PRIVACY AND SECURITY ISSUES IN SOCIAL NETWORKING SITES (SNS)

Naresh Khatri[1], Sunil Paudel[2]

[1]Department of Electrical Engineering, Khwopa College of Engineering, Bhaktapur, Nepal
[2]Post Graduate Department, Himalayan Institute of Science and Technology, Kathmandu, Nepal

Abstract

Social Networking Sites (SNS) have become very fashionable during the past decade, as they permit users to both express their personal feelings and meet friends, relatives, and people with similar interests. There are many potential threats to data privacy and security like fraud, identity theft, and disclosure of sensitive information. Many users are still not conscious of these threats. Moreover, the privacy settings provided by SNSs aren't flexible and reliable enough to protect user data. Users don't have any control over what others reveal about them. We conducted a preliminary study among internet users of Nepal which examines the privacy and security issues in SNSs because the users share their information and put varieties of data on SNSs. This study intends to protect the user information from any misuse, to make sure of data security, and to permit users to choose what information to share and with whom. Another objective of this study is to measure the level of steps taken by the SNS operators. We identified privacy and security issues in SNS and propose a Privacy and Security Framework as a foundation to deal with these problems.

Keywords: Social Networking Sites (SNS), Privacy and security issues

1. Introduction

The emergence of web technology has also increased a lot of online social activities, including instant messaging, blogs, newsgroups, and forums. The online community that has obtained dramatic popularity in the past few years is the social networking sites (SNS). Introduced in the late 1990s, SNSs have attracted billions of users around the world (Jahan & Ahmed, 2012).

ITU published data at the end of 2019 stating that 53.6 percent of the worldwide population, that is 4.1 billion people, are using the internet (International Telecommunication Union, 2020). Internet penetration within Nepal has reached 72.42 percent. There are 21,373,328 internet subscribers as of March 2020, according to the Management Information Systems (MIS) report published by Nepal Telecommunications Authority (Nepal Telecommunication Authority, 2020). Daily time spent on Social Networks rises to over 2 Hours (Mander, 2017).

Social networking has brought revolution to social life and is continuously gaining popularity among the web users. Through online social media, a large range of digital contents, such as blogging, vlogging, reviews, question-answer databases, digital video, mobile photography etc have been produced by users and have dramatically changed the way people work and interact. However, the simplicity of making such digital content online has also led to an increase in users' concern about the reliability of such information (Liu & Sun, 2014).

In the internet era, social networking sites are getting extremely popular. It is because communicating through SNSs is less complicated and cheaper. The expansion in the number of SNS users has led to the rise in data privacy and security issues. Data security and privacy associated with SNSs are fundamentally behavioral issues, not technology issues. The more information someone posts, the more information becomes available for potential threats from those with malicious intentions. People who publish private information, sensitive data or confidential matters about themselves or others, whether wittingly or unwittingly, pose a greater risk to themselves and others. Similarly, posting photos, videos or audio files may lead to an organization's breach of confidentiality or a personal breach of privacy (Faisal et al., 2013).

*Corresponding author: Naresh Khatri
Khwopa College of Engineering, Libali – 8, Bhaktapur
Email: naresh.khatri@khwopa.edu.np
(Received: Aug 30, 2020 Accepted: April 10, 2021)

2. Rationale of Study

The users' privacy and their information security on SNSs is significant to all SNS users. Users display pictures that may compromise personal security, allowing cyber criminals or other groups wishing to do harm. By learning what makes users more sensitive to their account privacy and security and what feelings users currently hold, it will be easier to educate users in a way that will promote user privacy and information security.

There are significant privacy and security related issues that revolve around SNS user account information. Often employers conduct Internet searches on prospective employees. These searches return SNS accounts, where the user's personal life is on display, often including pictures or messages. It is not just job seekers that are affected; beauty queens, trial defendants, and current employees are often punished or fired based on pictures shared online, either on their own accounts or other users'.

Privacy concerns of internet users are important for many reasons. Research on SNS users is important because there can be negative consequences to posting too much information, or the wrong kind of information on their accounts. By understanding what SNS users are thinking, it will be easier to warn them of the dangers.

Cybercrime has also become a threat to personal security and dignity with more people having access to the internet and SNSs. This study is an indicator of where social networking members stand in realizing the risks and even dangers of sharing too much personal information with strangers. The purpose of this research is to determine if users of SNSs are concerned with those risks. We examined the attitudes users of SNSs have toward those risks and what they do to mitigate them. Additionally, we looked at reasons why some users have more concern with privacy and security issues than others. This study is important as SNSs are still a new phenomenon. In the beginning, users did not have many options and many of the websites available today are very similar. The results of this study are of significance to website developers in creating social networking websites and knowing what criteria are important to users on a security and privacy basis. It will also help them to see what kind of users may be attracted by various settings.

Most of the cyber criminals use social networking as a platform taking advantage of privacy and security loopholes in SNSs. So, we carried out the extensive study on the privacy and security issues in social networking sites, proposed a privacy and security framework as a foundation to cope with these issues.

3. Methodology

The overall objective is to examine the privacy and security issues in social networking sites (SNSs). Based on the study, we identified privacy and security problems and proposed a Privacy and Security Framework as a foundation to cope with the privacy and security problems.

It is also important in obtaining relevant primary data from the selected group. From there, an analysis was conducted to study the data obtained from respondents and finally based on the results obtained, a conclusion was derived.

3.1. Study Area

The study area for the research is Nepal, and Nepalese internet subscribers were the targeted audience for the research.

3.2. Data Collection

Data collection for the research is performed by Sampling Method. Sample size for the survey is calculated using an online sample size calculator. The sample size for the survey has been calculated to be 241.

Primary data - Preliminary, the study is based on an online survey that lasted for one month with 241 participants. Primary data is the collection of firsthand information from the target audience (internet subscribers in Nepal). The primary data collection was carried out through following method:

Recruiting methods - Most of the participants of the survey are students and professionals in Nepal. During the survey, there were 241 participants, where 97.9% (236) had at least one SNS account.

Survey design - The survey questionnaire contained fifty-two questions: demographic questions (age, occupation, gender, etc.), SNS usage questions (purposes for joining SNS, profile information, friends, etc.) and privacy and security concern questions such as intellectual copyrights and unauthorized data access.

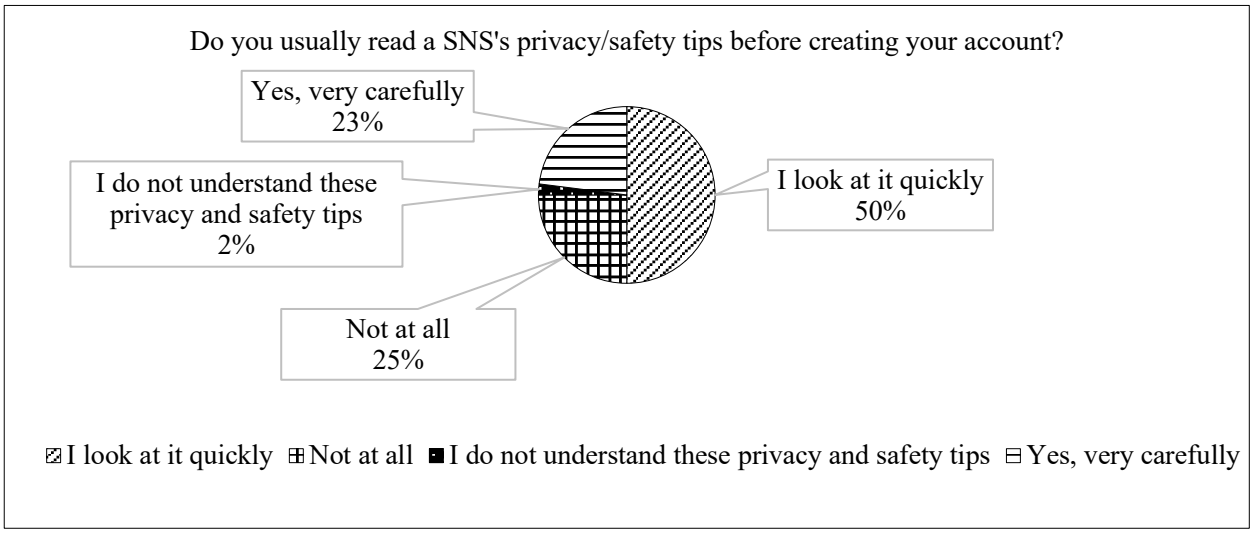

Fig. 1 User response about privacy policy/safety tips reading

Secondary data - Secondary data was collected from review of literature from various sources such as books, book sections, journal articles, articles in periodicals, conference proceedings, reports, web sites, documents from websites, electronic sources, online newspapers, social networking sites (SNS) and so on.

3.3. Data Analysis

The data was analyzed using MS Excel and IBM SPSS. All data was scrutinized to eliminate irrelevant elements. Relevant and useful data was sorted and organized in such a way as to simplify data analysis. Statistical tools were applied in computing results and drawing conclusions.

4. Analysis and Presentation of Data

The data analysis of the responses resulted in several categories. These categories are discussed below:

4.1. Usage of SNSs in Nepal

The result exhibits that a very large majority of respondents i.e. 98% are using some kind of social networking site. This implies that almost all internet users have an SNS Account. The respondents said they use SNSs mainly to get information (70%), to connect with real friends (57%), to be entertained and have fun (39%), to present themselves to the world (34%), to find new friends (25%), to join in to the trend (19%), and other potential aspects. A very low number of respondents (2%) do not use any social-networking sites.

4.2. Right Information on SNSs

Most respondents said that they shared the right information on SNSs. The respondents said that they share e-mail addresses, their own photographs, friend's photographs, date of birth, working place, educational information, hometowns, etc. openly on social networking sites. A significant 93% of people prefer to use their real name in the SNS profile. On the other hand, 23% of respondents said they do not publish their contact information on the internet. However, 21% publish their contact information to all internet users, and 45% make their contact information available only to a selected group of people.

4.3. Privacy Settings on SNSs

The results found that 51% of respondents always use privacy settings to control access to their profile and 38% use privacy settings for important information only. Rest 11% never change privacy settings after creating an account in any SNSs.

4.4. Users' Trust towards Privacy in SNSs

In response to another question about the visibility of users' status updates to all internet users, 28% said that some of their SNS postings were public. They make information that might be sensitive available only to a selected group of people. Another 28% said that all their SNS postings were public and visible to all internet users, and 21% said that their SNS postings were all public but they didn't publish any sensitive information that they didn't want other people to see, and 20% made their SNS posting

protected and visible only to selected group of people. Only a few (2%) users were not sure who could see their messages and 1% users did not publish anything online.

4.5. User Awareness towards Privacy Policy

Half of the respondents said that they look at privacy policy and safety tips quickly before creating their SNS account and 23% said they read them very carefully. Nonetheless, 25% of respondents did not read and 2% said that they did not understand the privacy and safety tips. This implies that majority of users (about 75%) read privacy policy and safety tips as shown in Fig. 1.

5. Privacy and Security Issues in SNS

Security, Profiling, Reputation, and Credibility are some of the areas of privacy risks. Such privacy risks are far more noticeable in SNS than in other internet media like personal websites, blogs, etc. because SNS provide a way of intimacy created by being among online friends. With the motivation to talk and maintain relationships, the number of personal matters revealed willingly by the user is far more than what s/he would have on other websites.

5.1. First Issue

Based on the chi-squared test as shown in Table 1 and Table 2, we concluded that most SNS users (53%) do not know about privacy warnings provided by SNS providers. SNS do not make users aware of the dangers of divulging their personal information.

Table 1: Chi Squared test on SPSS

Does your SNS provider warn you about the risk of divulging your personal information online?

	Observed N	Expected N	Residual
Yes, these warnings are very useful	109	77.0	32.0
I am not sure	91	77.0	14.0
No, I have never seen these warning	31	77.0	- 46.0
Total	231		

5.2. Second Issue

Only 70% of the participants used the spam blocking feature and succeeded, 8% used but didn't succeed. The rest did not know how to block spam or thought that the feature did not work as shown in Fig. 2. So, it can be said that privacy tools in SNS are not flexible enough to protect user data

Table 2: Non-Parametric tests on SPSS

Does your SNS provider warn you about the risk of divulging your personal information online?

		Fq	%	Val-id %	Cumu-lative %
Valid	Yes, these warnings are very useful	109	45.2	47.2	47.2
	I am not sure	91	37.8	39.4	86.6
	No, I have never seen these warning	31	12.9	13.4	100.0
	Total	231	95.9	100.0	
Missing	System	10	4.1		
Total		241	100.0		

5.3. Third Issue

In our survey, only 50% of the participants were concerned that other people might reveal their real identity and personal information online without their consent. Another 50% were still ready to disclose photos and comments of their friends. Users also have no control over third parties. Table 3 shows more than 17% of participants were "Very Much" concerned, 17% were "Much" concerned, more than 26% were "Neutral", more than 23% "Somewhat" concerned, and about 15% "Not at all" concerned that the SNS provider might disclose their information without their consent. Table 4 shows that more than 28% of participants were "Very Much" concerned,

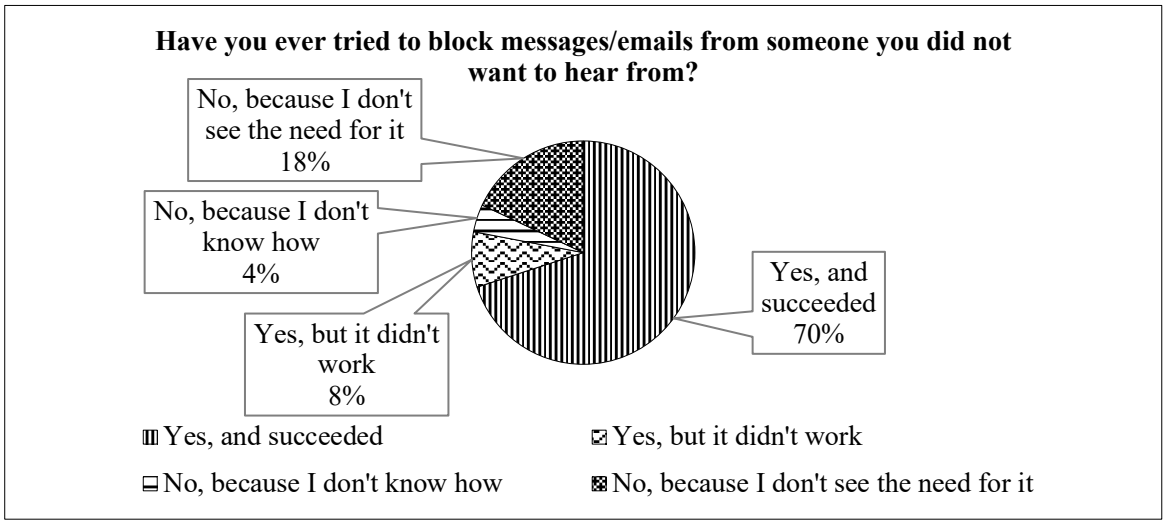

Fig. 2 Participants who used the spam blocking feature

and about 25% were "Much" concerned with online identity theft, profiling, and phishing. Table 5 shows, more than 29% of participants were "Very Much" and 24% were "Much" concerned that their intellectual properties, such as articles, photos and ideas might be copied or abused by others. We can see in Table 6 that 13% people were "Very Much", and 11% were "Much" concerned that the photos shown in their profile might be downloaded and transmitted inappropriately by others and Table 7

displays about 19% respondents were "Very Much" and 24% were "Much" concerned that the information they displayed specifically to someone might be inappropriately forwarded to others.

So, we conclude that the users cannot control what others may reveal about them. Users can control information in their profile but not in their friends' profile.

5.4. Privacy and Security Framework

The role of the Privacy and Security Framework is to provide a foundation for SNS in which privacy and security issues can be addressed. We categorized user data, user privacy concerns, and profile viewers. Based on these categorizations, we adapted the privacy levels and tracking levels to the context of SNS.

5.5. User data

Users list some type of information that they would place on their profile. We categorized user data into five groups: Identity, Demographic profile, Activity, Social Network, and Added content.

5.6. User privacy and information security concern

We perform the K-mean Cluster Analysis on the questions about user privacy concerns. The K-means

Table 3: User concern about divulging information by SNS provider

Are you concerned about divulging information by SNS providers?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	35	14.5	15.3	15.3
	Somewhat	54	22.4	23.6	38.9
	Neutral	61	25.3	26.6	65.5
	Much	39	16.2	17.0	82.5
	Very Much	40	16.6	17.5	100.0
	Total	229	95.0	100.0	
Missing	System	12	5.0		
Total		241	100.0		

Table 4: User concern about online identity theft, profiling or phishing

Are you concerned about online identity theft, profiling or phishing?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	26	10.8	11.4	11.4
	Somewhat	36	14.9	15.7	27.1
	Neutral	44	18.3	19.2	46.3
	Much	58	24.1	25.3	71.6
	Very Much	65	27.0	28.4	100.0
	Total	229	95.0	100.0	
Missing	System	12	5.0		
Total		241	100.0		

Table 5: User concern about intellectual properties

Are you concerned about intellectual properties? (For examples: articles, photos, and ideas)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	31	12.9	13.2	13.2
	Somewhat	30	12.4	12.8	26.1
	Neutral	49	20.3	20.9	47.0
	Much	56	23.2	23.9	70.9
	Very Much	68	28.2	29.1	100.0
	Total	234	97.1	100.0	
Missing	System	7	2.9		
Total		241	100.0		

Table 6: User concern about inappropriate information forward

Are you concerned about inappropriate information forward?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	42	17.4	18.0	18.0
	Somewhat	55	22.8	23.6	41.6
	Neutral	80	33.2	34.3	76.0
	Much	26	10.8	11.2	87.1
	Very Much	30	12.4	12.9	100.0
	Total	233	96.7	100.0	
Missing	System	8	3.3		
Total		241	100.0		

cluster analysis run with k=2 resulted in two user groups with 140 and 82 members respectively. In Table 8, we can see the contributions on each variable to the formation of the groups. Members of Group 1 (63%) considered online privacy a very important factor. In contrast, the members in Group 2 (37%)

Table 7: User concern about inappropriate information download and transmit

Are you concerned about inappropriate information download and transmit?

		Frequency	%	Valid %	Cumulative %
Valid	Not at all	32	13.3	13.6	13.6
	Somewhat	32	13.3	13.6	27.2
	Neutral	70	29.0	29.8	57.0
	Much	56	23.2	23.8	80.9
	Very Much	45	18.7	19.1	100.0
	Total	235	97.5	100.0	
Missing	System	6	2.5		
Total		241	100.0		

Table 8: K-mean clustering (1: not at all, 5: very much)

Final Cluster Centers

	Cluster	
	1	2
Are you concerned that the information you displayed specifically to someone may be inappropriately forwarded to others?	3	2
Are you concerned that the photos shown in your profile may be downloaded and transmitted by others?	4	2
Are you concerned that the people you only know online are not who they say they are?	4	2
Are you concerned that your intellectual properties might be copied or abused by others? (For example: articles, photos, and ideas)	4	2
Are you concerned about online identity theft, profiling or phishing?	4	2
Are you concerned that the SNS provider might divulge your information to other parties without your explicit consent?	4	2
Would you mind spending some time on some processes in order to protect your online privacy?	4	2

No. of cases in each Cluster		
Cluster	1	140.000
	2	82.000
Valid		222.000
Missing		19.000

seemed less concerned about privacy with ratings below average.

Since different users had different privacy concerns for each piece of information, we proposed four Privacy settings for user data according to impact on user privacy: Healthy, Harmless, Harmful, and Poisonous.

Profile Viewers

These four Privacy settings: “Healthy”, “Harmless”, “Harmful”, and “Poisonous” indicated to what extent the information disclosure could cause privacy and security risk to the user. In Table 9, we classified people who could see the user profile into four basic groups: Best Friends, Normal Friends, Casual Friends, and Visitors.

Privacy levels

Based on these four basic groups, we adapted the four levels of privacy into the context of SNS: No Privacy, Soft Privacy, Hard Privacy, and Full Privacy. Table 9 summarizes the access privileges of the four categories of friends to various groups of data, depending on the privacy level.

Tracking levels

We adapted the three Tracking Levels as defined in Aimeur et al. (2008) and Aimeur et al. (2020) for SNS as shown in Table 10.

Strong tracking - The user does not mind being tracked on SNS.

Table 9: Privacy Levels for SNS

	No Privacy	**Soft Privacy**	**Hard Privacy**	**Full Privacy**
Best Friends	All Data	All data	All data	All data
Normal Friends		Harmful, Harmless, and Healthy data	Harmful, Harmless, Healthy data	Healthy data
Casual Friends			Harmless, Healthy data	Healthy data
Visitor		Harmless, Healthy data	Healthy data	No data

Table 10: Tracking Levels

	Strong Tracking	Weak Tracking	No Tracking
Best Friends	Tracking allowed	No tag	No information
Normal Friends			
Casual Friends			
Visitors			

Table 11: Implementation of the Privacy and Security Framework

	SNS User 1 Alpha Socialisers (a minority)	**SNS User 2** Attention Seekers (some)	**SNS User 3** Followers (many)	**SNS User 4** Faithfuls (many)	**SNS User 5** Functionals (a majority)
Number of Friends	Many	Many	Medium	Medium	Several
Principal Types of Friends	Casual Friends	Casual Friends	Normal Friends	Normal Friends	Casual Friends
Spending Times	Usually	Nearly always	Often	Less than often	Occasionally
Data	Lots of Photos. Comments, Tags, Activity	Lots of Photos, Comments, Blog, Tags, Activity	Some photos, Comments, Activity	Some photos, Comments, Activity	n/a
Data Type	Mostly Harmful	Mostly Harmful, Poisonous	Harmless	Harmless	Harmless
Privacy and Security Risks	Security Reputation and Credibility	Security Reputation and Credibility	Reputation and Credibility Profiling	Profiling	Profiling
Proposed Privacy and Security Levels	**Soft Privacy No Tracking**	**Soft Privacy No Tracking**	**Hard Privacy No Tracking**	**Soft Privacy No Tracking**	**Hard Privacy Soft Tracking**

Weak tracking - The user does not mind if his name appears on the Friend list but he does not want his Friends to put a tag on their profile linking to his profile.

No tracking - The user does not want to be mentioned at all in his friends' profile: no name, no tags, and no photo.

6. Implementation of Privacy and Security Framework

A previous study points out five distinct prototypes of SNS users: Alpha Socialisers, Attention Seekers, Followers, Faithfuls, and Functionals (Office of Communication, 2008). A research done in Norway showed five distinct SNS user types: Sporadics, Lurkers, Socialisers, Debaters, and Actives (Brandtzæg & Heim, 2011). Table 11 summarizes these five prototypes, their characteristics, and the proposed privacy levels. Based on the characteristics of each prototype, we can propose to the user an appropriate privacy level. This approach can help the user determine their privacy level and tracking level.

7. Conclusions

There are numerous interactions between SNS users, large amounts of information circulating on the SNS, huge quantities of user data, including personal information, pictures, and videos continue to quickly fall into the hands of the public. The existing solutions are not enough because the problems lie in the foundation of SNS: specifically, the current SNS focuses on interaction and sharing information between users rather than on user privacy. Firstly, we identified three main privacy problems in SNS: lack of user awareness, the current privacy tools were not flexible enough, and users have no control on what others reveal about them. Secondly, we conducted a preliminary study including an online survey to examine the privacy and security issues in SNS. This survey included 241 participants and its results further confirmed the existence of these privacy and security problems. Thirdly, we set up the foundation for privacy and security and introduce a Privacy Framework for SNS. Specifically, since privacy revolves around user data, we categorized user data, user privacy, and security concerns as well as profile viewers into groups. Based on these categorizations, we presented four privacy levels and three tracking.

References

[1] Aimeur, E. A., Brassard, G., Fernandez, J M., Onana, F.S.M. & Rakowski, Z. (2008). Experimental demonstration of a Hybrid Privacy-Preserving Recommender System. *2008 Third Internation Conference on Availablity, Reliability and Security*, (pp.161-170).

[2] Aimeur, E., Hage, H., & Onana, F.S.M. (2008). Anonymous credentials for privacy-preserving E-learning. *2008 International MCETECH Conference on e-Technologies (mcetech 2008)*, (pp.70-80).

[3] Brandtzæg, P. B., & Heim, J. (2011). A typology of social networking sites users. *International Journal of Web Based Communities*, *7*(1), 28–51.

[4] Faisal, A. A., Nisa, B. S., & Ibrahim, J. (2013). Mitigating privacy issues on Facebook by implementing information security awareness with Islamic perspectives. *2013 5th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2013*.

[5] International Telecommunication Union (ITU). (2020). *Statistics*. Retrieved March 31, 2020, from International Telecommunication Union: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[6] Jahan, I., & Ahmed, S. M. Z. (2012). Students' perceptions of academic use of social networking sites: a survey of university students in Bangladesh. *Information Development, 28*(3), 235–247. DOI: 10.1177/0266666911433191

[7] Liu, Y., & Sun, Y. L. (2014). Securing digital reputation in online social media [Applications Corner]. In IEEE Signal Processing Magazine, (Vol. 31), 149–155. Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/MSP.2013.2282414

[8] Mander, J. (2017). *Daily Time Spent on Social Networks Rises to over 2 Hours*. Retrieved March 2020, from GlobalWebIndex (GWI), https://blog.globalwebindex.com/chart-of-the-day/daily-time-spent-on-social-networks/

[9] Nepal Telecommunication Authority (नेपाल दूरसञ्चार प्राधिकरण). (2020). *MIS Reports*. Retrieved March 31, 2020, from Nepal Telecommunication Authority: https://nta.gov.np/en/mis-reports/

[10] Office of Communication (2008). *Social Networking A quantitative and qualitative research report into attitudes, behaviours and use.* Office of Communication (Ofcom). www.ofcom.org.uk.