Security and Privacy Issues in Social Networks: A Survey

Dr. Atul Kumar * Corresponding Author
Associate Professor, SRMCEM Lucknow, Uttar Pradesh
atulverma16@gmail.com

Dr. Ashish Baiswar
Associate Professor, SRMCEM Lucknow, Uttar Pradesh
baiswarashish@gmail.com

Mr. Akshay Tiwari
Assistant Professor, SRMCEM Lucknow, Uttar Pradesh
akshay.tiwari92@gmail.com

Ms. Shilpi Khanna
Assistant Professor, SRMCEM Lucknow, Uttar Pradesh
vshilpi.khanna@gmail.com

Ms. Priyanka
Assistant Professor, SRMCEM Lucknow, Uttar Pradesh
priya.3092.singh@gmail.com

Abstract
In this Research, the different conditions of cyber security and its importance have been critically evaluated. It has been identified that 64% of large-sized businesses in the UK are facing cyber security related issues in the year 2021. Data breach-related issues had been confronted by 39% of the charity-related companies in the UK in the year 2021. In addition to this, it has also been identified that malware attacks are the most common cyber security-related issue in the country. Moreover, this research explains the different aspects of cyber security and its importance. However, using only primary quantitative data analysis creates a limitation in this research project. An analysis on the social media security issues has made a significant justification on the criticality of the present challenges in the digital platforms. Identity thefts and breach of personal information can lead to the compromise of business as well as personal accounts. Business compromising often leads towards loss of reputation and loss of revenue. Data collected through primary means are measured via objective analysis through regression testing. Results from the regression test have made significant contribution towards the hypothesis testing.

Keywords: Cybercrime, data breaching, survey, social media, personal information, cyber-attack, financial loss

Tob Regul Sci.™ 2022; 8(1): 259-273
DOI: doi.org/10.18001/TRS.8.1.25

1 Introduction

Security is the main essential in the social media platforms to maintain privacy presentation and images of the people along with different brands. Social media security is required to protect the private data of people in terms of providing digital risk protection to cover security from dark web surface and deep web. Web security is necessary to remember to keep the personal information of the people and pages. Therefore, the security providers are also required to acknowledge the necessary action that they are going to take when the security service is breached by someone.

2 Background

Security systems in social networking sites are essential in maintaining the privacy of the users, such as any brand or any website. As commented by Albladi and Weir (2018), providing the facility to manage security level is able to determine the complexities regarding attacks by the side of operators, whether it is software or a human being. The operator is able to decide on the level of privacy on the social networking sites by why the friendship connections and the privacy settings.

3. Literature Review

Social networking sites regarding security are divided into four parts such as operator, attack, receiver and network. The better the relationship between these four sections, the better the level of security services on the social networking sites. In contrast to this, Polzin *et al.* (2018) have described that by utilising the victims of social media attacks and developing friendship connections and regulating prices settings in the functionality of social network security and privacy preferences are able to be modified by the users.

It is essential to make the native social network secure from the people of the dark web and other hackers. On the other hand, Al-Zoubi *et al.* (2021) have highlighted that in terms of safe browsing on Google, some faced certain features are required to deal with different activities that are associated with 90% accuracy in terms of developing secure networking. The people needed to stay aware of these a few problems which are able to make their citizens and networking site instead of increasing their responsibility. Additionally, Schwartz-Chassidim *et al.* (2020) have argued that measuring the privacy of the users is referred to be concerned with social institutions, government agencies and human resources. The connection between several measurements and aspects of the social media users are required to be developed. This connection is able to help the security service providers to protect the users and provide the ultimate security.

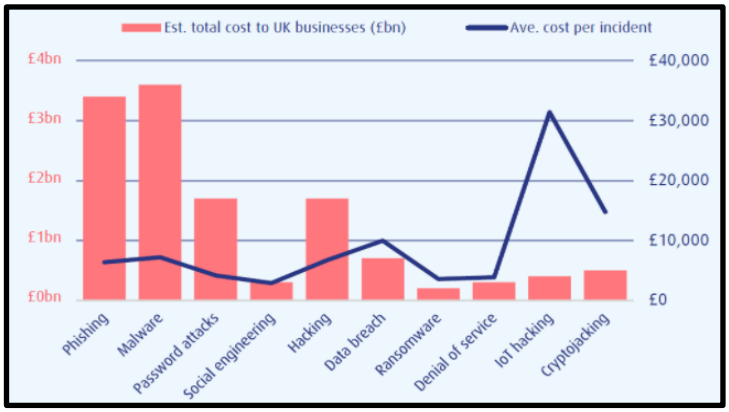


Figure 1. Rate of cybercrime in the UK

(Source: itgovernance.co.uk, 2022)

According to the graphical analysis in the UK, the malware attack has the highest cybercrime-related issue identified (itgovernance.co.uk, 2022). Moderate levels of hacking and password attacks have been identified in the UK, while phishing has a higher rate of conductance (itgovernance.co.uk, 2022). The different kinds of cyber security related issues and attacks from anonymous sources are able to diminish the business performances. Moreover, having personal data and data bridging and personal accounts are able to increase the risk of privacy among the people in the UK. Data breathing-related issues and was a lower level of rate in the UK. According to the government record, 39% of the businesses in the charity sector while 65% of the medium-sized businesses and 64% of the large size businesses have faced attacks of cyber security related issues in the last year (gov.UK, 2022). The increasing rate of cybercrime in businesses is able to reduce the business revenues and affects their business performances.

This research is being conducted in terms of developing a base idea of the importance level of social networks in security for the different websites and people who are using them. The previous research of disregard is associated with developing ideas about the necessity of social networking site security and safety. Moreover, all of those research articles are also providing in this knowledge about the specific security and safety measures either for websites or for the people using social media. In this research project, the importance of safety and security measures for both websites' brands and companies along with triple explained with primary quantitative data analysis.

4. Research objectives

To identify the different roles of cyber security for social networking sites
To describe the importance of maintaining cyber security for businesses
To highlight the importance of cyber security for people
To utilise primary quantitative data analysis techniques for describing the importance of cyber security

5. Research question

What are the different roles of cyber security in social networking?
How is cyber security essential for maintaining online businesses on social media platforms?
What is the role of cyber security in providing safety to people on social networking sites?
How to utilise primary quantitative data analysis techniques for describing the importance of cyber security in social networking?

6. Research methodology

The research has been conducted by following primary research methodology. Ten questions on social media usage have been developed based on research objectives and questions. That questionnaire has been inserted in online Google form to conduct an online survey. Hence the sampling size is 50, and random sampling techniques have been adopted to select the sample respondents so that no biasing can take place in the survey. It has been ensured that the research has followed UK Data Protection Act 2010 and the plagiarism act (Kothari, 2004). The choice of random sampling has allowed the researcher to provide an equal chance to each respondent to get selected. The link of the survey has been sent to social media users through Facebook messenger, and the respondents were requested in messenger to provide a response in that survey.

The deductive approach and exploratory design have been followed in this research. As mentioned by Saunders et al. (2010), the exploratory research design is helpful for primary research to explore the

research context. No data has been directly copied to make the content plagiarism-free. The author of the resources has been acknowledged, and no social media users have been forced to provide a response.

7. The hypothesis of the research

H(1): Social media has enhanced cyber-attack risks such as Cyber bullying, Invasion of privacy, Botnet Attacks, Phishing Attempts for the users

H(0): Social media has no contribution in enhancing cyber-attack risk such as Cyber bullying, Invasion of privacy, Botnet Attacks, Phishing Attempts for the users

H(1); Stealing of personal information, confidential data and business data has been the major threat in the social media network

H(0): Stealing of personal information, confidential data and business data has not been caused by social media network

8. Results

The output from the survey has been statistically analyzed, and SPSS software has been used to make the regression test. The hypothesis of the research has been tested in the data analysis section. A linear regression test has been performed in the SPSS case to make the hypothesis test. Hence in this case, randomly 50 social media users have been chosen; the use of online surveys has been supported to reach the respondents through online mode. Only the social media users have been chosen as respondents. At first, 80 respondents were chosen from social media and from that, ultimately, 50 respondents were selected for this research. As illustrated by Hu (2020), the online survey is the most effective method to reach target customers and collect their responses with a quick approach. On the other hand, an inductive approach supports the research to generate completely new theories based on data analysis and research context. The online survey is done when it becomes impossible to reach each respondent of a medium physically to large sampling size survey.

Regression test

As per the opinion of Stockemer *et al.* (2019), the Sig value of regression output indicates whether the null hypothesis or the alternative hypothesis will be accepted in that test. The sig value between, 0.00 to 0.05, indicates "the null hypothesis will be rejected and alternative hypothesis will be accepted". On the other hand, the Sig value between, 0.05 to 1 indicates "null hypothesis will be accepted, and alternative hypothesis will be rejected". As illustrated by Ong and Puteh (2017), the R squared value represents the "dependency of one dependent value on the independent value". In this case, the R square value "0 to 0.03 indicates poor dependency, 0.3 to 0.5 represent moderate dependency, 0.5 to 0.7 represent good dependency, and 0.7 to 0.9 represent very strong dependency". Hence the correlation between the two independent and dependent factors of the research is defined by the regression test. As mentioned by Sommet and Morselli (2017), the B value in the coefficient table of the regression test measures the exact dependency of the dependent factor.

Hypothesis 1

For the first hypothesis, the dependent factor is security issues in social media. The independent factors are financial risk and stealing personal information. Maximum respondents in the survey have agreed that phishing atoms are the most prevalent attack in social media networks. On the other hand, the

maximum respondents have agreed to that point that "social media brings financial danger for the users and after the invention of social media personal information has been more vulnerable to cyber-attack". In the hypothesis test, the Sig value becomes 0.02, which is less than 0.05. The sig value less than 0.05 indicates that "Social media has enhanced cyber-attack risk such as Cyber bullying, Invasion of privacy, Botnet Attacks, Phishing Attempts for the users" is accepted, and the null hypothesis is rejected. The hypothesis test has been performed by choosing questions 4, 7 and 8 from the questionnaire set and its responses from the excel sheet.

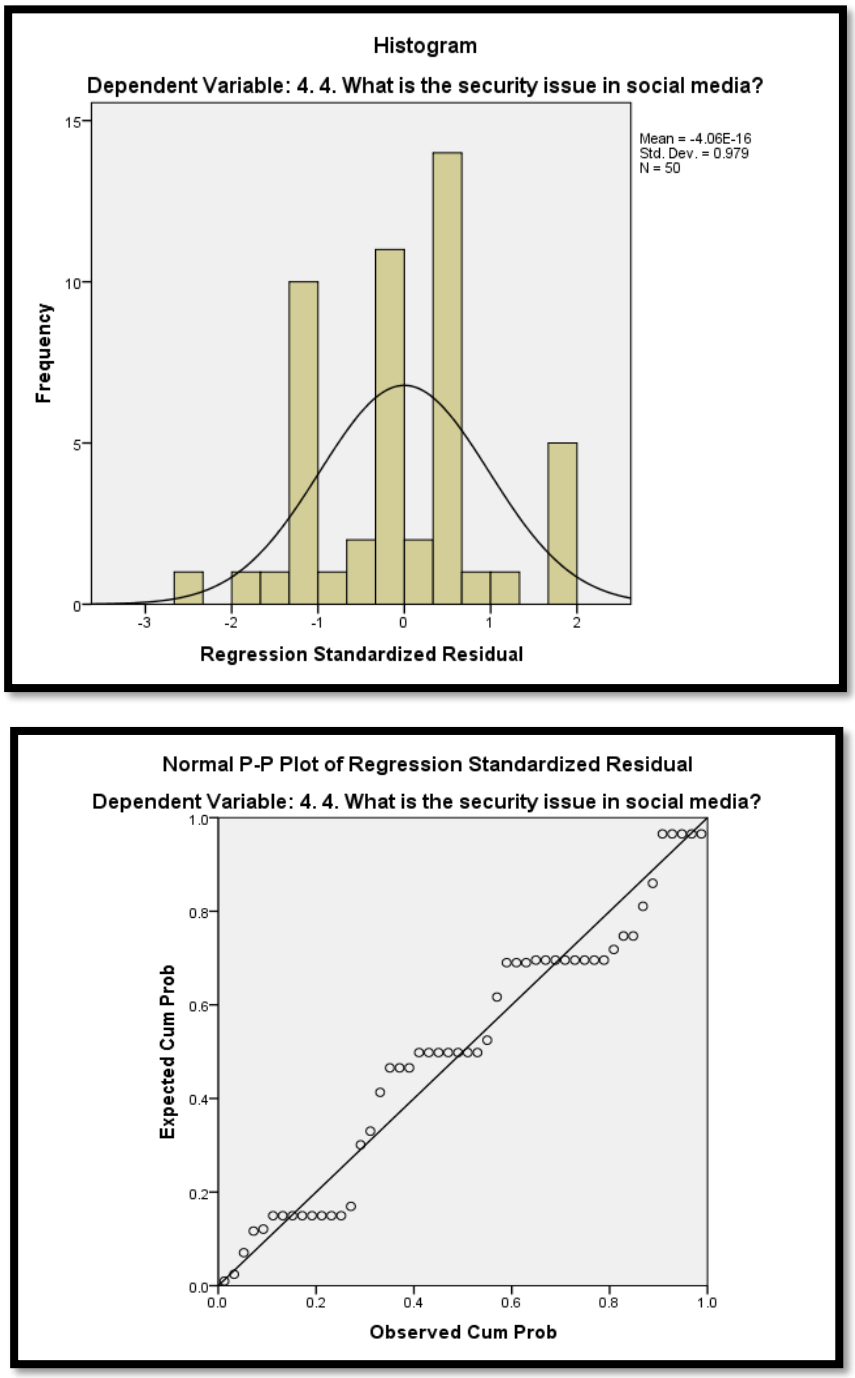


Figure 2: Regression test on hypothesis 1
(Source: SPSS file)

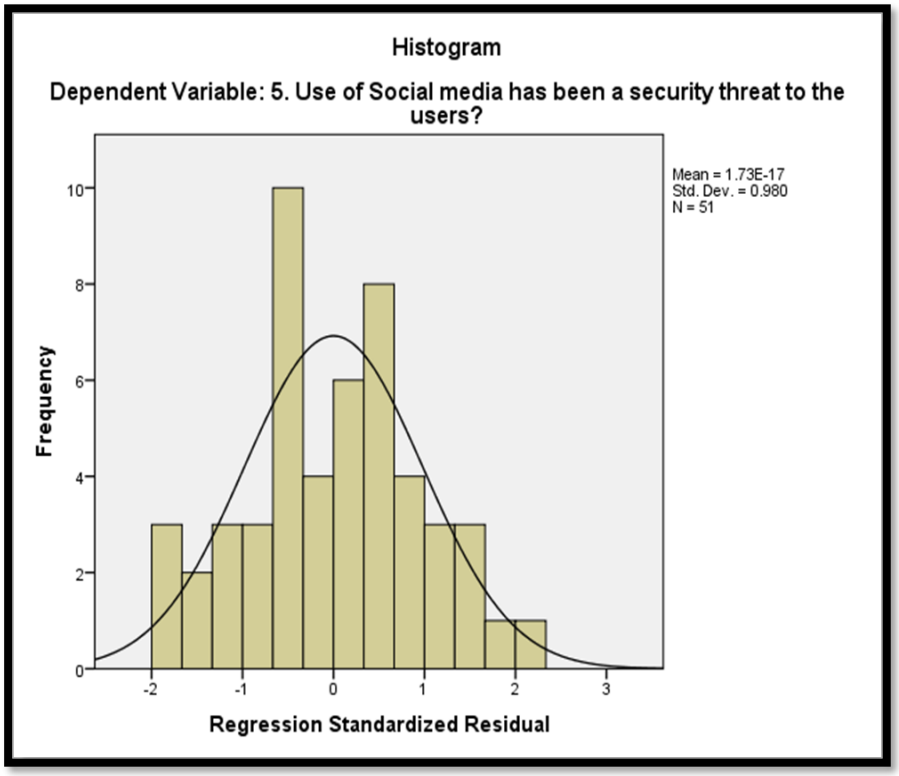
Moreover, in this hypothesis test, the R square value is 0.234. Hence it can be stated that social media use has slightly enhanced the security issue for the users. The users of social media now need to purchase an antivirus plan to protect the personal content in the device from cyber-attacks. However, social media is not the only gateway of cyber attacks, but it has provided more advantages to the hackers to make cyber attacks (Gorwa and Guilbeault, 2020). Hence social media is not the major use of all financial loss and personal information loss due to cyber-attack; but it has enhanced the security risk such as botnet attacks, phishing attacks, and privacy invasion for the users.

In addition, in the coefficient tables, the constant value is 16.75, and the variance values are 0.074 and 0.395. Hence it can be stated that with the change of social media use, the financial risk gets changed at a 0.74 % rate. On the other hand, the leaking of personal information through social media has impacted the security threat of the users with a 0.395% rate. The users fear using social media just because of its security gaps (Giustini *et al.* 2018). On the other hand, if the social media users can use strong passwords and stop the download content from social media or avoid opening any unknown link in social media, the social media attacking issue can be brought under control ***[Refer to appendix 1].***

Correlation test

The Pearson correlation test has been performed to check the correlation between the two variables. As depicted by Zhang and Xia (2017), "more the sig value of correlation will be enhanced more the strong relationship between the two marbles will be indicated". In this case, the correlation value between security issues and facial danger is 0.361, which indicates a moderate correlation. On the other hand, the correlation between personal information loss and social media security is 0.465, which indicates a good correlation ***[Refer to appendix 2]***.

Hypothesis 2



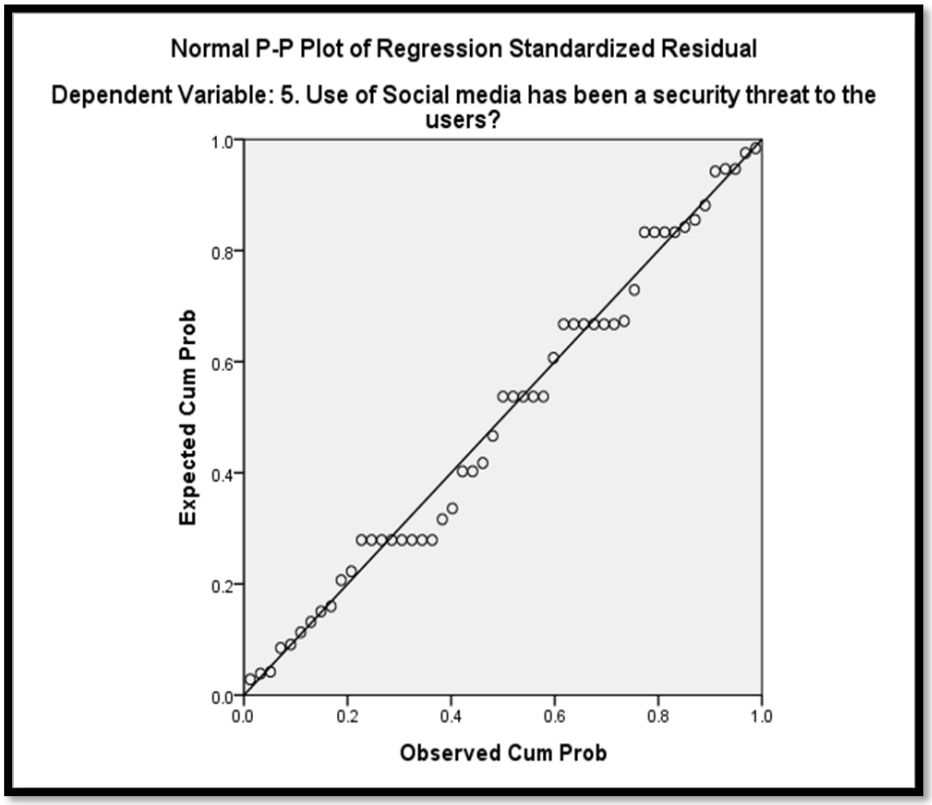


Figure 3: Regression test on hypothesis 2

(Source: SPSS file)

In the hypothesis 2 test, the dependent variable of security threat in social media and the independent variable is Stealing of sensitive data and the risk of personal information hacking. The Sig value of this test is 0.001, and it represents that "Stealing of personal information, confidential data and business data has been the major threat in social media networks' ' is accepted. On the other hand, the R square value in this hypothesis 2 test is 0.260. In this case, also there has been indicated a low dependency among the dependent and independent variables. Hence it can be illustrated that the unsecured use of social media has been a major cause of data loss, hacking of sensitive data and loss of personal information (Ayaburi and Treku, 2020). Moreover, in this case, the constant value is 1.006, and the variance values are 0.195 and 0.432.

Hence with the change of personal information attacks in social media, the security issue in social media will be changed at a 0.195 rate. On the other hand, with the change in security protocol in social media, the change in Stealing sensitive data and obtaining access to business accounts will occur at a 0.432 rate. The histogram plot and normality plot indicates the data set has consistency in its value ***[Refer to appendix 3]***.

9. Discussion

Spending a lot of time and being unaware of the different security purposes of social media is a key factor that increases the cybercrime rate. Therefore, it is able to handle that most of the time, young adults are getting affected by cyber bullying due to their over activities on social media platforms. Cyber bullying is inadequate in terms of the complexities of technology-mediated processes, which are generally suggested among peer groups. As committed by Kofoed and Staksrud (2019), negative actions like physical content and abusive words are used, such as making faces or intentional exclusion from a

group that falls under cyber bullying. It is able to create a threat for the mental as well as physical health of the individual who is facing and going through these painful positions. It has been identified that the rate of people getting affected due to social media platforms is not only limited among young adults. Youtube, Facebook, WhatsApp and Messenger are the most used social media networks in the UK. Social media networks have supported the users to get digitally connected with their closest ones, friends and relatives. The citizen uses social media to "get the news of the world at a fingertip, share information and make connections". Mostly the young generation spends a lot of time on social media platforms, and it's been a major issue in present days (Rogers, 2018). Hacking of personal information, leaking of business information, malware threat, phishing activity are some of the security issues in social media networks.

Social media users faced a hike in cyber attack issues due to the use of social media accounts. The hackers target the social media profile of the account holder, and by hacking the access of social media, they can take control of the device. Hence Social media is getting used as a gateway of stealing the personal information of the users (Stieglitz *et al.* 2018). For instance, the user saves and stores the soft copy of banking documents, confidential data and personal information in the device. As a result, when a social media network hacker attacks the device by accessing the user's social media account, he gets access to that confidential data.

From the above regression test value, it has been seen that maximum participants have agreed their device has been vulnerable to cyber attack, and they always face cyber attack fear just for using social media accounts. The hackers manipulated and misused those data, which has been the cause of financial and safety loss of the users (Ali *et al.* 2018). On the other hand, when a hacker gets access to the device, he can track the OTP sent from the attack to the phone number of the users for withdrawing the money. In this case, the hackers track the password, and without the consent of the bank account holder, they can withdraw the money from the bank account.

On the other hand, due to having a weak password and not using an antivirus plan in the device, the hackers get easy access to hack the personal information from the device (Dencik *et al.* 2018). On the other hand, some users share their location and other information on social media, and it's been the cause of security issues for the users. The hackers target the business profile of the business account holder in social media and try to steal the business information through utilizing the social media account.

10. Conclusion

From the entire discussion, it can be concluded that their increased level of use of social media has increased cyber-attacks. Moreover, stealing personal information and confidential data is creating a major threat in social media networks, invasion of privacy bullying bonnet. Phishing attacks of all users are very common as it is increasing the level of threats in the life of social media users. With the help of the conducted survey, it has been identified that social media users are continuously getting affected due to their continuous sharing of private life on social media platforms.

Sharing personal pieces of information without being aware of different pros and cons are able create a negative interest on the users. With the help of SPSS and appropriate statistical analysis, it has been identified that the users are required to be more aware of the different privacy policies of the social media network. Along with it, due to cyber bullying and other criminal offences with personal information available on social media networking sites, the mental health of the people is getting

affected negatively. Hence, cyber security is essential for the different levels of users of social networking sites.

11. Future scope

This study is creating awareness guidelines for the social media users of different platforms. Perspectives of people regarding cybercrime have also been discussed and critically evaluated with the help of statistical analysis. As a result, this research project has the potential to explore the different aspects of cybercrimes that have been reported by the secondary resources available on different databases. The readers of this research are going to be able to make better discussion of the secondary sources while aligning the secondary and primary data sets altogether. Therefore, this research project is able to help the researcher to develop further studies based on statistical identifications.

12. Limitation

Only primary quantitative data analysis techniques have been instrumental in this research project in terms of identifying the importance of cyber security. Only implementing the primary quantitative data analysis techniques is able to reduce the reliability level of the research work due to the presence of biases in the collected survey.

Reference list

[1]. Albladi, S.M. and Weir, G.R., 2018. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), pp.1-24.

[2]. Ali, S., Islam, N., Rauf, A., Din, I.U., Guizani, M. and Rodrigues, J.J., 2018. Privacy and security issues in online social networks. Future Internet, 10(12), p.114.

[3]. Al-Zoubi, A.M., Alqatawna, J.F., Faris, H. and Hassonah, M.A., 2021. Spam profiles detection on social networks using computational intelligence methods: The effect of the lingual context. *Journal of Information Science*, *47*(1), pp.58-81.

[4]. Ayaburi, E.W. and Treku, D.N., 2020. Effect of penitence on social media trust and privacy concerns: The case of Facebook. International Journal of Information Management, 50, pp.171-181.

[5]. Dencik, L., Hintz, A. and Carey, Z., 2018. Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. New Media & Society, 20(4), pp.1433-1450.

[6]. Giustini, D., Ali, S.M., Fraser, M. and Boulos, M.N.K., 2018. Effective uses of social media in public health and medicine: a systematic review of systematic reviews. Online journal of public health informatics, 10(2).

[7]. Golhar, A. R., Choudhari, N. K., and Patil, A. K. 2021, May. Prediction of aluminium content in a metal using SPSS based linear regression analysis. In Journal of Physics: Conference Series (Vol. 1913, No. 1, p. 012002). IOP Publishing. doi:10.1088/1742-6596/1913/1/012002

[8]. Gorwa, R. and Guilbeault, D., 2020. Unpacking the social media bot: A typology to guide research and policy. Policy & Internet, 12(2), pp.225-248.

[9]. gov.uk, (2022), *Cyber Security Breaches Survey 2021*, available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 [Accessed: 03-March-2022]

[10]. Hu, Z. 2020, August. Based on multiple linear regression analysis of the ability of postgraduate medical students to express SPSS experiment results with three-line table. In Journal of Physics: Conference Series (Vol. 1592, No. 1, p. 012060). IOP Publishing.

[11]. itgovernance.co.uk, (2022), *UK cyber crime rate has doubled in the past five years*, available at: https://www.itgovernance.co.uk/blog/uk-cyber-crime-rate-has-doubled-in-the-past-five-years [Accessed: 03-March-2022]

[12]. Kofoed, J. and Staksrud, E., 2019. 'We always torment different people, so by definition, we are no bullies': The problem of definitions in cyberbullying research. *New Media & Society*, *21*(4), pp.1006-1020.

[13]. Kothari, C.R., 2004. Research methodology: Methods and techniques. New Age International.

[14]. Atul Kumar *et al* 2021. A Comparative Analysis of Pre-Processing Time in Summary of Hindi Language using Stanza and Spacy *IOP Conf. Ser.: Mater. Sci. Eng.* **1110** 012019

[15]. Ong, M. H. A., and Puteh, F. 2017. Quantitative data analysis: Choosing between SPSS, PLS, and AMOS in social science research. International Interdisciplinary Journal of Scientific Research, 3(1), 14-25.

[16]. Polzin, F., Toxopeus, H. and Stam, E., 2018. The wisdom of the crowd in funding: information heterogeneity and social networks of crowdfunders. *Small Business Economics*, *50*(2), pp.251-273.

[17]. Rogers, R., 2018. Digital traces in context| Otherwise engaged: Social media from vanity metrics to critical analytics. International Journal of Communication, 12, p.23.

[18]. Saunders, V., West, R. and Usher, K., 2010.Applying Indigenist research methodologies in health research: Experiences in the borderlands. theaustralian journal of indigenous education, 39(S1), pp.1-7.

[19]. Schwartz-Chassidim, H., Ayalon, O., Mendel, T., Hirschprung, R. and Toch, E., 2020. Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy. *Heliyon*, *6*(2), p.e03298.

[20]. Sommet, N., and Morselli, D. 2017. Keep calm and learn multilevel logistic modeling: A simplified three-step procedure using stata, R, Mplus, and SPSS. International Review of Social Psychology, 30, 203-218.

[21]. Stieglitz, S., Mirbabaie, M., Fromm, J. and Melzer, S., 2018, June. The Adoption of social media analytics for crisis management-Challenges and Opportunities. In ECIS (p. 4).

[22]. Stockemer, D., Stockemer, and Glaeser. 2019. Quantitative methods for the social sciences (Vol. 50, p. 185). Springer International Publishing.

[23]. Zhang, M., and Xia, C. 2017. A loose wavelet nonlinear regression neural network load forecasting model and error analysis based on SPSS. Int. J. Inf. Technol. Comput. Sci.(IJITCS), 9(4), 24-30.

Appendices

Appendix 1: Regression test on Hypothesis 1

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.484[a]	.234	.202	1.043	.234	7.342	2	48	.002

a. Predictors: (Constant), 8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?, 7.7. Do you think that social media brings financial danger for the users?

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15.967	2	7.983	7.342	.002[b]
	Residual	52.190	48	1.087		
	Total	68.157	50			

a. Dependent Variable: 4. 4. What is the security issue in social media?

b. Predictors: (Constant), 8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?, 7.7. Do you think that social media brings financial danger for the users?

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.615	.333		4.853	.000
	7.7. Do you think that social media brings financial danger for the users?	.074	.157	.083	.473	.638
	8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?	.395	.165	.422	2.392	.021

a. Dependent Variable: 4. 4. What is the security issue in social media?

(Source: SPSS file)

Appendix 2: Correlation test on Hypothesis 1

Correlations

		4. 4. What is the security issue in social media?	7.7. Do you think that social media brings financial danger for the users?	8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?
4. 4. What is the security issue in social media?	Pearson Correlation	1	.361**	.465**
	Sig. (2-tailed)		.010	.001
	N	50	50	50
7.7. Do you think that social media brings financial danger for the users?	Pearson Correlation	.361**	1	.688**
	Sig. (2-tailed)	.010		.000
	N	50	50	50
8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?	Pearson Correlation	.465**	.688**	1
	Sig. (2-tailed)	.001	.000	
	N	50	50	50

**. Correlation is significant at the 0.01 level (2-tailed).

(Source: SPSS file)

Appendix 3: Regression test on Hypothesis 2

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.510[a]	.260	.229	1.098	.260	8.415	2	48	.001

a. Predictors: (Constant), 10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media? , 9. Social media has enhanced the risk of personal information hacking throughout the world?

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	20.289	2	10.144	8.415	.001[b]
	Residual	57.868	48	1.206		
	Total	78.157	50			

a. Dependent Variable: 5. Use of Social media has been a security threat to the users?

b. Predictors: (Constant), 10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media? , 9. Social media has enhanced the risk of personal information hacking throughout the world?

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.016	.430		2.362	.022
	9. Social media has enhanced the risk of personal information hacking throughout the world?	.195	.135	.188	1.450	.154
	10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media?	.432	.133	.422	3.252	.002

a. Dependent Variable: 5. Use of Social media has been a security threat to the users?

(Source: SPSS file)

Appendix 4: Correlation test on Hypothesis 2

Correlations

		5. Use of Social media has been a security threat to the users?	9. Social media has enhanced the risk of personal information hacking throughout the world?	10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media?
5. Use of Social media has been a security threat to the users?	Pearson Correlation	1	.290*	.462**
	Sig. (2-tailed)		.041	.001
	N	50	50	50
9. Social media has enhanced the risk of personal information hacking throughout the world?	Pearson Correlation	.290*	1	.268
	Sig. (2-tailed)	.041		.060
	N	50	50	50
10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media?	Pearson Correlation	.462**	.268	1
	Sig. (2-tailed)	.001	.060	
	N	50	50	50

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

(Source: SPSS file)

Appendix 5: Survey question

1. What is your gender?
   Male
   Female
2. What is your age?
   20-30
   30-40
   40-50
3. How much time do you spent time in social media?
   One hour
   More than 3 hour
   More than 5 hour
4. What is the security issue in social media?
   Cyber bullying
   Invasion of privacy
   Botnet Attacks
   Phishing Attempts
5. Use of Social media has been a security threat to the users?
   Strongly agree
   Agree
   Neutral
   Disagree
   Strongly disagree
6. Do you think use of strong password can protect the social media account from hacking?
   Strongly agree
   Agree
   Neutral
   Disagree
   Strongly disagree
7. Do you think that social media brings financial danger for the users?
   Strongly agree
   Agree
   Neutral
   Disagree
   Strongly disagree
8. Do you think after the invention of social media personal information has been more vulnerable to cyber attack?
   Strongly agree
   Agree
   Neutral
   Disagree
   Strongly disagree

9. Social media has enhanced the risk of personal information hacking throughout the world?
   Strongly agree
   Agree
   Neutral
   Disagree
   Strongly disagree
10. Stealing of sensitive data and obtaining access to business account is the negative impact of poor security network in Social media?
    Strongly agree
    Agree
    Neutral
    Disagree
    Strongly disagree