Scientific Research Publishing

Journal of Computer and Communications, 2022, 10, 41-63
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Identification and Validation of Social Media Socio-Technical Information Security Factors with Respect to Usable-Security Principles

Joe Mutebi[1], Margaret Kareyo[1], Umezuruike Chinecherem[1], Akampurira Paul[2]

[1]Department of Information Technology, School of Computing and Mathematics, Kampala International University (KIU), Kampala, Uganda
[2]Department of Computing, Faculty of Science and Technology, KIU—Western Campus, Kampala, Uganda
Email: mutebi.joe@kiu.ac.ug, margaret.kareyo@kiu.ac.ug, cumecuruike@kiu.ac.ug, akampurira.paul@kiu.ac.ug

How to cite this paper: Mutebi, J., Kareyo, M., Chinecherem, U. and Paul, A. (2022) Identification and Validation of Social Media Socio-Technical Information Security Factors with Respect to Usable-Security Principles. *Journal of Computer and Communications*, **10**, 41-63.
https://doi.org/10.4236/jcc.2022.108004

Received: June 15, 2022
Accepted: August 14, 2022
Published: August 17, 2022

Abstract

The goal of this manuscript is to present a research finding, based on a study conducted to identify, examine, and validate Social Media (SM) socio-technical information security factors, in line with usable-security principles. The study followed literature search techniques, as well as theoretical and empirical methods of factor validation. The strategy used in literature search includes Boolean keywords search, and citation guides, using mainly web of science databases. As guided by study objectives, 9 SM socio-technical factors were identified, verified and validated. Both theoretical and empirical validation processes were followed. Thus, a theoretical validity test was conducted on 45 Likert scale items, involving 10 subject experts. From the score ratings of the experts, Content Validity Index (CVI) was calculated to determine the degree to which the identified factors exhibit appropriate items for the construct being measured, and 7 factors attained an adequate level of validity index. However, for reliability test, 32 respondents and 45 Likert scale items were used. Whereby, Cronbach's alpha coefficient (α-values) were generated using SPSS. Subsequently, 8 factors attained an adequate level of reliability. Overall, the validated factors include; 1) usability—*visibility*, *learnability*, and *satisfaction*; 2) education and training—*help* and *documentation*; 3) SM technology development—*error handling*, and *revocability*; 4) information security—*security*, *privacy*, and *expressiveness*. In this case, the confirmed factors would add knowledge by providing a theoretical basis for rationalizing information security requirements on SM usage.

Keywords

Social Media Usage, Information Security Factors, Cyber Security, Socio-Technical, Usable-Security

1. Introduction

Social Media (SM) usage has often been perceived through the lens of traditional information security systems. Whereby, information security parameters are identified, developed and implemented using objective information security principles [1]. Contrarily, SM usage embraces both objective, and subjective principles of information security systems [1] [2]. Hence, the development of information security systems would take into consideration both the objective, and subjective aspects of information security principles. In this case, the study professes SM usage into social and technical dimensions, respectively. The social dimension attributes consist of the behavioral (subjective) aspects of information security, while the technical dimension entails the technology (objective) aspects of information security [1] [3] [4]. In line with usable-security principles, no study has been done to identify SM usage information security factors, in the domain of social, and technical dimensions [3]. Existing studies often focus on information security attributes associated with mainly the technical aspect of SM usage [5]. And yet, numerous studies have reported social-engineering (behavioral) attacks as one of the prevalent forms of online information security breaches [4] [5]. Therefore, this study was intended to identify, examine, and validate SM socio-technical information security factors, in line with usable-security principles.

Relatively, existing studies on SM usage often focus on the descriptive roles, or practitioner's experience, while specifying benefits and risks associated with mainly the technical aspect of information security, which may be context specific [3] [4] [6]. As such, their measures and findings could be limited in scopes, and prone to duplications, redundancy, or inconsistency [1]. Contrarily, this study focused on identifying the key SM usage information security factors within the social, and technical domain of SM usage, with respect to usable-security principles [4] [7] [8]. In this case, SM socio-technical information security factors are attributes of SM functions that embrace SM operational requirements ranging from hardware, software, personal, and organizational structures [3] [4]. The components of the social dimension include; the people (SM users), and organization (structure), while the technical dimension includes the technology (SM platforms), and tasks performed [3] [4]. With respect to usable-security principles, SM socio-technical information security factors are attributes of information security, which embraces the technical information security factors, but also takes into consideration usability aspects of those factors, in a seamless way [4] [7]. Thus, SM socio-technical information security factors were identified based on usable-security principles [4] [7] [9].

1.1. SM Definition

In congruent with SM practitioners and researchers, SM is often defined as "a group of internet-based applications built on ideological and technological foundation of Web 2.0 concepts, which enables creation, modification, and sharing of user-generated contents online" [10] [11]. In this case, SM usage domain entails the social dimension, and technical dimension, respectively [1] [6]. Generally, the key roles of SM usage include relationship development, information sharing, self-presentation, and entertainment [12] [13] [14] [15]. For instance, Facebook, Twitter, and LinkedIn are mainly used for relationship development, while Instagram, YouTube, and Snapchat are known for sharing multimedia contents online [16]. Notably, the unique characteristics of SM usage are its ability to enable individual users to subjectively create, modify, and share user-generated contents online. Relatively, the design of the traditional information security systems is characterized by objectivity, while SM usage embraces both objectivity, and subjectivity principles [1] [10]. Therefore, with respect to information security management, the subjective, liberal and transparence nature of SM operations propagates new information security challenges associated with mainly the social (behavioral) aspect of SM usage [5] [6]. According to [6], the main information security challenges associated with SM usage include; confidentiality, litigation, and information overload [6].

Nevertheless, from the technical (objective) perspective, various SM platforms are enhanced with customizable security functions to support SM users in managing information security [6] [17]. For instance, Facebook and Twitter use two-factor verification principles: passwords as well as verification codes established using mobile devices. This authentication process helps to diminish the risk of compromising user accounts, and could avert attackers from appropriating an authentic account [17]. Furthermore, Facebook users can adjust security configurations and select users who can view their contents, and sensitive information. It can also authorize the users to allow or deny accessibility to a third party to their private contents. On the other hand, WhatsApp communication is end-to-end encrypted between two parties. The other key information security settings include: firewall settings, anti-virus, anti-spam filter, VPN setting, intrusion detection, etc. [6]. This, therefore, could imply that much of the reported risks and breaches associated with SM usage could emanate from the social (behavioral) aspect of SM usage, such as lack of knowledge, weak policy, education/training in SM usage, etc. [2] [5] [6] [18]. Since the technical aspect are enhanced with capabilities to manage and mitigate some of the dominant information security risks associated with SM usage [17].

1.2. Socio-Technical Information Systems

The phrase "socio-technical information system" embraces and mainly two dimensions of information systems: the social (people, and structures) dimension and technical (technology, and tasks) dimension [4] [7] [8]. In this case, the social dimension consists of SM users, and organizational structures including; responsibilities, rules, and policies that guide SM users in achieving the intended tasks [19]. Synonymously, the technical dimension entails the technology artifact, and knowledge required to translate system inputs into outputs [20]. On the other hand, the term usable security refers to the technical aspect of information security functions, and the usability (visibility, learnability, satisfaction, etc.) of those functions [7] [8]. Ferreira *et al.* (2014) define a usable-security information system as "one that is secure technically, even when used by people". In this case, information security system which is secure technically, but difficult to use is less secure. Therefore, with respect to usable-security principles, the social, and technical dimensional factors could be identified as usability factors, and security factors, respectively [4] [7]. Altogether, the relevant factors were then identified, examined and validated, accordingly.

2. Objectives

The main objective of this study was to identify, verify, and validate Social Media (SM) socio-technical information security factors, in line with usable-security principles. Specifically, the study focused on the following specific objectives:

1) To identify the key Social Media (SM) socio-technical information security factors, in line with usable-security principles.

2) To verify the characteristics of the key Social Media (SM) socio-technical information security factors, in line with usable-security principles.

3) To validate the key Social Media (SM) socio-technical information security factors.

2.1. Methodology

The study followed literature search techniques, using mainly web of science databases. The strategy used in literature search includes Boolean keyword search, and citation guide. The relevant literatures were identified, and their contents scrutinized, in line with study objective. Afterwards, the key factors were verified and sanctioned for validation process. Both theoretical and empirical methods of validation were used. Thus, Theoretical validity test was conducted on 45 Likert scale items, using validity form, and involving 10 subject experts (reviewers). The expert was selected from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), all in Uganda. The validity process focused on "relevancy", and "clarity" of the items. From the score ratings of the reviewers, Content Validity Index (CVI) was calculated using mean score values, at acceptable levels of CVI ≥ 0.78 [21]. On the other hand, empirical method was employed in reliability test conducted on 45 Likert scale items, using questionnaire, and involving 32 respondents. The respondents were selected from MUST and KIU, accordingly. Afterwards, Cronbach's alpha coefficient (α-values) was then generated on SPSS, at acceptable range of $0.70 \leq \alpha \leq 0.90$ [22]. Overall, the results for both literature search and validation process (validity test, and reliability test) are presented in section 3, accordingly.

2.2. Literature Search Process

The strategies used in literature search include; keyword search, and citation guides, employing mainly web of science databases. Relatively, the criteria settings in web of science search engine match with the study theme, and objectives [23]. To optimize the accuracy and relevancy of search results, Boolean search criteria were used to configure the searches. The main sets of Boolean keywords used to initiate the search process include; "Social Media usage AND information security"; "socio-technical"; "usable-security". The other search criteria used to filter and streamline the search results further include; sort by relevance (keywords), availability of source (online, open access, and peer reviewed), resource type (article, and books), subject area (keywords), literature date range (2012 to 2022), and language used (English) [23]. The relevant literatures were then filtered, scrutinized, and presented using literature summary table. The main attributes used to summarize the literatures include; the author, country, research purpose, methodology used, type of source, and summary points (factors). Subsequently, the key SM socio-technical information security factors were identified from the relevant literatures, and sanctioned for validation process. However, some of the relevant literatures excluded by search criteria were scrutinized to substantiate some of the relevant facts mentioned in the literatures.

2.3. Factor Validation Process

Validation process was then conducted to evaluate the key factors identified. The process used included theoretical validity test, and reliability test methods. Thus validity test was conducted on 45 Likert scale items, using validity form, and involving 10 subject experts (reviewers). The validity form was developed based on 4-points Likert scale rating, focusing on the "relevancy", and "clarity" of the items. The form contained section on instructions to reviewers, demographic profiles, and the factors. Each item for "relevancy" was developed with responses (rating) ranging from "not relevant—1, item need some revision—2, relevant but need minor revision—3, very relevant—4". Similarly, for "clarity", the measures ranges from "not clear—1, item need some revision—2, clear but need minor revision—3, very clear—4" [21]. The experts used were experienced lecturers, and researchers from MUST and KIU, with MSc, and PhD qualifications. From the score ratings of the experts, Content Validity Index (CVI) was calculated using mean score values, at acceptable levels of CVI ≥ 0.78 [21]. The detailed CVIs results, are presented in Section 3, accordingly.

On the other hand, reliability test was conducted on 45 Likert scale items, using questionnaire, and involving 32 respondents. Each questionnaire item was developed with a 5-point Likert scale, with measures ranging from "strongly disagree—1, disagree—2, neutral—3, agree—4, and strongly agree—5" [21] [24]. The respondents used were students, and staff from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. The study selected higher institutions of learning because SM usage is more prevalent in higher education, than the other formal settings in Uganda [25] [26]. Data were then collected, processed, and captured into SPSS for analysis. Cronbach's alpha coefficient (α-values) was generated, at acceptable range of $0.70 \leq \alpha \leq 0.90$ [22] [24]. Overall, the detailed results are presented in section 3, accordingly.

3. Results

In line with the study objectives, section 3 covers data/results presentation. The results are presented in a narrative, tabular and chart formats, accordingly. At the beginning of the sections, the presentation commenced with literature search results, and demographic profiles of the experts, and respondents, respectively, followed by validity test, and reliability test results, accordingly.

3.1. Literature Search Results

The main sets of Boolean keywords used to initiate the search process include; "Social Media usage AND information security"; "socio-technical"; and "usable-security". The other search criteria used to filter and streamline the results further included; sort by relevance (keywords), availability of source (peer reviewed journals), resource type (journal articles), subject area (keywords), literature date range (2012 to 2022), and language used (English). At the onset of literature search process, the Boolean keywords; "Social Media usage AND information security", search results retrieved 170 literatures. However, after applying the other search criteria, the results were reduced to 99 literatures. Afterwards, the 99 literatures were scrutinized using citation guide and 13 literatures were found relevant to the study. The other sets of keywords used in the search process include; "socio-technical", and "usable-security". For each set of the keyword, the relevant literatures were 4 out 15 literatures retrieved, and 3 out of 14 literatures retrieved, respectively.

However, after applying search criteria using Boolean keywords; "Social Media usage AND socio-technical factors", in line with the study gap, only 1 literature was retrieved, even after adjusting the date range criteria from 2012 to 2000 [3]. With respect to study gap, no literature was returned with the Boolean keywords; "Social Media usage AND socio-technical AND usable-security". Overall, the key factors identified from the relevant literatures include; SM usage and information security factors (SMISF), socio-technical information security factors (STF), and information system usable-security factors (USF). Table A1 (**Appendix A**) presents the set of 20 relevant literatures, indicating the authors, country, study purpose, methodology used, type of source, and summary of key points (factors).

From Table A1 (Appendix A), factors appearing in all the 3 main sets of Boolean key words search (SMISF, STF and USF) were considered appropriate, and relevant for inclusion into the list of SM socio-technical information security factors. In this case, the key factors identified and examine under social dimension include; 1) usability factors—*visibility*, *learnability* and *satisfaction*, 2) training and education factors—*help* and *documentation* [9] [26] [27] [28]. On the other hand, the key factors identified under technical dimension include; 3) SM technology development factors—*error handling*, and *process revocability*; 4) information security factors—*security*, *privacy* and *expressiveness* [4] [9]. Therefore, with respect to SM usage, the relevant factors would be the common factors of the set elements represented by intersection of the 3 sets, (SMISF ∩ STF ∩ USF) [4]. **Figure 1** below present a venn-diagram indicating the common factors of the set elements denoted by the 3 sets (SMISF ∩ STF ∩ USF); SM information security factors (SMISF), socio-technical factors (STF), and useable-security factors (USF), accordingly.

3.2. Data Evaluation

After identifying the relevant SM socio-technical information security factors, questionnaire and validity forms, were developed. The questionnaire items were adopted from validated information security principles developed by [4] Mujinga, Eloff & Kroeze (2019), and moderated to suit the study objectives. Each questionnaire item was developed with a 5-point Likert scale measures, with responses ranging from "strongly disagree—1, disagree—2, neutral—3, agree—4, and strongly agree—5". The items were then revised to conform to positively worded questions. Thus, factors with "agree" and "strongly agree" would therefore mean better information security compliance, while low agreement levels such as "disagree" and "strongly disagree" would mean vulnerable or weak information security compliance. On the other hand, the 4-point Likert scale measures on the "relevancy" of the items include; "not relevant—1, item need some revision—2, relevant but need minor revision—3, very relevant—4". Similarly, for "clarity", the measures ranges from "not clear—1, item need some revision—2, clear but need minor revision—3, very clear—4". Afterwards, the contents (factors and items) of the questionnaire instrument, and validity forms were then developed, and operationalized on separate templates. However, **Table B1** (Appendix B) present the contents of the questionnaire, and validity form on a single template.

3.3. Demographic Profiles—Experts

The experts used in this study were information security lecturers, including ICT professionals from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), all in Uganda. The main attributes that guided the selection of the experts were qualifications (MSc. and PhD.), area of specialty, and year of experience in academics, and research [21]. Altogether, 10 experts were identified, and individually given validity forms with clear instruction, to independently complete the form. More so, they were verbally briefed, and guided on the study purpose, and how to complete the form, and they all consented. **Table 1** presents the demographic profiles of the experts.

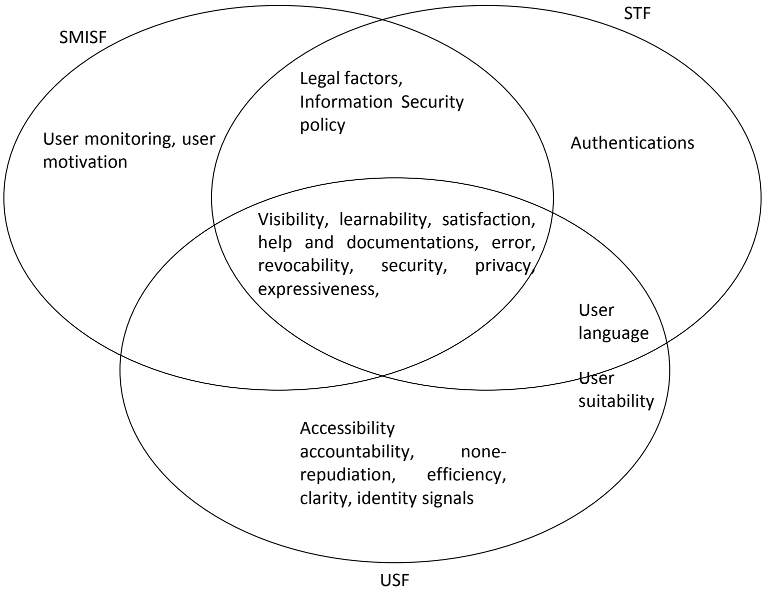
SMISF
STF
User monitoring, user motivation
Legal factors, Information Security policy
Authentications
Visibility, learnability, satisfaction, help and documentations, error, revocability, security, privacy, expressiveness,
User language
User suitability
Accessibility accountability, none-repudiation, efficiency, clarity, identity signals
USF

Figure 1. Common SM usage factors.

Table 1. Experts demographic profiles.

Experts ID	Institution	Gender	Age	Qualification	Specialization	Experience
Exp1	KIU	Male	36 - 40	MSc	Computer Engineering	11 - 15 years
Exp2	KIU	Male	41 - 45	PhD	Computer Science	11 - 15 years
Exp3	KIU	Male	Above 45	PhD	Information Systems	Above 15 years
Exp4	MUST	Male	36 - 40	MSc	Information Systems	6 - 10 years
Exp5	KIU	Female	36 - 40	MSc	Computer Science	11 - 15 years
Exp6	MUST	Male	Above 45	MSc	Information Systems	6 - 10 years
Exp7	MUST	Female	Above 45	PhD	Information Systems	11 - 15 years
Exp8	KIU	Male	41 - 45	PhD	Biomedical Science	11 - 15 years
Exp9	MUST	Female	31 - 35	MSc	Computer Science	6 - 10 years
Exp10	KIU	Male	36 - 40	MSc	Information Systems	Above 15 years

3.4. Demographic Profiles—Respondents

The respondents used in this study were mainly students, including few staff from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. The study preferred higher institutions of learning because SM usage is more prevalent in higher education, than the other formal settings in Uganda [25] [26]. **Table 2** below summarizes and presents the demographic profiles of the respondents, showing the representativeness of the sample characteristics within the category divides. Thus, indicating the frequency counts, and the corresponding percentage distributions, respectively.

Altogether, 32 respondents were given questionnaire to complete. Afterwards, the questionnaires were collected, processed, and captured into SPSS for analysis. In this case, the 10 experts were used in validity test, which was concerned with "how the measures sufficiently represent the construct that it was supposed to measure". While the 32 respondents were used in reliability test, which was mainly concerned with "the extent to which the measure of the construct is consistent and dependable" [21]. **Table 3** below summarizes and presents the results for the key factors, indicating percentage level of agreement on the items for each factor, accordingly. (n = 32; MUST n = 14, KIU n = 18).

From **Table 3**, the level of percentage agreement on each factor, combining "agree" + "strongly agree", include; *visibility* (MUST 40%; KIU 37%), *learnability* (MUST 40%; KIU 41%), *satisfaction* (MUST 42%; KIU 41%), *errors handling* (MUST 35%; KIU 37%), *revocability* (MUST 42%; KIU 32%), *help* and *documentations* (MUST 42%; KIU 37%), *security* (MUST 41%; KIU 35%), *privacy* (MUST 42%; KIU 40%), *expressiveness* (MUST 42%; KIU 38%). Relatively, MUST response shows slight over-edge in percentage agreement level compared to KIU, which could imply slightly better SM usage security compliance at MUST compared to KIU. However, the validity, and reliability test results explain the consistency levels within the datasets, as presented in the subsequent sections below.

Table 2. Respondent demographic profiles.

	MEDICAL INSTITUTIONS	MUST				KIU			
	Demographic profiles	Medical students		Medical staff		Medical students		Medical staff	
1	Gender	n = 11	(100%)	n = 3	(100%)	n = 13	(100%)	n = 5	(100%)
	Male	08	73%	02	67%	07	54%	04	80%
	Female	03	27%	01	33%	06	46%	01	20%
2	Age group								
	18 - 25	07	64%	00	00%	08	62%	00	00%
	26 - 35	03	27%	02	67%	05	38%	02	40%
	36 - 45	01	09%	01	33%	00	00%	03	60%
	46 years and above	00	00%	00	00%	00	00%	00	00%
3	Academic Department								
	Computer Science	04	36%	01	33%	04	31%	02	40%
	Information System	05	45%	02	67%	05	38%	02	40%
	Biomedical Science	02	19%	00	00%	04	31%	01	20%

Table 3. SM socio-technical factors, level of agreement.

Factors	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)	Total (%)
Mbarara University of Science and Technology (n = 14)						
Visibility	06%	14%	40%	28%	12%	100%
Learnability	03%	15%	42%	27%	13%	100%
Satisfaction	03%	18%	37%	30%	12%	100%
Error handling	05%	20%	40%	22%	13%	100%
Revocability	09%	18%	41%	23%	09%	100%
Help and documentation	03%	11%	44%	32%	10%	100%
Security	05%	15%	39%	28%	13%	100%
Privacy/confidentiality	03%	19%	36%	29%	13%	100%
Expressiveness	07%	16%	35%	30%	12%	100%
Kampala International University (n = 18)						
Visibility	09%	16%	38%	28%	09%	100%
Learnability	05%	19%	37%	27%	12%	100%
Satisfaction	05%	16%	38%	30%	11%	100%
Error handling	06%	18%	39%	27%	10%	100%
Revocability	07%	18%	43%	22%	10%	100%
Help and documentation	07%	18%	38%	27%	10%	100%
Security	12%	22%	31%	26%	09%	100%
Privacy/confidentiality	08%	17%	35%	27%	13%	100%
Expressiveness	06%	17%	39%	27%	11%	100%

3.5. Validity Test

Validity test was conducted on data generated through validity form, using 45 Likert scale items, and involving 10 subject experts. From the score ratings of the experts, Content Validity Index (CVI) was calculated using mean score values, at acceptable level of CVI ≥ 0.78 [21]. Table 4 presents validity test results for the 9 factors, based on the relevancy, and clarity of the items.

From Table 4, factors with strong validity index include; 1) usability factors—*learnability* and *satisfaction*. 2) SM technology development factors—*error handling*, and *process revocability*; 3) information security factors—*security*, and *privacy*. On the other hand, factors with weak validity index include; 1) usability factors—*visibility*, 2) training and education factors—*help* and *documentation*, and 3) Information security factors—*expressiveness*. Notably, all the factors with weak validity items were recorded under "clear but need minor revision—3" option. Therefore, as guided by the experts, the question statements were reviewed and revised accordingly. The revised items include; 1) *Visibility*: Social Media help function is visible, for instance, a key branded with the word "HELP" instead of "HELP or a special menu". 2) *Help* and *documentation*: Social Media system visibly "shows" instead of "displays" the current selection/data input field. 3) *Expressiveness*: Social Media system can "prompt the user with" instead of "tell" the security state of the system and the alternatives for security-related actions if needed. Altogether, 9 factors were reasonable considered valid, and were sanctioned for reliability test based on the data collected from 32 respondents.

3.6. Reliability Test

Reliability test was conducted on 45 Likert scale items, using questionnaire, involving 32 respondents. The respondents used were students, and staff from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. Each item was developed with a 5-point Likert scale, with measures ranging from "strongly disagree—1, disagree—2, neutral—3, agree—4, and strongly agree—5" [21] [24]. Subsequently, Cronbach's alpha (α) values were then generated to reveal the consistency in the responses within the dataset. Items with Cronbach's Alpha values ($\alpha \geq 0.70$) were considered strong reliability items, while those with Cronbach's Alpha values between 0.50 to 0.70 were considered moderate reliability items, and those with Cronbach's Alpha values ($\alpha < 0.50$) were considered weak reliability items [29] [21] [24]. **Table 5** below presents the summary of reliability test results for the items under each factor, indicating the Cronbach's alpha (α) values for each factor, and the conclusion thereof.

Table 4. Validity test results (Item relevancy, and clarity).

DIMENSIONS	No of Items	No of Strong Validity Items	No of Weak Validity Items	Relevancy CVI ≥ 0.78	Clarity ≥ 0.78	Conclusion
Visibility	5	4	1	0.88	0.76	Acceptable
Learnability	5	5	0	0.87	0.91	Acceptable
Satisfaction	5	5	0	0.84	0.90	Acceptable
Error handling	5	3	0	0.84	0.86	Acceptable
Revocability	5	5	0	0.78	0.82	Acceptable
Help and documentation	5	4	1	0.96	0.74	Acceptable
Security	5	5	0	0.83	0.89	Acceptable
Privacy/ confidentiality	5	5	0	0.94	0.81	Acceptable
Expressiveness	5	4	1	0.83	0.72	Acceptable

Table 5. Reliability test results.

Factors	No of Items	No of Strong Reliability Items	No of Moderate Reliability Items	0.70 ≤ α ≤ 0.90	Conclusion
Visibility	5	5	0 revised	0.811	Acceptable
Learnability	5	5	0 revised	0.701	Acceptable
Satisfaction	5	5	0 revised	0.859	Acceptable
Error handling	5	4	1 revised	0.722	Acceptable
Revocability	5	3	2 revised	0.649	Acceptable
Help and documentation	5	4	1 revised	0.716	Acceptable
Security	5	5	0 revised	0.721	Acceptable
Privacy/ confidentiality	5	5	0 revised	0.799	Acceptable
Expressiveness	5	4	1 revised	0.860	Acceptable

From Table 5 above, all the 9 factors attained the acceptable level of reliability. However, the reliability result for *revocability* factor did not meet the minimum value range of 0.70 ≤ α ≤ 0.90. Altogether, the validated and maintained factors under social dimension include; 1) usability factors—*visibility*, *learnability* and *satisfaction*, 2) training and education factors—*help* and *documentation*. Meanwhile, the factors identified under technical dimension include; 3) SM technology development factors—*error handling*, and *process revocability*; 4) information security factors—*security*, *privacy* and *expressiveness* [4] [9] [30]. Overall, the relevance of the 9 factors is based on the process followed in this study, notwithstanding the study limitations. However, the following sections cover discussion of the results.

4. Discussion of Results

Presumably, the key SM socio-technical information security factors were mainly adopted from existing literatures, as guided by socio-technical, and usable-security principles [4] [8] [9]. In this case, the key factors identified and validated under social dimension include; 1) usability factors—*visibility*, *learnability* and *satisfaction*, 2) training and education factors—*help* and *documentation* [9] [26] [27]. Meanwhile, the key factors identified under technical dimension include; 3) SM technology development factors—*error handling*, and *process revocability*; and 4) information security factors—*security*, *privacy* and *expressiveness* [4] [9] [30]. Overall, all the 9 factors attained the acceptable level of validity test, and reliability test results. Remarkably, categorizing this factor under social, and technical dimensions is a reasonable way of defining the vulnerable scope of information security within SM usage domain [3]. Thus, the validated factors would provide SM practitioners and researchers with theoretical basis for rationalizing information security requirements on SM usage [4] [7].

According to [4], the operational definition of these factor include; 1) Visibility: SM system visibly keep users informed about their security status. 2) Learnability: SM system should ensure that security actions are easy to learn and remember: 3) *Satisfaction*: SM system should ensure that users have good experience when using the system and its security features. 4) *Error handling*: SM system should provide users with detailed security error messages that they can understand and act on. 5) *Process revocability*: SM system should allow users to revoke any of their security actions. 6) *Help* and *documentation*: SM system should make security help apparent and easy to find for users. 7) *Security*: SM system should provide trusted communication channels between the user and the data servers. 8) *Privacy* and *Confidentiality*: SM system should protect user information against unauthorized access by third parties. 9) *Expressiveness*: SM system should guide users on security in a manner that still gives them freedom of expression [4]. From the literatures, the main information security challenges associated with SM usage include; confidentiality, litigation, and information overload [6]. While the dominant factors highlighted and linked to the challenges were mainly social factors including; education and training, awareness, error handling, and user monitoring [5] [6] [31] [32].

5. Recommendations

Presently, SM platforms have continued to improve and attract new users and groups of persons with similar interests [33] [34]. For instance, in academic settings, university students and academic staff have continued to embrace SM usage in enhancing their academic operations [33] [34] [35]. In this case, SM usage would then provide a ubiquitous network space for effective interaction among students, supervisors and stakeholders [36] [37] [38]. However, from related literatures, the profound needs of preserving information security seem to be a stumbling block hindering ratification and adoption of SM usage [25] [33] [39] [40]. In this case, the validated SM socio-technical information security factors would provide SM practitioners, and researchers with alternative theoretical basis to rationalize information security requirements on SM usage [7]. The factors could be used by researchers to support evaluation and adoption of SM usage in business operations.

In reference to the study limitations, more empirical studies need to be conducted to enrich the theoretical foundations supporting SM usage in business operations. The few existing studies related to SM usage in business operations often depend on the descriptive approaches, or practitioner experience, or literature-search, which may be context specific [37] [39] [40]. As such, their measures and findings could be limited in scopes, and prone to duplications, redundancy, or inconsistency. Reasonably, the subjective nature of SM concepts makes it complex for existing theories and studies to have a standard definition of SM concepts [1]. This is mainly due to the transparence and casual nature of SM functions, where individual use colloquial forms of subjective language to express their views and opinions. Therefore, to address the unique challenges associated with SM usage, more empirical studies need to focus on generating empirical evidence to conquer the challenges often associated with unique characteristics of SM usage. The study also recommend for more empirical research to be done to assess the relative influence of the different SM socio-technical information security factors, on the safety of electronic information in organization.

6. Conclusion

This study was conducted with intention of identifying, verifying, and validating SM socio-technical information security factors, in line with usable-security principles. The study followed literature search techniques, as well as theoretical and empirical methods of factor validation. The strategy used in literature search technique included Boolean keywords search, and citation guides, using mainly web of science databases, as well as related online libraries. At the onset of the search process, 170 literatures were retrieved from different sources, but 20 literatures were found relevant to the study. As guided by study objectives, 9 SM socio-technical factors were identified, verified and validated. Both theoretical, and empirical validation processes were followed, and 7 factors attained an adequate level of validity index. However, for reliability test, 8 factors attained an adequate level of reliability. Overall, the validated factors included: 1) usability—*visibility*, *learnability*, and *satisfaction*; 2) education and training—*help* and *documentation*; 3) SM technology development—*error handling*, and *revocability*; 4) information security—*security*, *privacy*, and *expressiveness*. In this case, the validated factors would add knowledge by providing a theoretical basis for rationalizing information security requirements on SM usage. Thus, the validated factors would provide SM practitioners, researchers, and institutions with the theoretical basis for rationalizing information security requirements on SM usage [4] [7]. For instance, the factors could be used by institutions, and researchers to support the process of evaluation, and adoption of SM usage in business operations. However, more empirical studies still need to be done to enrich the theoretical foundation associated with unique (subjective) information security concepts on SM usage.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Emamjome, F.F., Rabaai, A.A., Gable, G.G. and Bandara, W. (2013) Information Quality in SM: A Conceptual Model. In: *Proceedings of the Pacific Asia Conference on Information Systems* (*PACIS* 2013), AIS Electronic Library (AIsel), Jeju Island, 72.

[2] Di Gangi, P.M., Johnston, A.C., Worrell, J.L. and Thompson, S.C. (2016) What Could Possibly Go Wrong? A Multi-Panel Delphi Study of Organizational Social Media Risk. *Information Systems Frontiers*, **20**, 1097-1116.

https://doi.org/10.1007/s10796-016-9714-2

[3] Lombardo, G., Mordonini, M. and Tomaiuolo, M. (2021) Adoption of Social Media in Socio-Technical Systems: A Survey. *Information* (*Basel*), **12**, 132. https://doi.org/10.3390/info12030132

[4] Mujinga, M., Eloff, M.M. and Kroeze, J.H. (2019) Towards a Framework for Online Information Security Applications Development: A Socio-Technical Approach. *South African Computer Journal*, **31**, 24-50. https://doi.org/10.18489/sacj.v31i1.587

[5] Tayouri, D. (2015) The Human Factor in the Social Media Security—Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, **3**, 1096-1100. https://doi.org/10.1016/j.promfg.2015.07.181

[6] Wilcox, H. and Bhattacharya, M. (2015) Countering Social Engineering through Social Media: An Enterprise Security Perspective. In: Núñez, M., Nguyen, N.T., Camacho, D. and Trawiński, B., Eds., *Computational Collective Intelligence*, Springer International Publishing, Berlin, 54-64. https://doi.org/10.1007/978-3-319-24306-1_6

[7] Agrawal, A., Alenezi, M., Khan, S.A., Kumar, R. and Khan, R.A. (2022) Multi-Level Fuzzy System for Usable-Security Assessment. *Journal of King Saud University. Computer and Information Sciences*, **34**, 657-665. https://doi.org/10.1016/j.jksuci.2019.04.007

[8] Ferreira, Huynen, J.-L., Koenig, V. and Lenzini, G. (2014) A Conceptual Framework to Study Socio-Technical Security. In: Tryfonas, T. and Askoxylakis, I., Eds., *Human Aspects of Information Security*, *Privacy*, *and Trust*, Springer International Publishing, Berlin, 318-329. https://doi.org/10.1007/978-3-319-07620-1_28

[9] Yeratziotis, A., Pottas, D. and Van Greunen, D. (2012) A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. *International Journal of Human-Computer Interaction*, **28**, 678-694. https://doi.org/10.1080/10447318.2011.654202

[10] Obar, J.A. and Wildman, S. (2015) Social Media Definition and the Governance Challenge: An Introduction to the Special Issue. *Telecomm Policy*, **39**, 745-750. https://doi.org/10.1016/j.telpol.2015.07.014

[11] Kaplan, M. (2012) If You Love Something, Let It Go Mobile: Mobile Marketing and Mobile SM 4x4. *Business Horizons*, **55**, 129-139. https://doi.org/10.1016/j.bushor.2011.10.009

[12] Hu, T. and Zhang, P. (2016) Social Media Usage as a Formative Construct: Conceptualization, Validation, and Implication. *Journal of Information Technology Management*, **27**, 151-168.

[13] Hu, T., Kettinger, W. and Poston, R. (2015) The Effect of Online Social Value on Satisfaction and Continued Use of Social Media. *European Journal of Information Systems*, **24**, 391-410. https://doi.org/10.1057/ejis.2014.22

[14] Kim, H., Chan, H.C. and Kankanhalli, A. (2012) What Motivates People to Purchase Digital Items on Virtual Community Websites? The Desire for Online Self-Presentation. *Information Systems Research*, **23**, 1232-1245. https://doi.org/10.1287/isre.1110.0411

[15] Chai, Das, S. and Rao, H.R. (2011) Factors Affecting Bloggers' Knowledge Sharing: An Investigation Across Gender. *Journal of Management Information Systems*, **28**, 309-342. https://doi.org/10.2753/MIS0742-1222280309

[16] Kietzmann, J.H., *et al.* (2011) Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. *Bus Horizon*, **54**, 241-251. https://doi.org/10.1016/j.bushor.2011.01.005

[17] Jain, Sahoo, S.R. and Kaubiyal, J. (2021) Online Social Networks Security and Privacy: Comprehensive Review and Analysis. *Complex & Intelligent Systems*, **7**, 2157-2177. https://doi.org/10.1007/s40747-021-00409-7

[18] Swinney, A. (2019) Creating a Social Media Risk Assessment. *Bank News*, **119**, 10-13.

[19] Paja, E., Dalpiaz, F. and Giorgini, P. (2013) Managing Security Requirements Conflicts in Socio-Technical Systems. In: Ng, W., Story, V.C. and Trujillo, J.C., Eds., *ER* 2013: *Conceptual Modelling*, Lecture Notes in Computer Science, Vol. 8217, Springer, Berlin, 270-283. https://doi.org/10.1007/978-3-642-41924-9_23

[20] Bélanger, F., Watson-Manheim, M.B. and Swan, B.R. (2013) A Multi-Level Socio-Technical Systems Telecommuting Framework. *Behaviour and Information Technology*, **32**, 1257-1279. https://doi.org/10.1080/0144929X.2012.705894

[21] Zamanzadeh, V., Ghahramanian, A., Rassouli, M., Abbaszadeh, A. and Alavi, H. (2015) Design and Implementation Content Validity Study: Development of an Instrument for Measuring Patient-Centered Communication. *Journal of Caring Science*, **4**, 165-178. https://doi.org/10.15171/jcs.2015.017

[22] Taherdoost, H. (2016) Sampling Methods in Research Methodology, How to Choose a Sampling Technique for Research. *International Journal of Advance Research in Management*, **5**, 18-27. https://doi.org/10.2139/ssrn.3205035

[23] Bramer, W.M., Rethlefsen, M., Kleijnen, J. and Franco Duran, O. (2017) Optimal Database Combinations for Literature Searches in Systematic Reviews: A Prospective Exploratory Study. *Systematic Reviews*, **6**, 245-245. https://doi.org/10.1186/s13643-017-0644-y

[24] Joshi, A., Kale, S., Chandel, S. and Pal, D.K. (2015) Likert Scale: Explored and Explained. *Current Journal of Applied Science and Technology*, **7**, 396-403. https://doi.org/10.9734/BJAST/2015/14975

[25] Olum, R., Kajjimu, J., Kanyike, A.M., *et al.* (2020) Perspective of Medical Students on the COVID-19 Pandemic: Survey of Nine Medical Schools in Uganda. *JMIR Public Health and Surveillance*, **6**, e19847. https://doi.org/10.2196/19847

[26] Schneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N. and Diakopoulos, N. (2016) Designing the User Interface: Strategies for Effective Human-Computer Interaction. Pearson Education, London.

[27] Preece, J., Rogers, Y. and Sharp, H. (2015) Interaction Design: Beyond Human Computer Interaction. Wiley and Sons, Hoboken.

[28] Zahidi, Yan Peng Lim and Woods, P.C. (2014) Understanding the User Experience (UX) Factors That Influence User Satisfaction in Digital Culture Heritage Online Collections for Non-Expert Users. 2014 *Science and Information Conference*, London, 27-29 August 2014, 57-63. https://doi.org/10.1109/SAI.2014.6918172

[29] Tamarah, S. and Samantha, S. (2018) Reliability and Validity of the Research Methods Skills Assessment. *International Journal of Teaching and Learning in Higher Education*, **30**, 80-90.

[30] Schneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N. and Diakopoulos, N. (2016) Designing the User Interface: Strategies for Effective Human-Computer Interaction. Pearson Education, London.

[31] Nyblom, P., Wangen, G. and Gkioulos, V. (2020) Risk Perceptions on Social Media Use in Norway. *Future Internet*, **12**, 211. https://doi.org/10.3390/fi12120211

[32] Herath, T.B.G., Khanna, P. and Ahmed, M. (2022) Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and*

Privacy, **2**, 1-18. https://doi.org/10.3390/jcp2010001

[33] Nwankwo, W. and Chinecherem, U. (2020) Institunalising Social Network Solution in Tertiary Educational Institutions. *Journal of Applied Sciences*, *Information and Computing*, **1**, 20-28.

[34] Al-Rahmi, W.M., Othman, M.S. and Yusuf, L.M. (2015) The Role of Social Media for Collaborative Learning to Improve Academic Performance of Students and Researchers in Malaysian Higher Education. *International Review of Research in Open and Distance Learning*, **16**, 177-204. https://doi.org/10.19173/irrodl.v16i4.2326

[35] Hamm, A., *et al.* (2013) Social Media Use by Health Care Professionals and Trainees: A Scoping Review. *Academic Medicine*, **88**, 1376-1383. https://doi.org/10.1097/ACM.0b013e31829eb91c

[36] Alenezi, A.N. and Yaiesh, S.M. (2018) The Ubiquitous Invasion of Social Media in Lifelong Learning in Medical Education. *Review Article Kuwait Medical Journal*, **50**, 271-277.

[37] Roy, D., Taylor, J., Cheston, C., Flickinger, T.E. and Chisolm, M.S. (2016) Social Media: Portrait of an Emerging Tool in Medical Education. *Academic Psychiatry Journal*, **40**, 136-140. https://doi.org/10.1007/s40596-014-0278-5

[38] Musah, A. (2015) Social Media Network Participation and Academic Performance in Senior High School in Ghana. Lancaster University, Lancaster.

[39] Whyte, W. and Hennessy, C. (2017) Social Media Use within Medical Education: A Systematic Review to Develop a Pilot Questionnaire on How Social Media Can Be Best Used at BSMS. *MedEdPublish*, **6**, 1-36. https://doi.org/10.15694/mep.2017.000083

[40] Surani, Z., *et al.* (2017) Social Media Usage among Health Care Providers. *BMC Research Notes*, **10**, Article No. 654. https://doi.org/10.1186/s13104-017-2993-y

Appendix A

Table A1. Literature summary.

Social Media usage, and Information Security Factors (SMISF)				
Author	Country	Purpose	Type of source (Methodology)	Summary of key points (factors)
(Tayouri, 2015)	Israel	"Identify cyber security risks, and mitigations, focusing on the human factor and social media usage."	Conference proceeding (Literature Review)	Education and training Error handling Information security - **Privacy/confidentiality** - **Availability**
(Wu He, 2012)	USA	"Review social media security risks and mitigation techniques"	Journal article (Literature review)	Security policy User monitoring Education and training Software update Error handling
(Jain, Sahoo, & Kaubiyal, 2021)	India	"Review different security and privacy threats, and existing solutions that can provide security to social network users"	Journal article (Literature review)	Security and privacy setting Authentication mechanism Report users
(Wilcox, & Bhattacharya, 2015)	Australia	"Countering Social Engineering through Social Media: An Enterprise Security Perspective"	Book chapter Literature Review	Effective security policy Increase awareness Education and training Legal factors Technical factors - **Anti-virus** - **Firewalls** - **Anti-spam filter** - **Access control** - **VPN** - **Intrusion detection** - **Encryption** - **Two factors authentication**
(Ma, Zhang, Li, & Wu, 2019)	China	"Exploring information security education on social media use: Perspective of uses and gratifications theory"	Journal article Survey and (Literature review and modeling)	Education and training User satisfaction Information security awareness
(Di Gangi, Johnston, Worrell & Thompson, 2016)	USA	"A multi-panel Delphi study of organizational social media risk"	Journal article (Delphi approach)	Social factors - **Effective policy** - **Awareness** - **Education and training** Technical factors Legal factors

Continued

(Philip Nyblom, Gaute Wangen, & Vasileios Gkioulos, 2020)	Norway	"Risk Perceptions on Social Media Use in Norway"	Journal article (Survey)	Security awareness
(Andrew Swinney, 2019)	USA	"Creating a Social Media risk Assessment"	Journal article (Literature review)	User training Effective policy Awareness
(Obrain et al., 2021)	South Africa	"Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa"	Journal article (Literature review)	Information Security awareness
(Albladi, & Weir, 2018)	Saudi Arabia	"Identify user characteristics that influence judgment of social engineering attacks in social networks"	Journal article Literature review, (Expert validation of factors)	Socio-emotional **- Social network trust** **- Usage motivation** Socio-psychological **- Education** **- Computer knowledge** **- Information security awareness** Perceptual **- Privacy awareness**
(Thilini, Prashant, & Monjur, 2022).	Switzerland	"Cybersecurity Practices for Social Media Users: A Systematic Literature Review"	Journal article (Literature review)	Awareness Training and education Information security
(Yeratziotis, Pottas, & Van Greunen, 2012)		"Usable-security Heuristic Evaluation for the Online Health Social Networking Paradigm"	Journal article (Literature review, heuristics)	**Usability factors** Visibility Learnability Satisfaction Aesthetic and minimalist design User language User suitability User assistance Error handling Clarity Revocability Identity signal Expressiveness **Security and privacy** Availability Privacy Integrity Confidentiality

Continued

(Mujinga, Eloff & Kroeze, 2019)	South Africa	"Investigates design principles for usable security and proposes a validated framework usable security design principles."	Journal article Literature, (Validation using Expert)	Social dimension **- Visibility** **- Learnability** **- Satisfaction** **- Help and documentation** **- User language** **- User suitability** Technical dimension **- Error handling** **- Revocability** **- Availability** **- Security** **- Privacy/confidentiality** **- Expressiveness**
(Ferreira, Koenig, & Lenzini, 2014)	Portugal	"A Conceptual Framework to Study Socio-Technical Security"	Book chapter (Literature review)	Social factors Technical factors
(Lombardo, Mordonini, & Tomaiuolo, 2021)	Italy	"Adoption of Social Media in Socio-Technical Systems: A Survey"	Journal article (Survey)	Social factors Technical factors Legal factors
Usable-security factors (USF)				
(Agrawal, *et al.*, 2022)	India	"Develop factors for assessment of usable-security systems"	Journal article (Survey)	**- Security factors—*confidentiality, availability, accessibility, accountability and none-repudiation,*** **- usability factors—*effectiveness, efficiency, satisfaction* and *error protection***
(Yeratziotis, Pottas, & Van Greunen, 2012)		"Usable-security Heuristic Evaluation for the Online Health Social Networking Paradigm"	Journal article (Literature review, heuristics)	**Usability factors** Visibility Learnability Satisfaction Aesthetic and minimalist design User language User suitability User assistance Error handling Clarity Revocability Identity signal Expressiveness **Security and privacy** Availability Privacy Integrity Confidentiality

Continued

(Shneiderman *et al.*, 2016)		"Identify grand challenges for HCI researchers."	Journal (Literature review)	Help and documentation Learning
(Mujinga, Eloff & Kroeze, 2019)	South Africa	"Investigates design principles for usable security and proposes a validated framework usable security design principles."	Journal article (validation using experts)	Usability - **Visibility** - **Learnability** - **Satisfaction** Information security - **Security** - **Privacy/confidentiality** - **Expressiveness**
(Zahidi, Yan Peng Lim, & Woods, 2014)		"Understanding the user experience (UX) factors that influence user satisfaction."	Conference proceeding	User satisfaction factors

Appendix B

Table B1. Questionnaire items, and validity form contents, (Items adopted from: [4] Mujinga, Eloff & Kroeze 2019).

	QUESTIONNAIRE ITEMS, AND CONTENT VALIDITY INDEX (**CVI**) ASSESSMENT FORM CONTNETS								
	1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree								
Questionnaire Items		Your assessment, kindly tick appropriately							
		Relevancy				Clarity			
1	**Visibility**: Social Media system should visibly keep users informed about their security status:	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
1.1	Social Media system show the user the progress status during a visible delay in response time								
1.2	Social Media system visibly shows the current selection/data input field								
1.3	Social Media system clearly highlight the problem field with regard to error messages								
1.4	Social Media system give feedback for every security-related action								
1.5	Social Media system visibly show the location of security-related options								
2	**Learnability**: Social Media system should ensure that security actions are easy to learn and remember:	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
2.1	Social Media provide easy-to-learn training material								
2.2	Social Media system have a quick-start guide to assist the user								
2.3	Social Media security options are selected by default								
2.4	Social Media user interface make it obvious which security items are currently selected								
2.5	Social Media system protect users against making severe errors								

Continued

3	**Satisfaction**: Social Media system should ensure that users have a good experience when using the system and its security features	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
3.1	The actual process of using Social Media system is fun and enjoyable								
3.2	Most frequently used function keys on Social Media are placed in the most accessible positions								
3.3	Social Media security-related prompts imply that the user is in control								
3.4	Social Media security mechanisms of the system provide a sense of protection to the user								
3.5	Social Media system fulfil its claimed capabilities								
4	**Error handling**: Social Media system should provide users with detailed security error messages that they can understand and act on	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
4.1	Social Media security-related error messages inform the user of the severity of the errors								
4.2	Social Media system warn users if they are about to make a potentially serious error								
4.3	Social Media system allow users to recover from errors quickly and easily								
4.4	Social Media error messages of the system not interfere with the users' work, whenever possible								
4.5	Social Media system clearly ask for users' confirmation of serious and possibly irrevocable actions								
5	**Process revocability**: Social media system should allow users to revoke any of their security actions	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
5.1	Social Media users can easily reverse their security and non-security actions								
5.2	Social Media users can cancel operations in progress								
5.3	Social Media system have "undo" and "redo" functions at the level of a single security action or for a complete group of security actions								
5.4	Social Media system provide confirmation for actions that have drastic, possibly destructive consequences								
5.5	Social Media system have a clearly marked exit								
6	**Help and documentation**: Social Media system should make security help apparent and easy to find for users	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
6.1	Social Media help function visible, for example, a key labelled HELP or a special menu								
6.2	Social Media help function cover security and non-security related information								

Continued

6.3	Social Media system provide an up-to-date security center, with security training and awareness information								
6.4	Social Media system provide complete and accurate help and a FAQs section								
6.5	Social Media language selection is possible, the translation accurate, without errors								
7	**Security**: Social Media system should provide trusted communication channels between the user and the data Servers	1	2	3	4	1	2	3	4
7.1	Social Media system initiate a session lock after a period of inactivity or on user request								
7.2	Social Media system enforces a limit on consecutive invalid access attempts by a user during a period of time.								
7.3	Social Media system implement an appropriate time-out logoff period								
7.4	Social Media system encrypt passwords in storage and in transmission								
7.6	Social Media system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.								
8	**Privacy and Confidentiality**: Social Media system should protect user information against unauthorized access by third parties	1	2	3	4	1	2	3	4
8.1	Social Media system clearly state what personal information is collected and for what purposes it will be used								
8.2	Social Media system require users to confirm statements indicating that they understand the conditions of access								
8.3	Social Media system ask for permission before distributing personal information to third parties								
8.4	Social Media personal information collection and storage mechanisms comply with the data protection regulation of the institution								
8.5	Social Media private or confidential contents are accessed with passwords								
9	**Expressiveness**: Social Media system should guide users on security in a manner that still gives them freedom of expression	1	2	3	4	1	2	3	4
9.1	Social Media users are initiators of security actions rather than respondents								
9.2	Social Media system correctly anticipate, and prompt for, the user's probable next security-related activity								
9.3	Social Media user can tell the security state of the system and the alternatives for security-related actions if needed								
9.4	Social Media system clearly state its security capabilities								
9.5	Social Media system clearly state the users' responsibilities in terms of security actions								