awareness level. An item pool consisting of 90 items was generated by the study researchers based upon the cybercrime legislations and the cybercrime types of the Turkish penal code. Consequently, a Likert-type scale was developed and the psychometric-properties of the scale were tested based on a sample of 994 Turkish undergraduate students.

In the first the study, the EFA was conducted to determine factor-structure of the CAS. Results showed the proposed scale consists of 41 items and it has a three-factor structure. The subdimensions of the scale were named as "information systems crimes", "personal data crimes", and "privacy and security." In the first subdimension, there are items about illegally controlling an information system. The second subdimension includes items about crimes concerning personal data. In the third subdimension, there are items about crimes that violate privacy and security. The item analysis results indicated that 41 items can significantly distinguish the respondents in the 27% upper and lower groups.

In the second study, the CFA was conducted to validate structure of the proposed scale. Results indicated the three-factor model has a good fit with the data. Finally, correlation between the proposed scale and "Digital Data Security Awareness Scale" was tested for the concurrent validity. The results indicated that there was a positive and significant correlation between the two scales.

It is important to note that the proposed scale differs from the existing scales in several ways. First, the proposed scale was developed by taking into account the cybercrime legislations of the Turkish general directorate of security and the types of cybercrimes in the Turkish penal code. Second, the scope of the CAS is more comprehensive than other scales. Third, the psychometric properties of the CAS were tested by following rigorous methodological standards. Therefore, the CAS can be a better measurement tool than the alternative scales.

Some limitations of the study must be acknowledged. First, the items generated for the CAS were based on the types of cybercrimes in the Turkish penal code. Therefore, future studies should adapt the proposed scale to different cultures with caution since some items may not apply to other countries. Second, nearly half of the generated items (47/90) were eliminated based the experts' evaluations and two additional items were eliminated during the factor analysis. This may limit the content validity of the proposed scale. Third, three subdimensions of the CAS have been named as "information systems crimes, personal data crimes, and privacy and security." However, some items may not entirely represent the desired factor or subdimension. Finally, psychometric properties of the CAS were tested based on data obtained from university students aged between 17–48 years. Therefore, the CAS could be best applied to individuals with at least a high school degree and aged between 17–48 years. Despite these limitations, this study has a number of strengths, including the use of two different study designs for EFA and CFA, a large sample size, a well-established scale for concurrent validity, and external field experts for the content validity. In conclusion, the findings provide strong support for the psychometric properties of the CAS. Consequently, the CAS is a valid and reliable measurement tool that can be used to measure the cybercrime awareness levels of individuals.

## References

Abbas, H.S.M., Qaisar, Z.H., Xu, X. and Sun, C. (2022), "Nexus of E-government, cybersecurity and corruption on public service (PSS) sustainability in Asian economies using fixed-effect and random forest algorithm", *Online Information Review*, Vol. 46 No. 4, pp. 754-770, doi: 10.1108/OIR-02-2021-0069.

Abuda, B.F.Q., Rivera, K.D. and Noroña, R.V. (2020), "Predictive validity of a cybercrime awareness tool: the case of senior high school students in a Philippine secondary school", *International Journal in Information Technology in Governance, Education and Business*, Vol. 2 No. 1, pp. 18-26, available at: https://ssrn.com/abstract=4007646.

Arpaci, I. and Aslan, O. (2022), "Development of a scale to measure cybercrime-awareness on social media", *Journal of Computer Information Systems*. doi: 10.1080/08874417.2022.2101160.

Arpaci, I. and Sevinc, K. (2022), "Development of the cybersecurity scale (CS-S): evidence of validity and reliability", *Information Development*, Vol. 38 No. 2, pp. 218-226, doi: 10.1177/0266666921997512.

Arpaci, I., Cetin Yardimci, Y. and Turetken, O. (2015), "The impact of perceived security on organizational adoption of smartphones", *Cyberpsychology, Behavior, and Social Networking*, Vol. 18 No. 10, pp. 602-608, doi: 10.1089/cyber.2015.0243.

Ates, E. (2021), "Siber Suç farkındalık ölçeği geliştirme: Geçerlik ve güvenirlik çalışması", Master's thesis, Tokat Gaziosmanpasa University, Institute of Education Sciences, Tokat.

Büyüköztürk, S. (2004), *Data Analysis Handbook*, Pegem Publishing, Ankara.

Budak, O. (2015), "Cybercrime awareness of informatics students: the case of vocational and technical high schools in Erzurum", Master's thesis, Ataturk University, Institute of Educational Sciences, Erzurum.

Davis, L.L. (1992), "Instrument review: getting the most from a panel of experts", *Applied Nursing Research*, Vol. 5 No. 4, pp. 194-197, doi: 10.1016/S0897-1897(05)80008-4.

EGM (2022), Department of Anti-Cybercrime, General Directorate of Security, available at: https://www.egm.gov.tr/siber/sibersucnedir.

Gökçearslan, S., Nezgitli, S. and Çakır, H. (2020), "Presentation of cybercrime news in the press: a sample of online newspaper news between 2009-2019", *Journal of Information and Communication Technologies*, Vol. 2 No. 2, pp. 149-160, available at: https://dergipark.org.tr/en/pub/bited/issue/58421/817899.

İlbaş, C. and Köksal, M.A. (2011), "Turkey cybercrime report: 1990-2011 July", *Proceedings of the 2nd International Informatics Law Congress*. Izmir.

Kline, R.B. (2005), *Principles and Practice of Structural Equation Modeling*, 2nd ed., Guilford, New York.

Mesko, G. and Bernik, I. (2011), "Cybercrime: awareness and fear: slovenian perspectives", *2011 European Intelligence and Security Informatics Conference*, IEEE, pp. 28-33, doi: 10.1109/EISIC.2011.12.

Nzeakor, O.F., Nwokeoma, B.N. and Ezeh, P.J. (2020), "Pattern of cybercrime awareness in Imo state, Nigeria: an empirical assessment", *International Journal of Cyber Criminology*, Vol. 14 No. 1, pp. 283-299.

Rajasekar, S. (2011), *Cyber crime Awareness Scale*, National Psychological Corporation, KacheriGhat.

Seçer, D. (2013), *Practical Data Analysis with SPSS and LISREL*, Memoir Publishing, Ankara.

Tibi, M.H., Hadeje, K. and Watted, B. (2019), "Cybercrime awareness among students at a teacher training college", *International Journal of Computer Trends and Technology*, Vol. 67 No. 6, pp. 11-17.

Whitman, M.E. and Mattord, H.J. (2012), *Principles of Information Security*, 4th ed., Course Technology, Boston.

Yılmaz, E. (2015), *Öğretmenlerin Dijital veri güvenliği farkındalığı [Unpublished Doctoral Dissertation]*, Anadolu University, Institute of Education Sciences, Eskisehir.

Zayid, E.I.M. and Farah, N.A.A. (2017), "A study on cybercrime awareness test in Saudi Arabia-Alnamas region", *2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 199-202, doi: 10.1109/Anti-Cybercrime.2017.7905290.

## Appendix. Cybercrime awareness scale items

A. Information systems crimes

1. I am aware of using a prohibited device or program (e.g. password cracker, e-signature creation tool, etc.) in cyberspace is a crime
2. I know that to make qualified theft using information systems is a crime
3. I know that to engage in qualified interactive fraud in cyberspace is a crime
4. Hacking someone else's e-mail account is a crime
5. Using contact data (e.g. email, address, phone number) without users' permission is a crime
6. There is a penalty for violating investigation confidentiality in cyberspace
7. Promoting drug use in cyberspace is a crime
8. I know that to insult a state or institutions of a state in cyberspace is a crime
9. I am aware that posts with terrorist content constitute a crime
10. It is a crime to disable programs to protect hardware and software
11. It is a crime to make unfounded political and military posts in cyberspace
12. It is a crime to block/stop a computer system working in cyberspace
13. Selling illegal (e.g. stolen, counterfeit) products in cyberspace is a crime
14. It is a crime to direct individuals to illegal sites via links in cyberspace
15. It is a crime to provide a place and opportunity to commit cybercrime in cyberspace
16. I can be scammed when investing in cryptocurrencies on unreliable exchanges

*B. Personal Data Offenses*

17. Unauthorized access to an open information system requires legal action
18. Violating confidentiality of communication between people is a crime
19. It is a crime to share personal information with third parties in cyberspace
20. Illegal betting/gambling in cyberspace is a crime
21. Blackmail in cyberspace is a crime
22. I know that using insulting expressions in cyberspace is a crime
23. It is a crime to record audio or video without permission in cyberspace
24. It is a crime to gain unfair advantage through illegal transactions in cyberspace
25. Hacking of information systems is a crime
26. I know that cyber harassment and bullying are criminal offenses
27. I know that using e-signature data by someone else is a crime
28. I am aware that sexual content should not be shared in cyberspace
29. It is a crime to take action by obtaining someone else's social media account password
30. Sharing statements containing sabotage in cyberspace is a crime
31. It is a crime to corrupt information systems through malicious software (e.g. virus, Trojan horse, worm, etc.)
32. It is a crime to enter a website without permission
33. It is a crime to ask for money and valuables by using ransomware (cyber extortion) in cyberspace

*C. Privacy and Security*

34. I should cite references that I quote in cyberspace as a source in order not to violate copyright
35. I should file a criminal complaint against those who violate the privacy of private life in cyberspace
36. I comply with website access blocking decisions made by public institutions in cyberspace
37. It is a crime to destroy data in an information system
38. I am aware that falsely sent spam mails constitute a crime
39. It is a crime to make illegal transactions through cryptocurrencies
40. It is a crime to use software that violates license agreement in cyberspace
41. Disclosure of secrets regarding undercover assignments in cyberspace is a crime

**Note(s):** *Scoring*: Cybercrime Awareness Scale (CAS) is a Likert-type scale that measures cybercrime awareness level of individuals. The CAS consists of three dimensions and 41 items. All items are scored between "strongly disagree (1)" and "strongly agree (5)" on a five-point scale. Scale scores range from 41 to 205 and a high score indicates a high level of cybercrime awareness

## About the authors

Ibrahim Arpaci is currently Associate Professor in the Department of Software Engineering at Bandirma Onyedi Eylul University. He received his PhD degree and MSc degree in Information Systems

both from Middle East Technical University. He holds the BSc degree (with distinction) in Computer Education and Instructional Technology from Anadolu University. He was a visiting scholar at Ryerson University, Ted Rogers School of Information Technology Management, Toronto, Ontario, Canada. He was among the Top 2% scientists in the world, according to the scientific report published by Stanford University in 2020 and 2021. Ibrahim Arpaci is the corresponding author and can be contacted at: iarpaci@bandirma.edu.tr

Ersin Ateş received his MSc degree in Computer Education and Instructional Technology from Tokat Gaziosmanpasa University. He holds the BSc degree in Computer Education and Instructional Technology from Tokat Gaziosmanpasa University.