Athens Journal of Mass Media and Communications
Volume 8, Issue 3, July 2022 – Pages 179-200

A Development, Validity and Reliability of Safe Social Networking Scale

By Nilgun Tosun[*] & Aynur Gecer[±]

Social networks has become in the spotlight for millions of people since they create a dynamic and rich interaction environment between users, and allow free access and usage of fake identity information. Distance education and working from home around the world due to COVID-19 pandemic has affected the increase in the rate and duration of social media usage in the last year. Unfortunately, this increase has offered criminals, who have the potential to pose risks and dangers on social media, more opportunities. Therefore, it has become even more important to use social media as a safe environment. The objective of this study was to develop a Safe Social Networking Scale for determining the security levels in social network usage. The validity and reliability studies of the scale were conducted with 585 social media users. As a result of the validity study, 28 items under five factors were obtained. These factors were being "Time Tunnel/Wall Sharing", "Safety of Social Network Profile Information and Sharing", "Social Network Friends List and its Safety", "Safety of Social Network Information Input", "Safe Login to Social Network Account". The items obtained were capable of discriminating the individuals in terms of the features to be measured by the scale. There has not been any scale that directly determines the level of safe use of social media in the literature. The developed scale is expected to fill this scale gap in the literature.

Keywords: safety, social networks, scale development, reliability, validity

Introduction

Social networks are one of the applications introduced into the lives of people following the development of web 2.0 technologies. In addition to read shares, the social networks allow users many opportunities, such as to comment on what they read, to produce contents in different formats and to share these, to like, to play a game. The opportunities provided by the social networks make them attractive for users. In addition to this attractiveness, the number of social network users is increasing day by day due to the fact that the social networks are free, it is not necessary to become a member with real identity information, it is possible to access the social networks anywhere and anytime by a device with an internet connection. The studies conducted corroborate this idea. While 53% of the world's population were active social media users in October 2020 (Kemp, 2020), this figure increased by 13.2% compared to the same month of the previous year and

[*]Associate Professor, Department of Computer and Instructional Technology Education, Trakya University, Turkey.
[±]Professor, Department of Computer and Instructional Technology Education, Kocaeli University, Turkey.

https://doi.org/10.30958/ajmmc.8-3-3 doi=10.30958/ajmmc.8-3-3

increased to 53.6% in January 2021 (Kemp, 2021a). The number of active social media users between January 2020 - January 2021 increased by 11.1% in Turkey. As of January 2021, 70.8% of Turkey's population is active social media users (Kemp, 2021b). These figures are significantly high for both Turkey and the world. Significantly high values also draw attention in the duration of social media usage. Worldwide users spend average 2 hours and 25 min per day on social media (Kemp, 2021a), while this time is 2 hours and 57 min for Turkey (Kemp, 2021b). The number of social media accounts owned by all active social media users in the world is average 8.4 (Kemp, 2021a), while this figure is 9.4 in Turkey (Kemp, 2021b). The effect of COVID-19 pandemic period on the increase in social media usage rate, duration and number of accounts cannot be ignored. The rate increases can be considered normal considering that people around the world fulfil their job responsibilities at home, education activities are carried out remotely, communication and social activities are transferred to digital platforms such as social media for a long time during the pandemic.

These numbers show that we live with a more crowded community in social networks than our physical environment. In the real life, we try to take measures against the threats likely to be caused by people living around us. Although it seems that the social networks refer to only virtual participation, the people we share these virtual environments are actually people, and they may always pose threats. It is even possible that we may encounter dangers with higher risk and harmful effect than the dangers we may face in real life. We should take the measures, as taken in order to prevent the risks and dangers that may be caused by people in real life, in social network environments where we interact with a large group of people. For these measures, it is not only necessary to be aware of taking security measures, but also to be competent in practice.

The main reason of working with university students in this study is the fact that the rate of active social media users between 18-24 years is 25.2% in the world (Kemp, 2021a), while this rate in the same age range is 20.3% for Turkey (Kemp, 2021b). This age range corresponds to the students at the university level for Turkey and constitutes a significant portion of the population. Young participating in the study voluntarily are prospective teachers. The participation of teachers this study as a role model for their students and as a guide for their close circle makes the scale intended to be developed more meaningful.

In order to be protected from dangers and risks as much as possible and not to harm others, we should use the social networks consciously. The consciousness in the social networks may be provided by taking security measures and acting in accordance with the rules of social networks. For this reason, it has been an important issue to determine the adequacy of security behaviours of individuals in the social networks. In the literature, there are scales for identifying computer security, mobile device security, and internet security behaviours, but there is no tool measuring only the security behaviours of the social networks. The necessity of the scale is provided once more since it will be first in the literature and will fulfil a significant gap.

Literature Review

Social Networks Based Cyber Threats

The social networks are unequalled crime scenes for cybercriminals. Because it is not likely to meet billions of people from every age, gender, language, race, status and education in any other environment. For this reason, many and various crimes are committed in the social networks.

For example, the social network fraud is highly widespread. According to news published in Dailyword, there are 270 million fake accounts on Facebook (Dailyworld, 2017). This number is gradually increasing. The number of Facebook accounts determined to be fake between January and October 2019 is 5.4 million (Fung and Garcia, 2019). Menczer (2018) found out that 9% to 15% of Twitter accounts are fake. According to LinkedIn Community Report (2020), 98.4% of fake accounts were blocked between January-June 2020. 33.7 million fake accounts were detected by LinkedIn security systems and deleted during registration process. The number of fake Facebook accounts deleted only in December 2020 was 1957, while the number of fake Instagram accounts deleted was 707 (Facebook, 2021). Fake accounts are opened for many purposes such as trapping other users into phishing, spreading malware, spam or viruses and cyberbullying.

Phishing scams are mostly seen on the social media networks. Users are directed to fake web sites with the links containing attractive messages and offers in line with their interests (Sırt, 2017). Phishing scams are mostly lived on Facebook and Twitter (Eren, 2018). As Morris (2019) stated, cyber attackers now prefer social networks instead of e-mail for phishing attacks. Thus, it is much easier to reach more people and personal information through social networks. In phishing scams, the purpose is not only to get personal information, but also to access information about the institution where the person is working (Newberry, 2020) or studying. For this reason, it is extremely important to know the privacy and security settings in social networks as well as to confirm the content before clicking on phishing posts.

Social networks are the primary preference area of cyber attackers for spreading malware or spam and virus attacks. It is not difficult for a cyber attacker to reach and deceive people through a fake or stolen account (Morris, 2019). Because a malicious software link sent to a person can reach hundreds, even thousands of people in an instance like a snowball. This may affect not only users, but also the institutions and even the educational institutions where the users work. The last example of this happened in Nottinghamshire. 15 schools in the region had to shut down their IT systems supporting distance education for a while because of cyber-attacks on social networks (Priyanka, 2021).

Cyberbullying is another critic risk arising from the social networks, especially for children and youths. 40% of all cyberbullying cases are seen on the social networks (Cyberbully411, 2018). Tuncer and Dikmen (2016) focussed on cyberbullying in social networks. Sixty-two students studying at Fırat University, Organized Industry Vocational High School participated in the study. The results showed that participants who used social network web sites more heavily were

more likely to be both cyber victims and also cyber bullies, compared to those who usedsocial networks less frequently. Gonzales (2017) conducted a study where students themselves suggested how protection could be put in place while using social networks. In this study, data from Pew Research Center in 2014 were included. Gonzales showed that 60% of students had been harassed on social networks. In addition, one out of every 11 students was secretly monitored on social networks. Most students did not know what their online rights were. When faced with unwanted situations in online platforms, they were afraid to tell their teachers or parents. According to the report of a survey conducted in the UK in 2017, 42% of young social network users stated that they were victims of cyberbullying on Instagram and 37% on Facebook (Ditch The Label, 2017). The cyber bullying is mostly seen on Facebook (Cook, 2018). In a survey conducted with 1974 United Statian in the age group 18 and over in January 2020, 77% of the participants experienced cyber bullying on Facebook (Johnson, 2021). Undoubtedly, the use of internet and social networks by millions of students not only for educational purposes but also for socializing and having fun during the pandemic period has led to an increase in cyberbullying incidents. According to L1ght (one of the organizations publishing cyberbullying data), cyberbullying incidents increased by 70% in September-October (Micklea, 2020). Although the numbers and rankings change, it is clear that social networks are platforms where cyberbullying incidents are frequent. As a result of these data, it is revealed once again that social networks should be used by taking security measures.

The stealing of social networking or personal information through mobile applications has also become an important problem after the increasing popularity of smartphones. Some mobile applications require users to sign up with their social network personal information. Thus, the application owners can easily access private and social network information of individuals. Moreover, the social network accounts can be seized because of the security vulnerabilities of the applications registered with social network username and password no matter how strong the password of the social network account is (Newberry, 2020). Changing the current password at regular intervals can be offered to users as a solution in this regard and in order to protect against other social network-based cyber threats. Many banks in Turkey impose obligation to change password at regular intervals for internet banking customers. This application of banks can also be performed by social networking companies.

Some online games threaten security in the social networks. In addition to financial losses, these games lead to depression, physical injury and suicides. Some of these games are as follows: Blue Whale (Adeane, 2019), Mariam (Khalaf, 2017), Avataria (CNNTÜRK, 2016), Momo (Ryan, 2019), Doki Doki Literature Club (Hawken, 2018), 48 Hours Challenge (Johnson, 2019) and Eraser Challenge (Şalt, 2018).

Following the declaration of the pandemic on 11 March 2020, countries compulsorily took decisions on distance education, remote and flexible working. The popularity of the social networks, known as indispensable platforms of communication, news and shares, has increased more by being an important part of educational systems in this period. The World Bank revealed in a study that

teachers in many countries have preferred the social media for communication and information share with their students (The World Bank, 2020). However, some dangers and risks arising from social networks have been raised during COVID-19 quarantine days. Many infodemic examples, such as spreading fabricated news and rumours related to COVID-19, creating negative psychological atmosphere in the society, selling counterfeit drugs and vaccines, fake donation campaigns were seen and are still seen frequently on the social networks (Bitdefender 2020; Chakravorti, 2020; Gold and O'Sullivan, 2020; Hao and Basu, 2020; Koyuncu, 2020; Rakipoğlu, 2020; Rodríguez et al., 2020; Scott, 2020; TÜBA, 2020). The number of fake news deleted from LinkedIn social network platform between January and June 2020 is 22,846 (LinkedIn Community Report, 2020). According to the news of BBC (2021), YouTube announced that 30,000 videos published about the COVID-19 vaccine and determined to be false have been deleted from the platform.

Based on this information, it can be said that social networks provide users with advantages, but also bring some threats and risks. It is clear that adopting safe social networking behaviours is important for everyone in order to minimize the material and moral losses caused by these threats and risks personally, institutionally and nationally.

Studies on Security in Social Networks and Measuring Instruments Used

The increasing use of social networks for several purposes, especially by children and youngsters, has also caused an increase in the volume of national and international research investigating the safety of social networks. Although there are various scales to measure awareness of information security and to assess cybersecurity behaviour available in the literature, these scales do not focus on social network security behaviour.

Kjørvik (2010) developed the Information Security Awareness Questionnarie within the framework of his master's thesis. General computer security, e-mail usage, internet usage, backup, password usage, physical device security dimensions are included in questionnaire.

Kim (2013) also developed a scale to identify high school students' behaviour and perceptions of information security too. The scale consists of 21 questions: password usage, backup, antivirus usage, e-mail security, file security in devices, e-mail accounts and files.

Çakır et al. (2015) used the Safety Awareness Questionnaire in Social Networks, developed for their study to determine the awareness of pre-service teachers on social network safety. This study showed that the participants were highly aware of the risks related to login passwords and the confidentiality of answers to safety questions. However, it was also found that participants seldom read the terms of use and privacy policy.

Erol et al. (2015) also developed the Personal Cyber Security Scale. When the scale is analyzed, it is seen that the items related to password usage, e-shopping, e-banking, e-mail security, using web browser, and common computer use are

predominant. There are only 3 items related to security in social networks in the 25 item scale.

Dreibelbis (2016), in his research conducted with private sector employees, aimed to specify the cyber security behaviours of employees. For this purpose, he developed a Cyber Security Scale consisting of 23 items. There is no item that measures security behaviours in social networks in this scale.

In their Cyber Security Awareness Scale for high school students, Muhirwe and White (2016) included several questions in subjects such as software security, email security, password usage, backup, antivirus usage, sharing of devices and files.

The Risky Cyber Security Behaviour Scale used by the Hadlington (2017) its research consists of 20 items and only 2 items are intended to measure the types of safe behaviour in social networks.

Yan et al. (2018), in the study where university students examined the correct decision-making behaviours in the face of cyber threats, used the scenario-based Cybersecurity Judgment Scale.

Scenarios include general cyber threats. Giwah (2019) developed a scale, intending to determine the information security attitudes of mobile device users. The scale items consist of topics such as physical security of mobile devices, use of passwords and antivirus devices on devices, security in internet and e-mail transactions.

The absence of scales which only determine social network security behaviour was the starting point of this study. One of the objectives of The Safe Social Networking Scale development study was to remedy this deficiency together with determining the sub-dimensions of safe social network usage behaviour. We considered this scale would measure how much regard individuals have for security while using social networks, and what they do for security. In addition, we hoped that it would contribute to evaluation of the current status and identify faulty behaviour, thus enabling its elimination.

Materials and Methods

Research Objective

This study was a scale development study for determining and evaluating the security behaviour of the users while social networking.

Participants

The study group included students studying at different departments of the Education Faculty in a state university. The study invited a total of 598 students to participate. The students were chosen randomly according to a sampling method. Of these, 585 students participated in the survey and submitted a valid form and so were included in the evaluation process. The demographic characteristics of these 585 students are presented in Table 1. 47.86% of the participants are women and

52.13% of the participants are men. The students participating in the study are studying in various departments of the Faculty of Education (German, Information Technologies, English, Music, Painting, Preschool, Turkish Teaching). Their ages are between 17 and 23 years.

Table 1. Social Networking Usage Times

Social network usage time (year)	**N**	**%**	**Time spent in a day on social networks (hour)**	**N**	**%**
1-3	38	6.5	less than 1 hour	48	8.2
4-6	210	35.8	1-3	285	48.6
7-9	216	36.9	4-6	199	34.0
10 and over	121	20.6	7 and over	53	9.0
Total	585	100.0	Total	585	99.8

When Table 1 is examined; 36.9% of the students participating in the study stated that they have been using social networks for 7-9 years, 35.8% of them for 4-6 years, and 20.6% of them for 10 years and over. Considering the average time spent in a day in social networks; 48.6% of the students stated that they have been using social networks for 1-3 hours and 34% of them have been using social networks for 4-6 hours.

Table 2. Social Network Accounts they joined

Social network	**N**	**%**
Facebook	156	26.6
Twitter	357	60.9
Youtube	72	12.3
Total	585	100

When the social networks joined by the students are examined, it is seen that 60.9% of the students have joined in Twitter, 26.6% of them in Facebook and 12.3% of them in YouTube (Table 2).

Data Collection Tools

This scale has been developed in order to develop a Safe Social Networking use. In the first section of the study, the literature was reviewed. Scales which attempted to measure indicators of safe social network use were investigated. Each identified indicator relating to safe social network use was taken into consideration, and a pool of 67 items was created.

A draft of three categories was established: spelling, punctuation and expression errors, which were later analysed by five linguists.

The resulting, experimental 67-item questionnaire was evaluated by five experts (three from the Department of Computer Education and Instructional Technologies and two from the Department of Informatics) for content validity. Each item was evaluated for: measurability of the level of safe social network usage; for the relationship with relevant sub-dimensions; and understand ability of

the language used. A 5-point Likert scale was used (1: strongly disagree; 2: disagree; 3: neutral; 4: agree; 5: strongly agree).

Data Collection and Analysis

A Likert statement consisting of five stages was used to fully analyse and understand the responses given by the teachers who took part in the study. A statistical analysis was made according to the participants' responses that went from "strongly agree" (5 points) to "strongly disagree" (1 point). During the six month long data collection process, 598 students filled in electronic or printed versions of the developed questionnaire. After analysis of the submitted questionnaires, 585 out of 598 (97.8%) were determined to be suitable for statistical analysis. Validity and reliability of the questionnaire was conducted on these forms.

The literature recommends conducting exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) using different samples (Büyüköztürk et al., 2012; Ilhan and Çetin, 2014).

Therefore, the collected data are divided into two subgroups. In this context 300 of the forms were evaluated by EFA and remaining 285 by CFA.

When determining sufficient sample size, relative criteria such as the number of items or factors should be taken into consideration. It has been reported that the sample size should be 5-10 times greater than the number of items in the scale (Kline, 1994; Tavşancıl, 2005). In this study, the sample size was approximately 8 times more than the number of items.

All statistical analysis was performed with SPSS 20.0 (IBM Corporation, Armonk, NY, USA) and LISREL 8.7 software packages.

Results

It is important to check whether the data are suitable for factor analysis before performing exploratory factor analysis. For this purpose, Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity were performed.

According to the literature, the test should be finalized if the KMO value calculated for the sample size is smaller than 0.50. A value greater than 0.90 means "perfect", and the test can be maintained (Çokluk et al., 2010; Tavşancıl, 2005). In our study, KMO coefficient was 0.79. In the Bartlett's Test of Sphericity, a value greater than 0.001 was considered to be significant [χ^2=3078,454; df=378; p=0.001]. This finding will depend on the multivariate normal distribution and may be interpreted as obtaining another assumption of the factor analysis.

Exploratory Factor Analysis

The data collected for the exploratory factor analysis (EFA) were obtained from 300 students studying at different departments of the Education Faculty in a

state university. First, the unrotated principal components analysis was performed to determine the factor structure. The evaluation of the factors with an eigenvalue >1 was preferred for determining the number of factors and the run chart and variance rates of the factors were considered in relation to the factor eigenvalues (Zwick and Velicer, 1986). According to the literature, only factors with an eigenvalue equal to or greater than 1 could be considered as stable (Büyüköztürk, 2002; Çokluk et al., 2010). We determined that the eigenvalue was greater than 1, and the scale developed in the light of this information had a 5-factor structure. The total explained variance of 5 factors was 50.45%.

The determined factors were called "Time Tunnel/Wall Sharing", "Safety of Social Network Profile Information and Sharing", "Social Network Friends List and its Safety", "Safety of Social Network Information Input" and "Safe Entry to Social Network Account." The scale was named "The Safe Social Networking Scale" (SSNS) and the SSNS framework, showing the scale items and their respective main value divisions (factors) is shown in Table 3.

Table 3. Factor Structure and Factor Loads of the Safe Social Networking Scale (SSNS)

Main values	**Sample indicator**
1st factor: Time tunnel/wall sharing	1. In my time tunnel/wall, I do not share contents which can harm to other people (e.g., accusations, threats, mockery, unfounded news, lies, and gossips).
	2. In my time tunnel/wall, I do not share contents related to violence.
	3. In my time tunnel/wall, I do not share illegal statements.
	4. In my time tunnel/wall, there can be no sexually explicit contents.
	5. In my time tunnel/wall, I do not share private information of other people.
	6. In my time tunnel/wall, there can be no contents including insulting expressions.
	7. In my time tunnel/wall, I restrict access of people whom I do not want to see the statements I share.
	8. In my time tunnel/wall, I do not allow hateful messages.
	9. In my time tunnel/wall, anyone cannot share contents.
	10. In my time tunnel/wall, I do not share information I do not get from primary sources.
2nd factor: Safety of social network profile information and sharing	11. My cover photo in social networks is accessible to anybody.
	12. Anybody can share my cover photo in social networks.
	13. Anybody can see my profile photo in social networks.
	14. Anybody can share my cover photo in social networks.
	15. The private information about my birth date, birth place, address, ID number, phone number, e-mail address, bank account number, political opinion, religious belief and relationship status that I share in my social network profile is accessible to anybody.
	16. Anybody can access to my social network profile from search engines.
3rd factor: Social network friends list and its safety	17. I do not add persons whom I do not know in my social network friends list.
	18. I do not accept friendship requests from persons whom I do not know.

	19. If I realize that social network account of one of my friends is hacked, I inform the Help Desk.
	20. I report malicious contents in social networks to the Help Desk.
4th factor: Safety of social network information input	21. I run the applications with my social network login information.
	22. I log in to different applications and websites with my social network information.
	23. I do cybershopping with my social network information.
5th factor: Safe entry to social network account	24. In order to login my social network account, I get the backup codes in case of not receiving two-step authentication message.
	25. I use two-step authentication (via phone code messaging) to login my social network accounts.
	26. While logging in my social network accounts, I prefer using https which is a secure transfer protocol (hypertext transfer protocol secure) instead of http.
	27. I adjust my social network account setup in a way warning me if a new device is used to be logged in.
	28. I change my social network password periodically.

Information about the factor loads of the scale and the variance rates are presented in Table 4. The rotated factor loadings ranged between 0.54 and 0.81.

Table 4. Results of Exploratory Factor Analysis

Factors and item numbers	**Total variance explained**	**Cronbach's α**	**Mean**	**SD**	**Item total correlation**	**Common factor variance**	**Rotated factor load**
1st factor	18.70	0.71					
Item 1			4.61	0.95	0.70	0.74	0.81
Item 2			4.56	0.96	0.70	0.69	0.77
Item 3			4.52	0.95	0.71	0.58	0.77
Item 4			4.67	0.95	0.71	0.58	0.74
Item 5			4.28	1.15	0.72	0.53	0.73
Item 6			4.44	0.90	0.71	0.53	0.70
Item 7			4.50	0.94	0.72	0.51	0.69
Item 8			4.42	0.91	0.71	0.53	0.64
Item 9			4.36	0.91	0.70	0.41	0.58
Item 10			4.11	0.97	0.71	0.40	0.54
2nd factor	9.42	0.74					
Item 11			2.80	1.55	0.75	0.54	0.75
Item 12			1.62	1.03	0.73	0.54	0.73
Item 13			2.90	1.52	0.74	0.53	0.74
Item 14			1.83	1.24	0.72	0.50	0.72
Item 15			1.80	1.12	0.73	0.43	0.73
Item 16			2.75	1.39	0.75	0.42	0.75
3rd factor	8.34	0.70					
Item 17			4.14	1.15	0.72	0.68	0.72
Item 18			4.07	1.14	0.70	0.68	0.70
Item 19			3.98	1.16	0.71	0.44	0.71
Item 20			4.06	1.08	0.70	0.40	0.70
4th factor	6.70	0.73					
Item 21			3.18	1.32	0.73	0.69	0.73
Item 22			3.14	1.19	0.73	0.42	0.73
Item 23			2.67	1.36	0.74	0.48	0.74

5th factor	7.29	0.72					
Item 24			2.47	1.32	0.73	0.56	0.73
Item 25			3.10	1.41	0.73	0.47	0.73
Item 26			3.01	1.32	0.73	0.47	0.73
Item 27			4.11	1.14	0.71	0.41	0.71
Item 28			2.00	1.03	0.73	0.51	0.73
Total	50.45	0.72					

According to the results shown in Table 4, the first sub-dimension of time tunnel/wall sharing including 10 items explained 18.70% of the total variance. The factor loads of the items found in the sub-dimension of Time Tunnel/Wall Sharing ranged between 0.81 and 0.54. The second sub-dimension of Safety of Social Network Profile Information and Sharing included six items, and explained 9.42% of the total variance. The factor loads of the items in this sub-dimension varied between 0.73 and 0.42. There were four items in the third factor of the scale (Social Network Friends List and its Safety). This sub-factor explained 8.34% of the total variance and the factor loads ranged between 0.82 and 0.48. The fourth sub-dimension was named Safety of Social Network Information Input. There were three items in this sub-dimension and the factor loads ranged between 0.80 and 0.67. It explained 6.70% of the total variance. The fifth factor was called Safe Entry to Social Network Account and included five items. Its factor loads varied between 0.74 and 0.47, and it explained 7.29% of the total variance. The 5-factor structure of the SSNS could be evaluated as five separate scales, as well as yielding a total score for safe social networking.

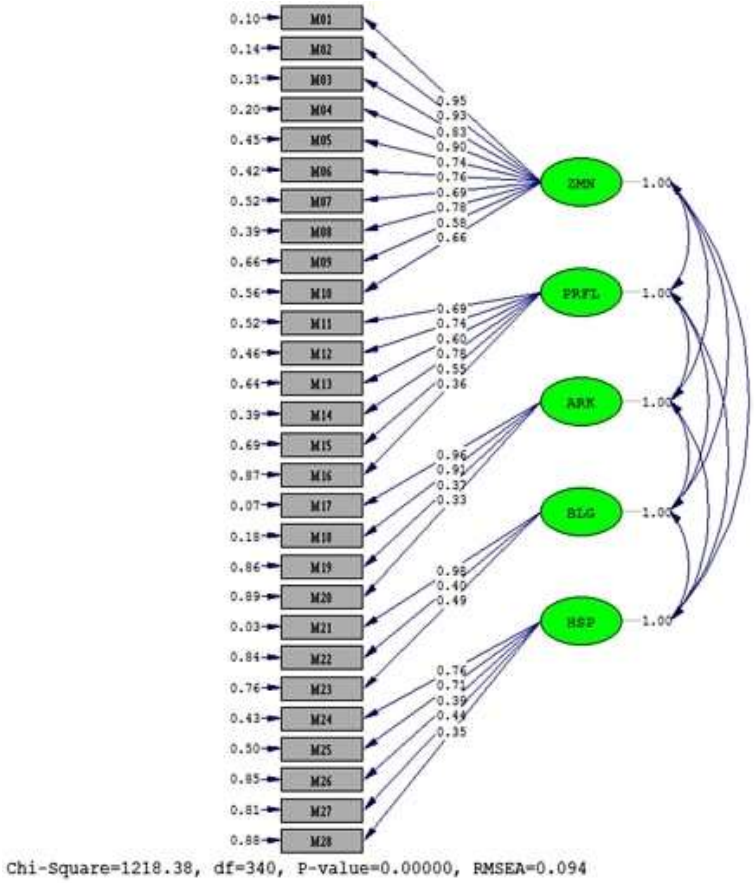
In order to determine the reliability of SSNS, the internal consistency coefficient (Cronbach's alpha) was calculated, and α value of the whole scale was determined to be 0.729. The Cronbach's alpha coefficient varied between 0.70 and 0.75 on the basis of item scores. It is generally accepted that a reliability level >0.70 indicates a statistically significant result for each factor (Tavşancıl, 2005; Turgut & Baykul, 1992).

Confirmatory Factor Analysis (CFA)

A total of 285 separate forms filled in by the students studying at different departments of the Education Faculty in a state university were used for the confirmatory factor analysis (CFA). CFA was administered in order to find out whether the factor structure of SSNS could be confirmed or not. In order to demonstrate the sufficiency of the tested model in CFA, Chi-square Goodness of fit test, Goodness of Fit Index (GFI), Adjustment Goodness of Fit Index (AGFI), Comparative Fit Index (CFI), Normed Fit Index (NFI), Non-Normed Fit Index (NNFI), Root Mean Square Error of Approximation (RMSEA) and Standardized Root Mean Square Residual (SRMR) values were evaluated. It has been reported that a value of 0.90 indicates an acceptable fit and 0.95 indicates a perfect fit for the criteria, which should be taken into consideration for fit indices (Marsh et al., 2006; Şimşek, 2007). In terms of NNFI, 0.95 was considered to be acceptable, and 0.97 a perfect fit while for AGFI, 0.85 was considered to be acceptable and 0.90 was considered to be perfect fit (Schermelleh-Engel et al., 2003; Wang and Wang,

2012). For RMSEA, 0.08 was acceptable and 0.05 was a perfect fit (Schumacker and Lomax, 2010). For SRMR, 0.05 was considered to beperfect and 0.10 an acceptable fit (Schermelleh-Engel et al., 2003; Waltz et al., 2010). In our study, the fit indices of the model obtained from CFA analysis were evaluated, and the minimum Chi-square value (χ^2=1218,38; SD=340; p<0.01) was significant. The evaluation of fit indices revealed the following results: RMSEA=0.94; GFI=0.89; AGFI=0.87; CFI=0.94; NFI=0.87; NNFI=0.89 and SRMR=0.07. The acceptable fit criteria related to the evaluated fit indices indicated that the 5-factor model assessed by CFA had a good fit and confirmed the scale. The factor loads related to the 5-dimension model resulting from the one-level CFA are presented in Figure 1.

Figure 1. Factor Loads Related to the 5-Dimension Model from Level One CFA



As seen in Figure 1, the factor loads varied between 0.58 and 0.95 for the sub-dimension of Time Tunnel/Wall Sharing (ZMN), between 0.36 and 0.78 for the sub-dimension of Safety of Social Network Profile Information and Sharing (PRFL), between 0.33 and 0.96 for the sub-dimension of Social Network Friends List and its Safety (ARK), between 1.17 and 0.38 for the sub-dimension of Safety of Social Network Information Input (BLG), and between 0.35 and 0.76 for the sub-dimension of Safe Entry to Social Network Account (HSP). The fit values of the suggested model and the standard fit criteria are shown in Table 5.

Table 5. The Fit Values of Suggested Model and the Standard Fit Criteria

Fit values	Good fit values	Acceptable fit values	i-value scale fit values
χ2/df	⩽3	⩽5	3.583
RMSEA	⩽0.05	0.05-0.08	0.088
SRMR	00.05	0.05-0.10	0.071
GFI	⩾0.95	0.90-0.95	0.89
AGFI	⩾0.90	0.85-0.90	0.87
CFI	⩾0.95	0.90-0.95	0.94
NFI	⩾0.95	0.90-0.95	0.87
NNFI	⩾0.95	0.90-0.95	0.89

T values obtained from one-level CFA are shown in Table 6.

Table 6. T Values Obtained from One-Level Cfa for Ssns

Item No	t	Item No	t	Item No	t	Item No	t
1	21.32**	8	15.67**	15	9.33**	22	5.71**
2	20.46**	9	10.66**	16	5.75**	23	6.66**
3	17.10**	10	12.44**	17	20.07**	24	11.42**
4	19.40**	11	12.40**	18	18.39**	25	10.67**
5	14.53**	12	13.15**	19	6.24**	26	5.86**
6	15.09**	13	10.33**	20	5.48**	27	6.63**
7	13.20**	14	14.18**	21	9.95**	28	5.21**

** $p<0.01$.

According to the results in Table 5, t values related to the items in SSNS varied between 5.21 and 21.32. It has been reported that t values greater than 1.96 indicate a significance level of 0.05, and t values greater than 2.58 indicate a significance level of 0.01 (Jöreskog and Sörbom, 1993; Kline, 2011). Thus, all t values obtained from one-level CFA had a significance level of at least 0.01. According to the results of one-level CFA, the sample size of the study was sufficient for factor analysis, and we concluded that there was no item which should be excluded from the model.

The Evaluation of SSNS Scores

Since there were ten items in the sub-dimension of time tunnel/wall sharing, the minimum and maximum scores were 10 and 50. The dimension of safety of social network profile information and sharing contained six items, and the minimum and maximum scores were 6 and 30. The minimum and maximum scores of the dimension of social network friends list and its safety were 4 and 20 since there were only four items in this dimension. There were three items in the sub-dimension of safety of social network information input, and thus the minimum and maximum scores were 3 and 15. The sub-dimension of safe entry to social network account had five items, and the minimum and maximum scores were therefore 5 and 25. As the whole scale had totally 28 items, the minimum and maximum possible scores were 28 and 140. As SSNS provided sufficient fit indices in one-level CFA, it could be concluded that the scores

obtained from the sub-dimensions could be separately processed and the total score could be used fora measure of safe social networking. An increase in the scores obtained from the sub-dimensions of SSNS and from the whole scale indicated a high security level in the social networking.

Discussion

The purpose of this study was to develop a simple, short, and psychometrically sound scale capable of measuring security behaviours in social networks. Considering that students have been using social networks for a longer period of time day by day, this scale may enable them to use social networks in a conscious and safe manner and to guide their environment in this regard. The present study aimed to develop and validate a safe social networking questionnaire in order to understand of social networking usage of university students in an Turkey context. This paper has presented the carefully methodological procedure carried out to develop and quantitatively validate a method measuring Turkey university students' safe social networking usage. A Safe Social Networking Scale not only has adequate statistical support but also has enough theoretical support. The factors extracted through exploratory factor analysis and validated through confirmatory factor analysis also have similar references in empirical studies. The scale included 28 items, and had a 5-factor structure. The defined factors were "time tunnel/wall sharing", "safety of social network profile information and sharing", "social network friends list and its safety", "safety of social network information input" and "safe entry to social network account". There are researches and studies that may be associated with these factors and that emphasize the importance of these factors in the literature:

Factor 1. Time tunnel/wall sharing: One of the most important reasons of the increasing interest in social networks is that users may share all kinds of content with their followers on their own time tunnel/wall without time and place. However, it is highly important to authorize those who will see the posts made on social networks and who will post on our own time tunnel/wall for the safety of personal information. After joining in a social network, it should be learned how to make privacy and safety settings in this regard (Aksakallı, 2021; Digital Nusiance, 2020; Tutorful, 2020).

Factor 2. Safety of social network profile information and sharing: Personal information shared on social networks is a powerful weapon for cyber attackers. Even information on hobbies and interests that many people find insignificant is enough for many cyber attackers to take action. Most cyber attackers can bring together personal information shared by the person on different social networking platforms and create a well-equipped database about the person (Chester, 2020). Academic studies hereof also draw attention to the importance of personal information sharing in social networks. Sharma and Gupta (2018) investigated the effects of situational factors such as control of information in social networks, protecting personal information and indifference of users towards privacy. Senthil Kumar et al. (2016) emphasized safety measures related to the privacy of personal

information, along with the possible risks of social networks. Yıldırım and Varol (2013) conducted a study at Fırat University and Bitlis Eren University with the participation of students, lecturers and instructors. They used a questionnaire to find out the safety level of the social networks and the awareness of the users concerning safety measures related to social networks. The results showed that most of the participants believed that the personal information was being abused by social network sites. More than half of the users had been subjected to spam or harmful applications. It was reported that 20% of accounts were fake, and that photographs, supposedly of the account owner, were usually used without the permission of the true owners. Personal information sharing errors in social networks are a factor threatening the cyber safety of institutions (Morris, 2019). For this reason, students who are a part of educational institutions should not share personal information on social networks in a publicly accessible way.

Factor 3. Social network friends list and its safety: Some of the cyber-crimes seen in social networks are performed by a fraud method called social engineering. In social engineering, the attacker first gains the victim's trust and then begins to gather information about the victim. To do this, the attacker asks questions or shares a link containing software infiltrating the victim's device. Therefore, it is important to make necessary investigation before adding new friends in social networks (Chester, 2020; Yavanoğlu et al., 2012). It is also an important sign that one(s) of the friends list constantly posts negative-content and repetitive messages. Some of the accounts sharing such things are fake accounts and should be deleted from the friends list (Digital Nusiance, 2020).

Factor 4. Safety of social network information input: Millions of people around the world use the internet for different purposes. Some sites on the Internet are logged in with user name and password information. However, sometimes this information may be forgotten for various reasons. In case of such situations, some of the sites provide access to the site with social network username and password information in order to hold users harmless. In case of forgotten username or password, the sites should not be logged in with social network login information. The entered information is saved in databases and may be used maliciously. Therefore social network login information should only be used for this purpose.

Factor 5. Safe entry to social network account: Digital Nusiance (2020), Morris (2019) and Sobers (2018); emphasize that it is highly important to determine a strong password, change the password regularly and log in social networks with two-step verification method for social network safety. Tosun (2015) investigated the social network habits of vocational high school students and found that the majority of students changing the security options regularly but only implemented updates when they considered it necessary and believed that their social network passwords had a high strength.

Finally, the evidence of this measurement suggests that this questionnaire has robust psychometric properties to measure a safe social networking usage among university students. This study will give researcher much needed tools and a fresh perspective in their research on the concept of the safe social networking usage.

When the strength of the study is considered, the Safe Social Networking Scale can be used to measure for wider age groups, including students and social network users.

Conclusion

A carefully, educated and conscious use of social networks is important for the privacy and safety of users. In this context, a Safe Social Networking Scale was developed. This scale developed, is the only scale developed regarding the use of secure, conscious social networks. The development of this scale may contribute to future studies with different groups and to compare the results with this study.

Both in Turkey at the level of university students in the world, there is a high prevalence of the use of social media. Young people use social networks for various purposes. It is seen that social networks, which are open to the use of everyone, bring along negatives as well as the positive sides. Probably, the most important one is cyber danger among these threats, because the cyber dangers incurred by conscious and improperly used social networks, can reach the extent that threatens individual, institutional and even national security. Incidents such as theft, fraud, cyberbullying, carried out by using social engineering methods and constitute a crime, may cause material losses, damage to reputation and even loss of life. The increase in this kind of criminal acts has forced countries to take deterrent measures. In Turkey, crimes committed through social networks have been identified in the Turkish Penal Code 243, 244, 245 and the penalties corresponding to these crimes were explained (Turkish Penal Code, 2004). Considering that young people use social networks intensively for various purposes, it is not difficult to predict the negativities that young people who lack security awareness in social networks will experience or cause. However, there is a need for more theoretically informed, reliable, and valid instruments that are able to measure developments in this area. The fact that there is no other scale measuring security behaviours only in social networks in the current situation and literature indicates the importance and necessity of the developed Safe Social Networking Scale. It can be stated that this scale is sufficient to determine the security behaviours of young people in social networks, as a result of the validity and reliability analyzes performed on the scale items.

As a result of the analysis and calculations performed on the substances, it can be expressed that the validity and reliability scores of the scale are high and the validity of the scale and structure is ensured. Put it differently, the scale is a valid and reliable scale that can be used to assess the status of security behaviours exhibited by university students in social networks.

In similar studies with young people, it is thought that it can be benefitted from Safe Social Networking Scale as a valid and reliable data collection tool. The sample studied in the development of the scale, consists of a state university Faculty of Education students. The scale can be applied to students studying in different units of the same university. This scale can also be applied in universities

with different geographical and cultural characteristics and comparisons can be made.

This study was conducted to assess the behaviours of college students on social media, related to the use of safe and informed. Besides, it helps to bridge the gap in the current literature with its new findings. However, having different samples for future research will contribute to the validity and reliability of the scale.

In addition to comparisons, it may also pave the way for students to have knowledge and skills on these subjects by revealing the wrong behaviours and habits seen in the social dimension of social network use with this scale.

Limitations

Even though it used highly reliable and valid scale development procedures, there are still some limitations. The first limitation is that both the techniques of the scale refinement, of exploratory factor analysis and confirmatory factor analysis are quite sample-size specific. To have better results a bigger and different sample size is advisable.

References

Adeane, A. (2019). *Blue whale: what is the truth behind an online 'suicide challenge'?* BBC News.

Aksakallı, G. (2021). *Dijital mahremiyet.* (Digital privacy). Ankara, Türkiye: Güvenli İnternet Merkezi.

BBC (2021, March 13). *YouTube deletes 30,000 vaccine misinfo videos*. BBC News.

Bitdefender (2020). *Koronavirüs aşısı çalışmaları için bağış yapılmasını isteyen mesajlara dikkat!* (Attention to messages requesting donations for coronavirus vaccine studies!) Bitdefender.

Büyüköztürk, Ş. (2002). Factor analysis: basic concepts and use in scale development. *Journal of Educational Administration: Theory and Practice*, *8*(32).

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., Demirel, F. (2012). *Scientific research methods*. Ankara: Pegem Academy.

Çakır, H., Hava, K., Gülen, Ş. B., & Özüdoğru, G. (2015). Investigating the security awareness of pre-service teachers in social network websites. *International Journal of Human Sciences*, *12*(1), 887–902.

Chakravorti, B. (2020). *Social media companies are taking steps to tamp down coronavirus misinformation – But they can do more*. The Conversation.

Chester, D. (2020). *Social media safety rules for 2020*. Cool Tech Zone.

CNNTÜRK (2016). *Everyone is talking this game: Avataria*. CNNTÜRK.

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2010). *Multivariable statistics for social sciences*. Ankara: Pegem.

Cook, S. (2018). *Cyberbullying facts and statistics for 2016-2018*. Comparitech.

Cyberbully411 (2018). *Myths and facts*. Cyberbully411.

Dailyworld (2017, November 4). *Facebook knows it has 270 mn fake accounts*. Dailyworld.

Digital Nusiance (2020). *Social media security: tips, policy and best practices*. Digital Nusiance.

Ditch The Label (2017). *The annual bullying survey 2017*. Ditch The Label.

Dreibelbis, R. C. (2016). *It's more than just changing your password: exploring the nature and antecedents of cyber-security behaviours*. M.A. Thesis. Florida, USA: University of South Florida.

Eren, B. (2018). Retrieved from: https://twitter.com/erenbilal/status/1001416233475026945/. [Accessed 19 October 2021]

Erol, O., Şahin, Y. L., Yılmaz, E., Haseski, H. İ. (2015). Personal cyber security provision scale development study. *International Journal of Human Sciences*, *12*(2), 75–91.

Facebook (2021, January 12). *December 2020 coordinated inauthentic behavior report*. Retrieved from: https://about.fb.com/news/2021/01/december-2020-coordinated-inauthentic-behavior-report/. [Accessed 19 October 2021]

Fung, B., Garcia, A. (2019, October 13). *Facebook has shut down 5.4 billion fake accounts this year*. Retrieved from: https://edition.cnn.com/2019/11/13/tech/facebook-fake-accounts/index.html. [Accessed 19 October 2021]

Giwah, A. D. (2019). *Empirical assessment of mobile device users' information security behavior towards data breach: leveraging protection motivation theory*. Doctoral Dissertation. Florida, USA: Nova Southeastern University.

Gold, H., O'Sullivan, D. (2020). *Facebook has a coronavirus problem. It's WhatsApp*. Retrieved from: https://edition.cnn.com/2020/03/18/tech/whatsapp-coronavirus-misinformation/index.html. [Accessed 19 October 2021]

Gonzales, L. (2017, March 1). *Best practices around social media safety*. Tech & Learning.

Hadlington, L. (2017). Human factors in cyber security; examining the link between Internet addiction, impulsivity, attitudes towards cyber security, and risky cyber security behaviours. *Heliyon*, *3*(7), e00346.

Hao, K., Basu, T. (2020). *The coronavirus is the first true social-media "infodemic"*. MIT Technology Review.

Hawken, A. (2018). *Parents warned not to let their children use DokiDoki Literature Club 'suicide' app because it's 'DANGEROUS'*. The Sun.

Ilhan, M., Cetin, B. (2014). Development of classroom assessment environment scale: validity and reliability study. *Education and Science*, *39*(176), 31–50.

Johnson, J. (2021, June 25). *U.S. cyber bullying environments 2020*. Statista.

Johnson, M. (2019). *Police are warning parents about a '48-hour challenge' that encourages teens to go missing*. Retrieved from: https://www.yahoo.com/lifestyle/police-warning-parents-48-hour-challenge-encourages-teens-go-missing-170544613.Html/. [Accessed 19 October 2021]

Jöreskog, K. G., Sörbom, D. (1993). *Structural equation modelling with the SIMPLIS command language*. Chicago: Scientific Software International, Inc.

Khalaf, R. (2017). *UAE police and experts warn against Saudi 'Mariam' game*. Step Feed.

Kemp, S. (2020). *Digital 2020 global overview report*. Datareportal.

Kemp, S. (2021a). *Digital 2021 global overview report*. We are social.

Kemp, S. (2021b). *Digital 2021 Turkey*. Datareportal.

Kim, E. B. (2013). Information security awareness status of business college: undergraduate students. *Information Security Journal: A Global Perspective*, *22*(4), 171–179.

Kjørvik, H. (2010). *Implementing and improving awareness in information security*. Master Thesis. Norway: University of Agder.

Kline, P. (1994). *An easy guide to factor analysis*. New York: Routledge.

Kline, R. B. (2011). *Principles and practice of structural equation modeling*. New York: Guilford Press.

Koyuncu, H. (2020). *Sosyal medyada koronavirüs paylaşımları: Doğru bilinen 10 yanlış*. (Coronavirus shares on social media: 10 wrongs that are known to be true). Euronews.

Linkedin Community Report (2020). *Fake accounts*. Retrieved from: https://about.linkedin.com/transparency/community-report. [Accessed 19 October 2021]

Marsh, H. W., Hau, K.T., Artelt, C., Baumert, J., Peschar, J. L. (2006). OECD's brief self-report measure of educational psychology's most useful affective constructs: cross-cultural, psychometric comparisons across 25 countries. *International Journal of Testing*, *6*(4), 311–360.

Menczer, F. (2018). *How many social media users are real people?* GIZMODO.

Micklea, Z. (2020, October 4). *Increase in cyberbullying during COVID-19*. MI Blues Perspectives.

Morris, E. (2019). *7 social media security risks you need to be aware of today*. BestTechie.

Muhirwe, J., White, N. (2016). Cybersecurity awareness and practice of next generation corporate technology users, *Issues in Information Systems*, *17*(II), 183–192.

Newberry, C. (2020, May 20). *Social media security tips and tools to mitigate risks*. Hootsuite.

Priyanka, R. (2021, March 5). *Cyberattack shuts down online learning at 15 UK schools*. CyberSafe.

Rakipoğlu, Z. (2020). *Bir tık uğruna paylaşılan asılsız bilgiler 'psikolojik enfeksiyon' yayıyor*. (Unfounded information shared for the sake of a click spreads a 'psychological infection'). Retrieved from: https://www.aa.com.tr/tr/yasam/bir-tik-ugruna-paylasilan-asilsiz-bilgiler-psikolojik-enfeksiyon-yayiyor-/1805491. [Accessed 19 October 2021]

Rodríguez, C. P., Carballido, B. V., Redondo-Sama, G., Guo, M., Ramis, M., Flecha, R. (2020). False news around COVID-19 circulated less on Sina Weibo than on Twitter. How to overcome false information? *International and Multidisciplinary Journal of Social Sciences*, *9*(2).

Ryan, J. (2019). *GAME OF DEATH The truth behind sinister Momo Challenge suicide game that's been linked to a string of deaths and is spreading panic around UK*. The Sun.

Şalt, M. (2018). *Social media madness "eraser challenge" hospitalized a young student!* Retrieved from: https://www.webtekno.com/sosyal-medya-cilginligi-silgi-meydan-okumasi-genc-ogrenciyi-hastanelik-etti-h26987.html/. [Accessed 19 October 2021]

Schermelleh-Engel, K., Moosbrugger, H., Müller, H. (2003). Evaluating the fit of structural equation models: tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*, *8*(2), 23–74.

Schumacker R. E., Lomax, R. G. (2010). *A beginner's guide to structural equation modeling*. New York: Taylor & Francis Group.

Scott, M. (2020). *Social media giants are fighting coronavirus fake news. It's still spreading like wildfire*. Politico.

Senthil Kumar, N., Saravanakumar, K., & Deepa, K. (2016). On privacy and security in social media – A comprehensive study. *Procedia Computer Science*, *78*(Dec), 114–119.

Sharma, S. & Gupta, B. (2018). Information privacy on online social networks: illusion-in-progress in the age of big data? In *Analytics and Data Science*, 179–196. Springer.

Şimşek, Ö. F. (2007). *Yapısal eşitlik modellemesine giriş, temel ilkeler ve LİSREL uygulamaları*. (Introduction to structural equation modeling, basic principles and LISREL applications). Ankara: Ekinoks.

Sırt, T. (2017). *Be careful about the bait of gift tokens*. Sabah.

Sobers, R. (2018). *Social media security: how safe is your information?* Varonis.

Tavşancıl, E. (2005). *Measuring the attitudes and data analysis with SPSS*. Ankara: Nobel Publishing.

The World Bank (2020). *How countries are using edtech (including online learning, radio, television, texting) to support access to remote learning during the COVID-19 pandemic*. The World Bank.

Tosun, N. (2015). Social network use of vocational high school students. In *Internet in Turkey Conference Book*, 123–135. Turkey: Istanbul University.

TÜBA (2020). *Türkiye bilimler akademisi COVID-19 küresel salgın değerlendirme raporu, 26 Nisan 2020*. (Turkish academy of sciences COVID-19 global outbreak evaluation report, 26 April 2020). Ankara: TÜBA.

Tuncer, M., Dikmen, M. (2016). *New danger in social networks: cyber bullying. Re-discovery learning with digital learners*. Elazığ: Electronic Book.

Turgut, F., Baykul, Y. (1992). *Scaling techniques*. Ankara: ÖSYM Publishing.

Turkish Penal Code (2004). *Turkish penal code*. 9024. Retrieved from https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf. [Accessed 19 October 2021]

Tutorful (2020). *Social media safety*. Tutorful.

Waltz C. F., Strcikland, O. L., Lenz, E. R. (2010). *Measurement in nursing and health research*. New York: Springer Publishing Company.

Wang, J., Wang, X. (2012). *Structural equation modeling: applications using Mplus*. Chichester: John Wiley & Sons.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., et al. (2018). Finding the weakest links in the weakest link: how well do undergraduate students make cybersecurity judgment? *Computers in Human Behaviour, 84*(Feb), 375–382.

Yavanoğlu, U., Sağiroğlu, Ş., Çolak, İ. (2012). Social networking threats and precautions. *Gazi University Journal of Polytechnic*, *15*(1), 15–27.

Yıldırım, N. & Varol, A. (2013). Security in social networks: a case study carried out in Bitlis Eren and Fırat universities. *Journal of TBV Computer Science and Engineering*, *6*(1).

Zwick, W. R. & Velicer, W. F. (1986). Comparison of five rules for determining the number of components to retain. *Psychological Bulletin*, *99*(3), 432–442.

Appendix

Below are statements regarding the behaviors demonstrated by users in a safe social networking. Please read each statement attentively and mark one option (Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, Strongly Agree) that best defines you. Please, respond to all the questions without skipping any		Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Agree Strongly
1	In my time tunnel/wall, I do not share contents which can harm to other people (e.g., accusations, threats, mockery, unfounded news, lies, and gossips).					
2	In my time tunnel/wall, I do not share contents related to violence.					
3	In my time tunnel/wall, I do not share illegal statements.					
4	In my time tunnel/wall, there can be no sexually explicit contents.					
5	In my time tunnel/wall, I do not share private information of other people.					
6	In my time tunnel/wall, there can be no contents including insulting expressions.					
7	In my time tunnel/wall, I restrict access of people whom I do not want to see the statements I share.					
8	In my time tunnel/wall, I do not allow hateful messages.					
9	In my time tunnel/wall, anyone cannot share contents.					
10	In my time tunnel/wall, I do not share information I do not get from primary sources.					
11	My cover photo in social networks is accessible to anybody.					
12	Anybody can share my cover photo in social networks.					
13	Anybody can see my profile photo in social networks.					
14	Anybody can share my cover photo in social networks.					
15	The private information about my birth date, birth place, address, ID number, phone number, e-mail address, bank account number, political opinion, religious belief and relationship status that I share in my social network profile is accessible to anybody.					
16	Anybody can access to my social network profile from search engines.					
17	I do not add persons whom I do not know in my social network friends list.					
18	I do not accept friendship requests from persons whom I do not know.					
19	If I realize that social network account of one of my friends is hacked, I inform the Help Desk.					
20	I report malicious contents in social networks to the Help Desk.					
21	I run the applications with my social network login information.					
22	I log in to different applications and websites with my social network information.					
23	I do cybershopping with my social network information.					
24	In order to login my social network account, I get the backup codes in case of not receiving two-step authentication message.					
25	I use two-step authentication (via phone code messaging) to login my social network accounts.					
26	While logging in my social network accounts, I prefer using https which is a secure transfer protocol (hypertext transfer protocol secure) instead of http.					
27	I adjust my social network account setup in a way warning me if a new device is used to be logged in.					
28	I change my social network password periodically.					