

**FACTORS INFLUENCING UNDERGRADUATE
STUDENTS' INTENTION TO USE SECURITY AND
PRIVACY PROTECTION MEASURES OF SOCIAL
NETWORKING SITES:
“A CASE STUDY IN MOGADISHU UNIVERSITY”**

ABDULKADIR JEILANI MOHAMOUD

ASIA e UNIVERSITY

2021

**FACTORS INFLUENCING UNDERGRADUATE
STUDENTS' INTENTION TO USE SECURITY AND
PRIVACY PROTECTION MEASURES OF SOCIAL
NETWORKING SITES:
“A CASE STUDY IN MOGADISHU UNIVERSITY”**

ABDULKADIR JEILANI MOHAMOUD

A Thesis Submitted to Asia e University in
Fulfillment of the Requirements for the
Degree of Doctor of Philosophy (ICT)

November 2021

ABSTRACT

Social networking sites (SNSs) have simplified the way people communicate and interact with each other, in addition to the benefits of using social media, there are also privacy risks surrounding the posting of personal data details on social media. Furthermore, students are vulnerable to cyber security attacks because their account was created by his/her friend. This resulting, to a lot of weakness and poor risk management. Therefore, the primary goal of this research is to advance students' intent while using social media through successful security and privacy-setting awareness. Four sub-objectives were investigated to reach the primary purpose of the study. The first sub-objective was to investigate students' awareness of security and privacy settings offered by social networking site providers. The second sub-goal of this study was to identify the impact of perceived training, value, attitude towards share, perceived benefit, and perceived severity attack on students' intention to use security and privacy safety options in social media. The third sub-goal of this study was to identify the comprehensive approach to making the students use the security and privacy measures in Social Networking Sites (SNSs). The fourth sub-objective of this study was to propose a suitable model (framework) for promoting security and privacy protection measures in Social Networking Sites (SNSs). This research is based on already recognized models: the model Protection Motivation Theory (PMT), the Technology Acceptance Model (TAM), and the Theory of Reasoned Action (TRA). The researcher sought empirical suggestions for the validation of the theoretical model and hypotheses. A web-based survey instrument was developed that contains 45 –items survey using Likert-type scales. The target population of this study was undergraduate students at Mogadishu University (Freshman, sophomore, junior and senior). The sample for this study was 378 students with and high response rate. Descriptive analysis was used to

accomplish the objectives of the study. The structural equation modeling technique was utilized to investigate both measurement model testing (reliability and validity) and structural models (hypotheses testing) to determine the factors influencing students' intention to use security and privacy protection measures in social media by undergraduate students. A pilot study was conducted to get valuable feedback about the questionnaire, and the researcher tested the validity and reliability of the gathered data through the questionnaire. The Cronbach's alpha reliability score of each item (independent variables and dependent variable) exceeded the recommended value of 0.70. the range of level of internal reliability became between 0.939 and 0.818. this result illustrates that the measurement of the questionnaire items is reliable and can be used in the study. The results revealed that perceived training, severity attack, perceived value, perceived benefits, and attitude toward share have a positively related to students' intention to use security and privacy safety option in social networking sites (SNSs); perceived awareness was not significant to the student's intention to use security and privacy safety option.

Keywords: Social Networking Sites, Students, Intention, Security and Privacy, Protection Measures

APPROVAL

This is to certify that this thesis conforms to acceptable standards of scholarly presentation and is fully adequate, in quality and scope, for the fulfillment of the requirements for the degree of Doctor of Philosophy

The student has been supervised by: Professor Ts. Dr Titik Khawa Abdul Rahman and co-supervised by: Dr John M. Kandiri

The thesis has been examined and endorsed by:

Ts Dr Sanath Sukumaran,

Agile Management Consultancy

Examiner 1

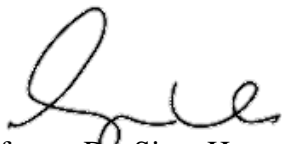
Associate Professor Dr. Roshayu Mohamad,

Associate Professor

University of Jeddah, Saudi Arabia

Examiner 2

This thesis was submitted to Asia e University and is accepted as fulfillment of the requirements for the degree of Doctor of Philosophy.



Professor Dr. Siow Heng Loke

Asia e University

Chairman, Examination Committee

3 October 2022

DECLARATION

The researcher, hereby declares that the thesis submitted in fulfillment of the Ph.D. degree is my work and that all contributions from any other persons or sources are properly and duly cited. Further, the researcher declares that the material has not been submitted either in whole or in part, for a degree at this or any other university. In making this declaration, the researcher, understand and acknowledges any breaches in this declaration constitute academic misconduct, which may result in my expulsion from the program and/or exclusion from the award of the degree.

Name: Abdulkadir Jeilani Mohamoud

Signature of Candidate

Date: 1 November 2021

ACKNOWLEDGEMENTS

A million thanks to the Almighty ALLAH who created me and moved me to pursue this degree. It's my pleasure to have a great chance to propose my research. This research on an excellent topic such as "Factors Influencing Students' Intention to Use Security and Privacy Protection Measure in social media (SM). "A case study Mogadishu University"

Secondly, I would like to offer my heartfelt to my wonderful supervisors, Prof. Dr. Tiktik Khawa Abdulrahman & Dr. John M. Kandiri for their tolerance and appreciated feedback in the enlargement and accomplishment of this research and support throughout my research, and for their great extent contributions to the success of this research. Special appreciation to the members of the thesis committee. Prof Dr Siow Heng Loke, AeU, Assoc Prof Dr Nasiroh Omar, UiTM, Dr Sanath Sukumaran &. Assoc Prof Dr. Roshayu Mohamad. The advice I received from these people significantly improved my research. Also, I am thankful to the administration and undergraduate students at Mogadishu university for their assistance in this research.

Thirdly, I want my thanks to going my parents, who are without them I do not exist. My next thanks go to my big brother Mr. Aweis Jeilani Mohamoud and to my biggest sister Malyun Jeilani Mohamoud who made me possible to reach this level of my knowledge, and both played an unforgettable role in my life. Their advice and direction have seen me through this work.

Finally, Great thanks go to my family and friends, especially to Dr. Said Abubakar Ahmed and Mohamed Ali Assier who supported me in the final phase of my research.

TABLE OF CONTENTS

ABSTRACT	ii
APPROVAL	iv
DECLARATION	v
ACKNOWLEDGEMENTS	vii
TABLE OF CONTENTS	viii
LIST OF TABLES	xi
LIST OF FIGURES	xiii
LIST OF ABBREVIATIONS	xiv
CHAPTER 1 INTRODUCTION	1
1.1 Introduction	1
1.2 Background of the study	1
1.3 Problem statement	5
1.4 Research objectives	9
1.5 Research questions	10
1.6 Justifications and significance of the study	13
1.7 Scope and limitations of the study	14
1.8 Assumptions of the study	15
1.9 Motivation	15
1.10 Structure of the chapters	17
1.11 Chapter summary	19
CHAPTER 2 LITERATURE REVIEW	21
2.1 Introduction	21
2.2 Concepts of social networking sites	22
2.3 Early social networking sites	23
2.4 Social media users in east Africa	26
2.5 The importance of social networking sites	27
2.6 Security identity in social networking sites	29
2.7 Characteristics of social networks	30
2.8 Social media and future consequence	31
2.9 Concepts, types, and attacks of cyber security	32
2.10 Managing social media privacy settings	36
2.10.1 Facebook privacy tab	36
2.10.2 Facebook profile setting	37
2.10.3 Facebook photo settings:	38
2.10.4 Summary of privacy settings on Facebook	38
2.10.5 Twitter privacy setting	39
2.10.6 Default privacy setting on Twitter	40
2.10.7 LinkedIn privacy setting	41
2.10.8 Instagram privacy setting	42
2.10.9 Privacy policy of social networking sites	43
2.11 Factors influencing identity theft in social networking sites (SNSs)	46
2.12 Factor influencing privacy protection in social media	48
2.12.1 Perceived awareness	48

2.12.2	Perceived training	50
2.12.3	Intention to use security and privacy protection measures.	52
2.12.4	Perceived values	53
2.12.5	Attitude towards sharing	55
2.13	Security and privacy threats on social networking sites	56
2.13.1	Multimedia content threats	58
2.13.2	Traditional threats	63
2.13.3	Social threats	66
2.14	Privacy concerns on social media	67
2.15	Security and privacy in social networking sites (SNSs)	70
2.16	Default privacy settings on Facebook	77
2.17	Events of social networking sites users being affected	79
2.18	Security and privacy issues in social networking sites (SNSs)	80
2.19	Security and privacy features in social networking sites (SNSs)	82
2.20	Comprehensive approach in making the users use privacy measures	85
2.21	Theoretical model	85
2.21.1	Protection Motivation Theory (PMT)	87
2.21.2	Technology Acceptance Model (TAM)	90
2.21.3	Theory of Reasoned Action(TRA)	93
2.22	Hypotheses and research model	95
2.22.1	Awareness and training	95
2.22.2	Protection motivation theory	96
2.22.3	Technology acceptance model	96
2.22.4	Theory of reasoned action	96
2.22.5	Summary of the hypotheses	96
2.23	Chapter Summary	97

CHAPTER 3 METHODOLOGY 100

3.1	Introduction	100
3.2	Operational definitions	101
3.3	Research design	102
3.4	Theoretical framework	107
3.5	Conceptual framework	114
3.6	Dependent variable	117
3.7	Independent variables	117
3.8	Population and sampling technique	117
3.8.1	Target population	117
3.8.2	Stratified random sampling technique	118
3.8.3	Determining sample size	119
3.9	Data collection	121
3.10	Development of instrument: survey questionnaire	122
3.11	Data analysis	126
3.12	Reliability & validity	127
3.12.1	Reliability	128
3.12.2	Validity	129
3.13	Pilot study	131
3.14	Pre-analysis data screening	132
3.15	Formats for presenting findings	133
3.16	Resource requirements	133
3.17	Chapter Summary	133

CHAPTER 4 RESULTS	135
4.1 Introduction	135
4.2 Pre-analysis data screening	135
4.3 Number of participants and response rates	136
4.4 Demographic data of participants	137
4.5 Descriptive analysis of student's level awareness	139
4.6 Descriptive analysis of gender difference	140
4.7 Descriptive analysis of privacy protection measures	141
4.8 Descriptive analysis of perceived training	142
4.9 Descriptive analysis of severity attack	143
4.10 Descriptive analysis of perceived benefit	143
4.11 Descriptive analysis of perceived value	144
4.12 Descriptive analysis of attitude toward share	145
4.13 Descriptive of students' intention to use privacy settings	146
4.14 Structural equation modeling	148
4.15 Measurement model testing	149
4.15.1 Reliability and validity	150
4.15.2 Common method bias	153
4.15.3 Structural model testing	157
4.15.4 Evaluation of structural model	162
4.16 Chapter summary	164
CHAPTER 5 CONCLUSIONS, IMPLICATIONS, AND SUMMARY	165
5.1 Introduction	165
5.2 Conclusion of research	165
5.3 Contributions to the theory and practice	168
5.4 Training framework	171
5.5 Strength of the study	172
5.6 Limitations of study	173
5.7 Implications of study	174
5.8 Recommendations for future research	175
REFERENCES	178
APPENDICES	194
APPENDIX A	194

LIST OF TABLES

Table	Page
1.1 Problem Statements, Research Objectives & Questions	12
2.1 Facebook features and default privacy settings	39
2.2 Default privacy setting on Twitter	41
3.1 Types of research design	104
3.2 Possible justifications for the sample size	121
3.3 Survey Questionnaire	124
3.4 Reliability and Validity	127
3.5 Types of reliability and purposes	129
3.6 Types of validity	131
4.1 Profile of the respondents	138
4.2 Level of awareness	140
4.3 Gender different	141
4.4 Perceived Training	142
4.5 Severity Attack	143
4.6 Perceived Benefit	144
4.7 Perceived Value	145
4.8 Attitude Towards Sharing	146
4.9 Perceived Value	147
4.10 Reliability and validity	151
4.11 Discriminant validity	153
4.12 Common Method bias analysis	154
4.13 Structure Model	159
4.14 Summary of support for hypotheses	162

4.15	Goodness model fit	163
5.1	Training, Awareness, and Intention Use	172

LIST OF FIGURES

Figure	Page
2.1 Facebook Privacy Settings	36
2.2 Twitter Privacy Setting	40
2.3 LinkedIn Privacy Setting	42
2.4 Security and login	74
2.5 Privacy Settings and Tools	76
2.6 Facebook privacy change strategy	78
2.7 Core and Full Nomologies in Context of PMT	89
2.8 Technology Acceptance Model	92
2.9 The relationship between attitude, subjective norm, and behavior	94
2.10 Conceptual Framework	97
3.1 Research Design	106
3.2 Overview of PMT's Core and Complete Nomologies	108
3.3 Technology Acceptance Model	110
3.4 Attitude, subjective norm and behavioral	113
3.5 Overview of Conceptual framework	115
3.6 Detail of proposed conceptual model	116
4.1 Measurement model	157
4.3 Structural Model	160

LIST OF ABBREVIATIONS

SNSs	Social Networking Sites
OSN	Online Social Networking
PII	Personally, Identifiable Information
NIST	National Institute of Standards and Technology
ASA	Advertising Standards Authority
HTML	Hyper Text Markup Language
HTTPS	Hyper Text Transfer Protocol Security
SMS	Social Media Services
SE	Self-Esteem
ICT	Information Communication Technology
URL	Uniform Resource Locator
LS	Life Satisfaction
SPSS	Statistical Package for Social Science
PMT	Protection Motivation Theory
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
SEM	Structured Equation Modeling
TRA	Theory of Reasoned Action
HEI	Higher Education Institutions
IV	Independent Variable
DV	Dependent Variable
PS	Problem statement
CEO	Chief Executive Officer

CHAPTER 1

INTRODUCTION

1.1 Introduction

Social networking sites (SNSs) play an important role in people's communication and sharing of ideas in today's world village. Thanks to the internet which is the global largest social media under web 2.0. According to a new study, People throughout the world have similar major motivations for utilizing social media, however, these motivations may be weighted differently in different cultures. In other words, discrepancies in social media adoption between cultures are caused by factors such as demographic characteristics, cultural values, and network connection type. Individuals use social networking sites (SNSs) for different reasons such as business marketing, political campaigns, and academic purpose through their devices(Salehan et al., 2018). This chapter briefly discussed the background of the study, problem statement, research aims, research questions, justification and significance, scope and limitations, chapter arrangement, and chapter summary.

1.2 Background of the study

In 2002 in Somalia especially in Mogadishu, people started using the internet for general purposes such as research and sending emails with their counterparts. In 2003 people started using instant messaging like MSN, but today SNSs (Social Networking Sites) are quickly gaining popularity as a way of both interpersonal and public communication in Somalia, especially in Mogadishu(Jeilani, 2021). The research in this area depicts the evolution of social networking sites, as well as the fundamental concepts of social media security and privacy. There are many purposes because individuals utilized internet services to get news, shop online, watch TV channels, navigate using maps, and communicate with others using social networking sites

(SNSs). Individuals are spending time on Social Networking Sites (SNSs) like Twitter, Google+, Facebook, YouTube, WhatsApp, Snapchat, and LinkedIn(Alaslani & Alandejani, 2020). WhatsApp and Facebook are common social networking sites (SNSs) for communication among all individuals in Somalia, and most undergraduate students use social networking sites (SNSs) at Mogadishu - University especially Facebook and WhatsApp. In December 2020, Mark Zuckerberg said Facebook had over 2.8 billion active members worldwide(Sproutsocial, 2021).

Individuals who use social media are concerned about the security and privacy of social networking sites (SNSs), as there has been a rise in harassment of social media users recently. The online Oxford English Dictionary describes the term privacy refers to a condition of being free from being noticed or disturbed by others. Data integrity refers to the fact that user data has not been altered and is identical to the original data. A man-in-the-middle attack is a common type of data integrity assault. During a man-in-the-middle, the data transmitted can be interrupted and manipulated by hackers. Whereas the appropriate use of security and privacy settings on social media can be prevented users' data misuse. To put it another way, merchants, businesses, and third parties should only use the information provided to them for legitimate purposes. Information privacy is another term for data privacy. Data privacy applies information technology to decide what data of individuals or Social Networking Sites (SNSs) can be shared with third parties. Awareness of how to change the security and privacy settings in social media plays a vital part in ensuring their privacy is protected(Sim, 2010). When uploading personal information online, one should examine the risks involved and not rely solely on the website's privacy controls; there is always the risk of human error, which can result in data leaking. This error might occur either on the part of the service provider or on the part of the individual. Furthermore, not every online service should

be trusted. For example, third-party developers have produced a large number of Facebook applications for various reasons. When attempting to use any of them, Facebook openly tells users about the information they can collect; if a user agrees, he or she can use the app, but his/her personal information will be available to it. Users should be wary of apps and should not trust anything until they are aware of the third-reliability parties (Leaver, 2013).

Several factors affect the security and privacy protection of social networking sites attitude, behavior, subjective norm, belief, intentional and unintentional, personality, the severity of the attack, perceived vulnerability, perceived response efficacy, reward, trust, and personal experience. Currás-Pérez, Ruiz-Mafé, & Sanz-Blas (2013) assert that the importance of attitude in enhancing pleasure and loyalty to social networking sites cannot be overstated. Users' attitudes toward social networking sites are largely determined by sociability and entertainment gratifications, as well as perceived risks (psychological, time loss, and social). Maier, Laumer, Eckhardt, & Weitzel, (2015) Assert that Users' emotions of tiredness from social networking sites (SNSs), low levels of user happiness, and a strong desire to minimize or even stop using social networking sites are all psychological and behavioral effects of social overload. According to Pornsakulvanich (2017) Personality qualities, perceived usefulness, perceived ease of use, perceived enjoyment, attitude toward utilizing social networking sites (SNSs), social influence, and use of social networking sites (SNSs) all played a role in online social support satisfaction and frequency. Salleh et al. (2013) Although much has been published on information privacy and privacy leakage on social media sites, few have used the Protection Motivation Theory (PMT) as a framework to investigate users' information disclosure behavior on social networking sites (SNSs). The privacy of users' data has become a significant challenge (Mousavizadeh & Kim, 2015). Not only

for users of social networking sites (SNSs) but also for governing organizations, protecting users' exposed information has become a big concern. In a study focused on social networking site (SNSs) users' protection from privacy breaches caused by or facilitated by SNS providers, the impact of privacy assurance mechanisms on social networking sites (SNSs) users' privacy-preserving actions is studied (Mousavi, Chen, Kim, & Chen, 2020). Data protection requires more than just security and privacy; software must also be dependable. Normally, security, privacy, and dependability are dealt with separately. (Hatzivasilis, Papaefstathiou, & Manifavas, 2016).

Zlatolas, Welzer, Heričko, & Hölbl(2015) conducted a study of a theory that encompasses privacy awareness, privacy social norms, privacy policy, privacy control, privacy value, privacy concerns, and self-disclosure was created to gain a better understanding of how privacy issues influence self-disclosure. Social networking site service providers are encouraged to create easy-to-understand privacy indices that indicate to consumers what amount of privacy protection they have(Cheung et al., 2015)

Eid & Al-Jabra(2016) claimed that talking and online conversation, file sharing and knowledge sharing, and student learning, as well as pleasure and satisfaction, have strong beneficial relationships. Their research also looks at the many aspects of users' information-sharing behavior on Social Networking Sites (SNS) and the factors that influence such behavior. Their research looked at two aspects of information sharing: sharing regularity and sharing density. Sharing regularity is a depth feature of sharing behavior that relates to the frequency with which people share personal information with others on social networking sites (SNSs). Sharing density deals with the degree of personal information sharing with others (Salehan, Kim, & Koo, 2018). The findings imply that when users opt to share personal information on social networking sites, they

focus on the benefits as well as the social influence, but they pay less attention to the potential privacy hazards. Educators are encouraged to start instructional programs to improve student understanding of the dangers of self-disclosure on social media networks.

Presently, most of the studies regarding integrity and privacy on Social Networking Sites(SNSs)have been conducted in developed countries(Al-qurishi et al., 2017; Aldhafferi et al., 2013; Menard et al., 2017; Nur Fadzilah Othman1, Rabiah Ahmad1, 2013; Pornsakulvanich, 2017; Saleh Zolait et al., 2014). Investigations of the security and privacy of Social Networking Sites (SNSs) in different settings are necessary to determine their effect on users' attitudes toward using social media. Therefore, it is significant to explore the factors influencing students' intention to use security and privacy protection options on social networking sites (SNSs). In the context of perceived awareness, training, and intention in Somalia.

1.3 Problem statement

Although social networking services (SNS) have several security safeguards, they cannot guarantee that one's privacy is completely protected(Saridakis et al., 2016). One of the most pressing concerns about people's behavior on social networking sites (SNSs) is their privacy(David Hiatt and Young B. Choi, 2016). Through viruses and worms, new malicious encryption is discovered every day. The majority of users are unaware of the importance of applying patches and updating consistently (Bradley, 2012).

The challenges discussed in this study are to investigate the factors influencing students' intention to use security and privacy protection measures on social networking sites these predictors are: training, awareness, intention, attitude, severity

attack, value, and perceived benefits. Based on the prior literature on these variables linkages have deserted the following aspects that form the research problems or gap analyses.

PS1 - Lack of awareness of the users on security and privacy settings provided by social networking site providers caused users to be exposed to cyber security attacks.

The challenges such as the rapid growth of social networking sites, changes in the individual users of this social media, and also increases in the number of victims using these social networking sites. User awareness and user knowledge have a strong influence on user attitudes to behave securely when using such social media (Saleh Zolait et al., 2014). Users' status updates, photographs, and information are likewise protected by privacy settings on online social networking sites (OSNs). However, issues arise when users are unaware of and fail to use the privacy options provided by social media platforms. As a preferred method of controlling and addressing their privacy concerns, the awareness appears to rely on their ability to manage the information they publish. Privacy must be considered when using social networking services. Especially when sensitive and often private information about users may be sold to third parties without their knowledge or consent (Zurbriggen et al., 2016). Facebook users are unaware of their privacy options, which should be used to warn them about the dangers of giving out sensitive information such as cell phone numbers and images to strangers. A study conducted by (Whitney & Cummings, 2020) related to the user's knowledge of their profile to check if they changed the quantity of information they provided and/or who they shared it with. If users modified their profiles, it suggests that users are unconcerned about safeguarding the information they give out about themselves. If users' profiles stayed untouched, it implies that users are unconcerned about protecting the information they give out about themselves.

PS2 – Lack of training on security and privacy protection measures on social networking sites caused users to be vulnerable to cyber security attacks.:

The field of social networking sites has gradually recognized the importance of the role users play to protect one's privacy and change the default setting of their accounts. Users' recognized the importance of privacy protection brings to stay connected on social media. Because the majority of users access the Internet via their mobile phones, privacy settings that are compatible with mobile phones must be established and offered video clips on how to manage privacy settings(Aldhaffer et al., 2013). The majority of these devices and applications are not designed to handle security and privacy attacks, which leads to a slew of security and privacy issues in social networking sites (SNSs), including confidentiality, authentication, data integrity, access control, and secrecy. As a result, training is critical when using any device or application.(Abdi et al., 2019; Abdur et al., 2017). Highlighting that all information sent through social media should be considered insecure, and that sensitive information should not be sent over social media. Customizing users' privacy has a favorable impact on their safety(Mousavi et al., 2020). When using social networking sites, self-disclosure refers to the purposeful and voluntary release of personal information(Mousavi et al., 2020). Users of social media believe that convenience is paramount. Users have no qualms about disclosing personal information as part of their profile. The extent to which personally identifiable information (PII) has been disseminated is unknown to the users. One source of this perplexity is the way social media platforms offer account settings. The purpose is for friends to profit from personally identifiable information (PII) such as address and date of birth. Users assume that their friends are already aware of the PII and that they are providing information that solely benefits their circle of friends. (Report, 2021). Training is one of the best methods for protecting users' data privacy in social media.

Nevertheless, perceived training refers to users' ability to use social media, with a focus on privacy and security settings. (Johani, 2016).

PS3 – Lack of comprehensive approach in making students use the security and privacy measures in Social Networking Sites(SNSs):

Previous studies conducted have proven significant in making users use security and privacy settings on social media(Aghasian et al., 2017; Bender et al., 2017; Bertino & Ferrari, 2018; Lax et al., 2021; López-Vizcaíno et al., 2021; Rathore, Sharma, et al., 2017; Wisniewski et al., 2017). In a study conducted by Squicciarini et al. (2014) Security and privacy protection measures should accomplish two main goals: (1) they should allow social media users to safely share personal data with others without being burdened by tedious policy specification tasks, and (2) they should create privacy settings that are consistent with users' preferences in the long run. Because social networking sites (SNSs) let users store vast amounts of personal data on their boards, security and privacy precautions are becoming more important. For the usual user, who has hundreds of contacts and maintains an extensive profile on his or her primary social networking sites, the procedure of selecting privacy preferences may be onerous, time-consuming, and complex (SNSs)(Squicciarini et al., 2014). According to Rathore et al.(2017), cyber security threats are divided into three categories. The first section focuses on multimedia content threats, in which multimedia material posted on Social Networking Sites (SNSs) is exploited to expose SNSs users. The second part includes traditional threats in which traditional attack techniques or vulnerabilities are used to expose Social Networking Site (SNSs) infrastructure used to attack Social Networking Site (SNSs) users. The third part covers social threats in which attackers begin a social relationship with Social Networking Site (SNSs) users to endanger them. The intention is the core element of social networking sites(SNSs) and refers to individuals' readiness

to perform a given behavior and ethical dilemmas(Jafarkarimi et al., 2016). Awareness and intention play important to the users to be a safeguard regarding social media(Seo & Park, 2020).

Social networking services are used in most public areas, colleges, and residences in Somalia special the capital city Mogadishu. Some universities have made it illegal to utilize social media platforms. Many studies in industrialized countries show that social networking sites help people improve their technical abilities, social skills, and learning opportunities(Aarssen & Crimi, L.,2016;queensu.ca et al., 2017; Torten et al., 2018; Xu et al., 2019; Zurbriggen et al., 2016). Privacy issues in social media become a contentious subject for both providers and consumers(Aldhaffer et al., 2013) Today, there is little or no study being conducted in impoverished nations such as Somalia, and there is also little discussion about safety and security on social networking sites.

1.4 Research objectives

The primary goal of this study is to improve students' intention to use security and privacy protection measures in social networking sites (SNSs) through successful security and privacy awareness campaign. Four sub-objectives were investigated to accomplish the main objective of the study. The sub-objectives of this study are: -

- i. To investigate the level of students' awareness of security and privacy settings offered by social networking site providers.
- ii. To examine the effect of perceived training, value, attitude towards share, perceived benefit, and perceived severity attack on students' intention to use security and privacy protection measures in social networking sites (SNSs).