

Personal Information Threats and Cybersecurity in Online Social Networking Sites: Measuring Attitude and Perception of Educated Youth in District Dera Ismail Khan

Muhammad Junaid¹, Majid Ul Ghafar², Rooh-ul-Amin³

¹MPhil Scholar, Department of Communication & Media Studies, Gomal University, D.I.Khan, Pakistan.

²Associate Professor, Department of Communication & Media Studies, Hazara University Mansehra, Pakistan.

³PhD Scholar, Department of International Relations, Qurtaba University of Science and Technology, Peshawar, Pakistan.

Correspondence: drmajidghafar@hu.edu.pk²

ABSTRACT

Aim of the Study: Social media is an online social networking tool powered by computers that promotes community building and information exchange. Within a well-defined border system, social media users may limit their privacy risks and generate information. The current study aims to gather information about the viewpoints of young individuals with higher education on threats to personal information when they are using different types of social networking sites and the corresponding actions taken in response.

Methodology: A cross-sectional research design entails the collection of data from participants at a certain moment in time. Routine Activity Theory (RAT) was used in this research work as relevancy. The present study used the survey approach to gather data from the Universities in Dera Ismail Khan, Khyber Pakhtunkhwa. A standardized questionnaire was developed to gather data from two distinct institutions in District D.I. Khan. Sample size of the study was consisted on (n=364) respondents studying in the universities.

Findings: A significant proportion of the educated youth in district Dera Ismail Khan, as per the data analyzed that youth have actively engaged with social networking sites and social media applications, an unexpected finding of the study was that majority of the students use social media for business purposes, which indicate the current interest in online earnings and business particularly among the young people.

Conclusion: The present research study concluded that only Facebook users showed significant concerns about their privacy, while users of other social media showed no such concerns. It indicates that for users, Facebook is more vulnerable to cyber threats than other social media platforms.

Keywords: Cybersecurity, Personal Information Threats, Purpose of Media Usage, Social Media Usage.

Article History

Received:
February 11, 2025

Revised:
May 02, 2025

Accepted:
May 05, 2025

Online:
May 07, 2025

1. INTRODUCTION

Social media platforms first appeared at the beginning of the 21st century when the internet was introduced at the end of the previous century. Social media is an online social networking tool powered by computers that promotes community building and information exchange. Within a well-defined border system, social media users may limit their privacy risks and generate information (Safdar, 2023; Tallat et al., 2024; Frederic & Woodrow 2012).

Social networking sites (SNS) on the internet have not only created new channels for human contact, but they have also raised the risks associated with online communication. Data and information security over the internet, especially on social media, is a major worry due to the ease of access to these platforms and the absence of regulating authorities that exist in the case of conventional media. The main drivers of this expansion are the comfort of use, the accessibility of social media platforms, and the degree to which most activities have been ingrained in our everyday lives (Ayub et al., 2024; Irfan 2018; Mao et al. 2020).

The advent of social networking sites (SNSs) has significantly altered the manner in which individuals engage in communication and disseminate information in their everyday routines. Prior to the advent of social networking sites (SNSs), individuals had limited options for communication and information exchange, particularly in terms of engagement. People mostly establish contact with others they were directly acquainted with. Now, users utilize social networking sites (SNSs) as a means to disseminate user-generated material on the internet using computers or smartphones, employing various forms that are contingent upon the specific social network they choose for (Ge, Peng, & Chen, 2014).

The advent of smartphones has facilitated the introduction of mobile application versions and the creation of standalone mobile apps by social networks. This advancement facilitated and enhanced the accessibility of users' online profiles, enabling them to update them with greater frequency and now (Aldhaffer, et al., 2013). Despite this, social networks have become more reachable and user-friendly, individuals tend to share more information (Coyle & Vaughn, 2008) since it is consistently present in their life. Social networking sites (SNSs) undeniably have a significant influence on society, leading to a blurring of boundaries between people's online and offline existence. The interaction between social media and its users is influenced by cyber security and its surrounding environment.

1.1 Statement of the Problem

Millions of people use the internet and social media; thus, security risks and online safety are issues that worry them. Therefore, to avoid the risks and improve the security of online communication, it is important to comprehend the nature of these social media apps and site hazards. The concentration on the risks to users' personal information threats that exist on social networking sites, as well as cyber security, with an emphasis on the attitudes and perspectives of the educated young in the D.I. Khan region is the statement of the problem.

1.2 Objectives of the Study

- To determine the usage frequency of different social media platforms.
- To examine the concerns of people about personal cybersecurity.
- To investigate the awareness towards cybersecurity of personal information.
- To examine the perception towards cybersecurity of personal information.
- To examine the frequency of facing online data theft.
- To determine the privacy concerns of platform users regarding cybersecurity of personal information.

1.3 Hypotheses of the Study

H¹. There is a significant difference in personal cybersecurity of various social media profile status.

H². There is a significant relationship in the use of various social media platforms and their purposes of usage.

H³. There is a significant relationship between demographic characteristics of the students and their level of attitude towards threats to personal information.

H⁴. There is a significant relationship between demographic characteristics of the students and their level of perception towards threats to personal information.

H⁵. There is a significant relationship between social media use and facing threats to cybersecurity of social media accounts.

2. REVIEW OF THE LITERATURE

Online Social networking sites (SNSs) are platforms that provide a user-run online community to connect, communicate, and interact with each other. Social networking site users may interact by sharing personal information, news, videos, photographs, and engaging in real-time chats via chat features (Shin 2010). Boyd and Ellison (2007) describe social networking sites (SNSs) as web-based services and apps that allow users to build a profile inside a specific system that might be public, semi-public, or private. Users may establish A collection of online friends made up of other individuals from the same connection who have similar interests or connections. Each social networking site serves a distinct function, resulting in variations in their characteristics and names across platforms (Boyd & Ellison, 2007).

Students' everyday lives are now deeply impacted by social media, which plays a crucial role in information acquisition, entertainment, socializing, commerce, time organization, and education. The different research studies literature review seeks to examine the many methods by which students use social media, by analyzing a diverse array of scholarly papers and research projects. Many students who are looking for information typically rely on social media as their main source. Previous research states that social media platforms such as Twitter, Facebook, and Wikipedia provide instant access to news and academic materials, enabling students to remain informed about current events and intellectual debates (Kim et al. 2019).

Poushter's research in 2016 emphasized that social media provides a platform for business endeavors. Students could promote their goods or services, interact with clients, and get feedback, which is crucial for the development of their company. In addition, Mangold and Faulds (2009) explored the use of social media as an economical marketing tool for student entrepreneurs, allowing them to expand their reach to a larger audience without requiring substantial financial resources. A widespread trend among students is the use of social media as a method of entertainment and recreation.

Social media platforms change quickly, the biggest problems for platform makers are still security and privacy issues (Rathore et al. 2017). Social media expansion is leading to heightened worries over privacy and security in contemporary society. This is attributed to the increasing elements including accessibility, usefulness, and the extent to which the practice has become a part of our daily lives and routines (Irfan 2018 & Mao et al.2020).

Initially, Teenagers and young adults mostly used online social networking sites like Facebook, WhatsApp, and Twitter to talk to each other. Social networking sites (SNS) had evolved into significant communication platforms for young people across all age categories. Developers must concentrate on addressing the security concerns associated with utilizing social media sites as online networking continues to evolve (Hiatt and Choi, 2016). A Research examining the use of online social networking sites and cybersecurity knowledge among Saudi Arabians revealed that around 70% of those who encountered cybercrime reported the offenses (Alzubaidi 2021).

Social media users freely provide personal information on their accounts to captivate the attention of those who share their interests. These profiles often include details such as name, gender, address, year of birth, phone number, occupation, and many other personal details (Rafique, 2017). According to research carried out in Pakistan by Avais et al. (2014), almost 80% of people provide their personal details, such as phone numbers, ages, residences, and emotional states, to strangers. Furthermore, more than 20% of respondents admitted to disclosing personal information to acquaintances. Nearly half of the participants said they never used nicknames at all, whereas more than half acknowledged using pseudonyms or nicknames online (Avais et al., 2014). A pseudonym, sometimes referred to as a nickname, is a term that is different from a person's true name that they use for a particular reason (Pseudonym, 2013). It's possible that they use these aliases or pseudonyms to conceal their identity online (Avais et al., 2014).

Utilizing the internet and social networking sites always involves risks. The accessibility of the internet facilitates the growing use of social networking sites (Martinez-Ferrer, Moreno, & Musitu, 2018). There is a concept that encompasses various potential attacks, such as character theft, spam attacks, and phishing attacks. These attacks are part of the range of motives that cybercriminals use to target social networking sites (SNS) and end users. These motives include retaliation or emotional distress, monetary gain, news, and even excitement. Many studies emphasize the importance of Users are aware of the hazards of their private, public, and financial details online, as well as knowing how to protect it (Zhang and Gupta 2018).

When using different social media platforms, several people lack awareness about their personal privacy and cybersecurity, typically, people disregard the risks to their privacy, due to the widespread availability of personal and business data on the internet and the ability of social media platforms to grant access to third parties, these parties can exploit the social network by illicitly accessing it, operating phishing attacks for the purpose of stealing personal information, or engaging in other hacking activities (Das, Karmarkar, and Kamrul zaman, 2019). For example, Facebook suffered hacking attacks in 2016 and 2018, revealing the personal information of its fifty million subscribers, while LinkedIn leaked user email addresses in 2012 (Das, Karmarkar, and Kamruzzaman 2019).

2.1 Theoretical Framework

The Routine Activity Theory was first introduced by Cohen and Felson in 1979, and since then, it has been used to explain criminal behavior, deviant behavior, fear of victimization, and criminal victimization (Reyns, 2015).

Marcum (2008) asserts that the routine activity theory (RAT) is useful in understanding the experiences of young individuals in relation to cyber victimization. According to Marcum (2008), the more time individuals spend communicating online and sharing personal information with others, the higher their risk of becoming victims of online threats. The present research does not specifically examine crime, but Marcum (2008) asserts that the Routine Activity Theory (RAT) is efficacious in understanding the experiences of young individuals in relation to cyber victimization. According to Marcum (2008), in the context of the current study analysis and following the principles of RAT, the more time individuals spend communicating online and sharing personal information with others, the higher their risk of becoming victims of online threats. As new technology continuously evolves, society adapts its activity patterns to keep pace with these changes.

This study focused on the target suitability and guardianship aspects of the RAT theory. How the usage pattern (target suitability) of students can lead them toward threats to their personal information on social media platforms. Similarly, how much proper monitoring (guardianship) can reduce that threat.

3. RESEARCH METHODOLOGY

This research utilizes a cross-sectional research approach to collect up-to-date and recently acquired data. The present research is a quantitative study following the positivist philosophical approach and is based on survey research method, which involves collecting, analyzing, and summarizing data to obtain new Information.

3.1 Universe of the Study

The present research study is interrelated to the group of the people in a specific geographical location, i.e. educated youth of district D.I. Khan. The reason for selecting Dera Ismail Khan District, was because this district is located at the crossroad of the three provinces of Pakistan: KPK, Punjab and Baluchistan. People and students of these areas are from all three provinces, particularly from the parts of the provinces adjacent to the district Dera Ismail Khan. This fact increases the significance of the selection of the area of population.

3.2 Unit of Analysis

This study investigates and explores the effects of social networking sites on educated youth. Each individual student studying in the two universities of district Dera Ismail Khan is the unit of analysis for present research.

3.3 Sample

Sample is the subset of population. The researcher was used simple random sampling method for the selection of sample

3.4 Sample Size

Sample size is a number which choose by the research for the purpose to collect the data from the respondent. The sample size of the present research study was taken according to the John curry (1984) 2% formula where the 364 students are the sample size of this research.

3.5 Data Collection

A standardized questionnaire was developed to gather data from two public universities in district D.I. Khan. The questionnaire consisted of closed-ended questions, designed to facilitate easy and accurate responses from the respondents.

3.6 Data Analysis

The researcher used SPSS software for analyzing the collected quantitative data, which used to measure the statistical validity of data and reach the conclusion of the research work.

3.7 Data Tabulation and Analysis

The current study is based on survey research method to investigate and explore the personal information threats & cybersecurity in social media among the educated youth. The data was gathered according to the objectives of the present research from two public universities in district Dera Ismail khan, male and female. The purpose behind the selection of male and female to measure the level of attitude and perceptions regarding online threats to personal information. The collected data was tested by using SPSS software to reach the conclusion.

4. RESULTS

Table 1: Demographic Variable

Category	Value	Responses	Percent
Gender	Male	200	54.9
	Female	164	45.1
Age	18- 22	295	81.0
	23-27	44	12.1
	28 to 32	11	3.0

	More then 32	14	3.8
Education Level	BS	325	89.3
	Master	15	4.1
	MPhil	10	2.7
	Ph.D	14	3.8
Residential Status	Rural	179	49.2
	Urban	185	50.8

N=364

Table one indicated the demographics of the respondents, these demographics include gender, age, educational level and residential area. As for as gender of the respondents is concern table one shows that 54.9% respondents are male, and 45.1% respondents are females. Table one also reveals that 81% of respondents have the age between 18 to 22 followed by 12.1% respondents having the age between 23 to 27, 3% have the age between 28 to 32 and 3.8% respondents have the age more than 32. Table one shows that 89.3% respondents studying in BS level followed by 4.1% in master level, 2.7% M. Phil and 3.8% respondents studying in PhD level. Table one reveals that overall, 50.5 respondents living in Urban areas while 49.2% respondents living in Rural areas.

Table 2: Usage of Social Media Platforms

Category	Value	Responses	Percent
Facebook	Never	113	31.0
	Rarely	54	14.8
	Sometimes	105	28.8
	Frequently	42	11.5
	Very Frequently	50	13.7
WhatsApp	Never	28	7.7
	Rarely	46	12.6
	Sometimes	84	23.1
	Frequently	101	27.7
	Very Frequently	105	28.8
Instagram	Never	101	27.7
	Rarely	57	15.7
	Sometimes	88	24.2
	Frequently	42	11.5
	Very Frequently	76	20.9
Twitter	Never	206	56.6
	Rarely	54	14.8
	Sometimes	35	9.6
	Frequently	35	9.6
	Very Frequently	34	9.3

N=364

Table two indicates the usage of social media platforms by the youth of D.I. Khan. This table reveals that overall, 31% of respondents never use Facebook social media platform followed by 28% respondents sometimes use Facebook and while more than 25% of respondents frequently use Facebook social media platform, and more than 14% respondents rarely use Facebook. Table two also indicates that overall, more

than 56% of respondents use WhatsApp smartphone social networking site followed by more than 23% respondents sometime using WhatsApp and 12.6% respondents rarely use WhatsApp social networking site. Table two indicates that overall, more than 32% of respondents frequently use Instagram smartphone application followed by 24.2% sometime use this application while 27.7% respondents never used this application, and 15.7% respondents rarely used this application. Table two also reveals that 56.6% respondents never used Twitter social media site followed by 18.9% frequently use this social networking site while 14.8% respondents rarely use this social networking site.

Table No 3: Social Media Use for Different Purposes

Category	Value	Responses	Percent
Information			
	Never	48	13.2
	Rarely	27	7.4
	Sometimes	83	22.8
	Frequently	98	26.9
	Very Frequently	108	29.7
Entertainment			
	Never	41	11.3
	Rarely	40	11.0
	Sometimes	111	30.5
	Frequently	82	22.5
	Very Frequently	90	24.7
Education			
	Never	29	8.0
	Rarely	52	14.3
	Sometimes	66	18.1
	Frequently	107	29.4
	Very Frequently	110	30.2
Business			
	Never	158	43.4
	Rarely	40	11.0
	Sometimes	75	20.6
	Frequently	42	11.5
	Very Frequently	49	13.5
Social Interaction			
	Never	101	27.7
	Rarely	64	17.6
	Sometimes	89	24.5
	Frequently	41	11.3
	Very Frequently	69	19.0

N=364

Table three reveals the purpose of using social networking sites for different reasons. Table three reveals that overall, 56.6% of respondents frequently use social networking sites for information followed by 22.8% respondents use social networking sites for information and 13.2% of respondents use social networking sites for information. Table three reveals that 47.2% respondents use social networking sites for entertainment followed by 30.5% sometimes use social networking sites for entertainment and as for as the option of rarely and never is concerned the table three reveals that both options were equally considered and the percentile of the equally frequency was 11%. Table three reveals that 43.4% of respondents never used social networking sites for business purposes followed by 25% using social networking sites for business purposes while 20.6% respondents used social networking sites for business

purposes. Table three reveals that 30.3% of respondents used social networking sites for social interaction followed by 24.5% respondents using social networking sites for interaction purposes and 27.7% respondents never use social networking sites for social interaction and 17.6% respondents rarely use social networking sites for social interaction.

Table No 4: Attitude Regarding Threats to Personal Information

Category				
My browsing information may be collected by third party, When I am online, but I don't take it seriously. By the Respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	126	34.6	34.6	34.6
Disagree	81	22.3	22.3	56.9
Don't Know	60	16.5	16.5	73.4
Agree	76	20.9	20.9	94.2
Strongly Agree	21	5.8	5.8	100.0
Category				
I always feel like someone is monitoring me when I am online. By the Respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	85	23.4	23.4	23.4
Disagree	101	27.7	27.7	51.1
Don't Know	89	24.5	24.5	75.5
Agree	67	18.4	18.4	94.0
Strongly Agree	22	6.0	6.0	100.0
Category				
I remain conscious when sharing something on social media by the Respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	48	13.2	13.2	13.2
Disagree	68	18.7	18.7	31.9
Don't Know	90	24.7	24.7	56.6
Agree	100	27.5	27.5	84.1
Strongly Agree	58	15.9	15.9	100.0
Category				
In social media people can access my online information which is not danger for me by the Respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	72	19.8	19.8	19.8
Disagree	80	22.0	22.0	41.8
Don't Know	81	22.3	22.3	64.0
Agree	95	26.1	26.1	90.1
Strongly Agree	36	9.9	9.9	100.0
Category				
I don't care about my personal information on social media by the Respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	162	44.5	44.5	44.5
Disagree	72	19.8	19.8	64.3
Don't Know	58	15.9	15.9	80.2
Agree	47	12.9	12.9	93.1
Strongly Agree	25	6.9	6.9	100.0
Category				
I don't think that my personal information is leaked through social media by the Respondent				

Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	113	31.0	31.0	31.0
Disagree	63	17.3	17.3	48.4
Don't Know	73	20.1	20.1	68.4
Agree	74	20.3	20.3	88.7
Strongly Agree	41	11.3	11.3	100.0

N=364

Table four reveals about the attitude of the respondents towards threats to personal information. Table five indicates that 34.6% respondents disagree with the statement that my browsing information may be collected by third party, When I am online, but I don't take it seriously followed by 26.7% respondents agree that my browsing information may be collected by third party, When I am online, but I don't take it seriously while 16.5% respondents don't know about it. Table four indicates that 51.1% respondents disagree that they feel like someone is monitoring me when they are online, as for as agree and don't know is concerned the table four reveal that both the option appeared with similar frequency i.e. 24%. Table four reveals that 42.4% respondents agree that they remain conscious when sharing something on social media followed by 31.9% respondents disagree with the statement. Table four indicates that 38.8% respondents disagree social media people can access my online information which is not danger for them while 36% respondents agree that social media people can access my online information which is not danger for them and 22.3% respondents don't know about the statement. Table four reveals that 64.3% respondents disagree with the statement that they don't care about personal information on social networking sites followed by 19.8% respondents agree that they don't care about the personal information on social media 15.9% respondents don't know about the statement. Table four indicates that 48.3% respondents disagree that they don't think that their personal information is leak through social media followed by 31.6% respondents agree with the statement that there is threat of leak of personal information through social media and 20.1% respondents don't know about the statement.

Table No 5: Privacy Concerns of Social Media Users

Category				
It is very important to read the privacy policies when creating social media account by the respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	64	17.6	17.6	17.6
Disagree	40	11.0	11.0	28.6
Don't Know	26	7.1	7.1	35.7
Agree	91	25.0	25.0	60.7
Strongly Agree	143	39.3	39.3	100.0

Category				
It is my responsibility to protect my social media account by the respondent				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	29	8.0	8.0	8.0
Disagree	35	9.6	9.6	17.6
Don't Know	39	10.7	10.7	28.3
Agree	84	23.1	23.1	51.4
Strongly Agree	177	48.6	48.6	100.0

Category				
When the respondent using social media, he/she need to know about media security settings.				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	29	8.0	8.0	8.0
Disagree	32	8.8	8.8	16.8
Don't Know	43	11.8	11.8	28.6

Agree	115	31.6	31.6	60.2
Strongly Agree	145	39.8	39.8	100.0

Category

When the respondent feels someone is using my social media account than he/she will turn on two step verification.

Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	33	9.1	9.1	9.1
Disagree	38	10.4	10.4	19.5
Don't Know	35	9.6	9.6	29.1
Agree	110	30.2	30.2	59.3
Strongly Agree	148	40.7	40.7	100.0

Category

Respondent don't know how to set the two-step verification on social media account.

Value	Responses	Percent	Valid Percent	Cumulative Percent
Strongly Disagree	132	36.3	36.3	36.3
Disagree	55	15.1	15.1	51.4
Don't Know	45	12.4	12.4	63.7
Agree	80	22.0	22.0	85.7
Strongly Agree	52	14.3	14.3	100.0

N=364

Table five reveals about the privacy concerns regarding the use of social media and social media accounts. Above table indicates 64.3% respondents agree that it is very important to read the privacy policies when creating social media account followed by 28.6% respondents disagree with the statement and 7.1% respondents don't know about the privacy concerns. Table five reveal that overall, 71.3% respondents think It is their responsibility to protect their social media account followed by 17.6% respondents disagree that it is not their responsibility to protect their social media account while 10.7% respondent don't know about the statement. The above table shows that 71.4% respondents is of the view that when they are using social media, they need to know about media security settings followed by 16% respondents disagree with the statement while 11.8% respondents don't know about it. Table five shows that 71.4% respondents of the view that when they feel someone is using their social media account than he/she will turn on two step verification followed by 19.9% respondents disagree with the statement and 9.6% respondents don't know about it. The question was asked that respondent don't know how to set the two-step verification on social media account and data table shows that 51.4% respondents disagree with the statement followed by 36.3% agree and 12.4% respondents don't know that how to set the two-step verification on social media account.

Table No 6: Facing threats to cybersecurity on social media profile

Category				
Hack of Account				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Never	242	66.5	66.5	66.5
Rarely	33	9.1	9.1	75.5
Sometimes	54	14.8	14.8	90.4
Often	13	3.6	3.6	94.0
Very Often	22	6.0	6.0	100.0
Category				
Misuse of Name				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Never	216	59.3	59.3	59.3
Rarely	42	11.5	11.5	70.9

Sometimes	64	17.6	17.6	88.5
Often	24	6.6	6.6	95.1
Very Often	18	4.9	4.9	100.0

Category				
Misuse of Mobile Number				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Never	230	63.2	63.2	63.2
Rarely	36	9.9	9.9	73.1
Sometimes	61	16.8	16.8	89.8
Often	17	4.7	4.7	94.5
Very Often	20	5.5	5.5	100.0

Category				
Misuse of Email				
Value	Responses	Percent	Valid Percent	Cumulative Percent
Never	244	67.0	67.0	67.0
Rarely	30	8.2	8.2	75.3
Sometimes	51	14.0	14.0	89.3
Often	15	4.1	4.1	93.4
Very Often	24	6.6	6.6	100.0

N=364

Table five is about users facing threats to cybersecurity on social media. Table five reveals that 66.5% respondents never faced the hacking of social media account followed by 14.8% sometime faced the issue of hacking of account while 9% often and never faced the issue of hacking of social media account with equal percentile. The above table reveals that 59.3% of the respondents is of the view that they never faced the issue of misuse of their name on social media accounts followed by 17.6% respondents faced the issue of misuse of their names and 11.5% respondents often face the problem of misuse of their name on social media accounts. A question was asked about the misuse of mobile number and table five reveals that overall, 63.2% respondents never faced this problem of misuse of mobile number and 16.8% respondents face the misuse of mobile number saved on their social media accounts. Misuse of email is also one of the major concerns of the respondents table five explore that 67% respondents never faced the issue of misuse of email saved on their social media accounts followed by 14% sometime face the issue while 10.7% respondents often face this issue.

5. CONCLUSION

The present research aimed to understand perception and attitudes towards personal information risks on social networking sites of university students in district Dera Ismail Khan, Pakistan. Data was collected through statistical methods and a questionnaire without open-ended questions. The study also aimed to determine the methods used to reduce the impact of these hazards. Demographic parameters such as age, gender, educational level, and residence pattern were also considered. The empirical scrutiny of the research work and its consequent analysis determines that majority of the educated youth use social networking sites and social media applications very frequently for different types of purposes e.g. Information, entertainment, education, timepass, business, social interaction and any others. Educated youth can share their personal information like their age, gender, profile picture, phone number, school information, extracurricular activities, goal and description about themselves frequently and have some privacy concern the present research conclude that only the change in one unit of demographic variable only gender can be different level of attitude and perception regarding threats to personal information.

An unexpected finding of the study was that majority of the students use social media for business purposes, which indicates the current interest in online earnings and business particularly among young people.

This research study included seven hypotheses which were tested using inferential statistics. The findings showed that majority of the hypotheses were partially supported. The findings of this study showed that people having different levels of profile statuses for social media accounts have nearly same concerns about their cyber security. Therefore, it is concluded that profile setting does not reflect on user's concerns about cyber security. These findings did not support the first research hypothesis of the study.

The gist of the study is that gender is an important demographic variable when studying concern about online privacy and threats over social media. One new aspect of the findings of this study was that now a days, young people use social media for business purposes (online earning) compared to other purposes. This indicates that now social media is not just a tool of information and entertainment of social connectivity, but it is growingly becoming platforms for business activities. The findings of this study lend support to the previous literature in the area as well as adding its own unique knowledge about the importance of gender and business purpose while using social media. The study also concluded that government and different organization should launch a proper campaign through different mediums about the cybersecurity and risks involved in using social media without understanding different threats related to personal information.

Acknowledgements

None.

Conflict of Interest


Author declared NO conflict of interest.

Funding Source

The author received NO funding to conduct this study.

ORCID iDs

Muhammad Junaid ¹  <https://orcid.org/0009-0007-6570-0875>

Majid Ul Ghafar ²  <https://orcid.org/0000-0002-0686-8893>

Rooh-ul-Amin ³  <https://orcid.org/0009-0007-0337-6563>

REFERENCES

- Aldhafferi, N., Watson, C., & Sajeev, A. S. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 2(2), 1-17. <https://doi.org/10.5121/ijstpm.2013.2201>
- Alzubaidi, A. (2021). Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia. *Heliyon*, 7(1), e06016. <https://doi.org/10.1016/j.heliyon.2021.e06016>
- Avais, M. A., Wassan, A. A., Narejo, H., & Khan, J. A. (2014). Awareness Regarding Cyber Victimization among Students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, 4(5), 632–641. Retrieved from <https://archive.aessweb.com/index.php/5007/article/view/2662>

- Ayub, U. A., Syed, U. E., Khan, A., & Yaseen, N. (2024). Fear of Missing Out (FOMO), Cyberloafing and Role of Dark Triad in Employees: A Study in the Pakistani Context. *Online Media and Society*, 5(4), 49-68. <https://doi.org/10.71016/oms/0aema451>
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1), 210-230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Das, R., Karmarkar, G., and Kamruzzaman, J. (2019). How Much I Can Rely on You: Measuring Trustworthiness of a Twitter User. *IEEE Transactions on Dependable and Secure Computing*, 18(2), 949-966. DOI: [10.1109/TDSC.2019.2929782](https://doi.org/10.1109/TDSC.2019.2929782)
- Ge, J., Peng, J., & Chen, Z. (2014). Your privacy information are leaking when you surfing on the social networks: A survey of the degree of online self-disclosure (DOSD). *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, 329 - 336. <https://doi.org/10.1109/icci-cc.2014.6921479>
- Hiatt, D., and Choi, Y. B. (2016). Role of Security in Social Networking. *International Journal of Advanced Computer Science and Applications* 7(2), 12–15. <https://doi.org/10.14569/ijacsa.2016.070202>
- Irfan, A., (2018). The History of Social Media. <https://www.socialmediatoday.com/news/the-history-of-social-media>
- Kim, Y., Sohn, D., & Choi, S. M. (2019). The effects of social media on information processing and decision making. *Journal of Communication Research*, 21(3), 345-365.
- Mangold, W. G., & Faulds, D. J. (2009). Social media: The new hybrid element of the promotion mix. *Business Horizons*, 52(4), 357-365. <https://doi.org/10.1016/j.bushor.2009.03.002>
- Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, 2(2), 346-367.
- Martínez-Ferrer, B., Moreno, D., & Musitu, G. (2018). Are adolescents engaged in the problematic use of social networking sites more involved in peer aggression and victimization? *Frontiers in psychology*, 9. <https://doi.org/10.3389/fpsyg.2018.00801>
- Poushter, J. (2016). Social media use continues to rise in developing countries but plateaus across developed ones. Pew Research Center, 22. Available at <https://www.pewresearch.org/global/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/>
- Pseudonym. (2013). In Wikipedia. The Free Encyclopaedia. Retrieved September 28, 2018, from <http://en.wikipedia.org/wiki/Pseudonym>
- Rafique, G. M. (2017). *Personal Information Sharing Behaviour of University Students via Online Social Networks*. Library Philosophy & Practice.
- Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information sciences*, 421, 43-69. <https://doi.org/10.1016/j.ins.2017.08.063>
- Reyns, B. W. (2015). A routine activity perspective on online victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, 22(4), 396-411. DOI: [10.1108/JFC-06-2014-0030](https://doi.org/10.1108/JFC-06-2014-0030)
- Safdar, G. (2023). Digital Challenges: Unraveling the Connection of Cyberbullying and Students' Social Anxiety. *Online Media and Society*, 4(3), 75-85. <https://doi.org/10.71016/oms/tjxqc24>

- Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers*, 22(5), 428-438. <https://doi.org/10.1016/j.intcom.2010.05.001>
- Tallat, F., Saeed, I., & Zia, A. (2024). University Students' Internet Addiction and Cyberstalking: A Moderating Model of Psychological Resilience. *Online Media and Society*, 5(1), 1-11. <https://doi.org/10.71016/oms/554xpb07>
- Zhang, Z., and Gupta, B. B. (2018). Social Media Security and Trustworthiness: Overview and New Direction. *Future Generation Computer Systems* 86, 914–925. <https://doi.org/10.1016/j.future.2016.10.007>