The Role of Social Media Apps and its Cyber Attacks in India

S. Shrilatha [a], K. Aruna [b] and Hepzibah Christinal [b]

[a] *Christian Medical College, Katpadi, Vellore, 632001, India*
[b] *Karunya University, Karunya Nagar, Coimbatore, 641114, India*

Abstract

A cyber-attack is a malicious and deliberate attempt by cyber criminals to breach information against a single or multiple networks using one or more computers. The COVID – 19 pandemic is not only a health issue; it also leads to an increase in cyber-attacks on people who work from home during lockdown. According to a report on lockdown, 40 percent of society appears to be using data, including performing day-to-day tasks such as shopping, banking, watching content, and socializing. This research focuses on India, which has 77 internet users. According to the study's findings, users spend more than 4 hours per day on the internet with their smartphones. They primarily use the internet for entertainment purposes. The majority of respondents have always preferred to use WhatsApp messenger. In addition, respondents are aware of a phishing/hacking attack in the app during the lockdown period. Users strongly agree that the best way to avoid cyber-attacks is to install known/authenticated software on their smartphones/computers/tablets/laptops during the COVID lockdown period.

Keywords

Cyber Attacks, COVID, WhatsApp, Smartphone, Lockdown

1. Introduction

A cyber-attack is a malicious and deliberate attempt by cyber criminals to breach information against a single or multiple networks using one or more computers. By hacking a vulnerable system, a cyber-attack can steal, alter, destroy, or gain unauthorized access to a specific target. It can be part of cyberwarfare or cyberterrorism, and it can be carried out by sovereign states, individuals, groups, societies, organizations, and so on.

The previous study reveals that 99 percent of the business environments are not properly safeguarded from the existence of the various hacks and cyber attacks in the digital platform. The inputs to cyber resistance are the solution for all over the time towards the cyber protection, a mysterious structural design that spread all over the web, ultimate aim (finishing point) and smart phones, and the cloud. By choosing the proper channel in the organization, the management could properly buildup effective measures for security control and strategy as a single person. Teppers, E., Luyckx, K. A., Klimstra, T., Goossens, L. (2014) As a result, events are correlated across overall branches of the business situation, and internet services provided by the various service providers through software for computers and other devices.

The Corona virus has created a great impact towards all over the world on health, economy and life style. Further, it has also increased the cyber-attacks on digital platform, especially people who work from home during lockdown. Nie, N. H. (2001) According to a report on lockdown, 40 percent of society appears to be using data for daily activities like purchasing the products, financing

WCNC-2022: Workshop on Computer Networks and Communications, April 22 – 24, 2022, Chennai, India.
EMAIL: arunasubu75@gmail.com (K. Aruna)
ORCID: 0000-0002-5800-0340 (K. Aruna)


activities, entertainment and social activities. On April 28, 2020, cyber security researchers at the UK-based Sophos has found out that the person hacking are now focusing the individuals across the globe through the false e-mails, web link as Zoom HR and videos like organizing the meetings for salary hike for getting access to their personal details.

As a result, this research focuses on the role of social media apps and cyber-attacks in the digital platform and during the Corona lockdown period.

1.1. Importance of the Study

A cyber-attack is an attempt by cyber criminals to hack into each individual's data via various systems all over the world. Morahan-Martin, J., Schumacher, P. (2003) Cyber attackers' use different plan of action to utilize, duplicate, and destroy many private as well as Government Sector detail in the world of digitalization. In the modern era of digital world, businesspeople have to be vigilant of increasing unprotected environment in terms of cyber threats and its security issues.

1.2. Statement of the Problem

The present literature relating to the cyber-attacks in the automated world and during the COVID-19 lockdown period it has been considerably increased. This study identified the gap by creating an awareness of the various cyber-attacks and few measures to the India Internet Users to avoid the cyber-attacks during the pandemic lockdown period. Lee, K.-T., Noh, M.-J., Koo, D.-M. (2013) Thus, this study has focused on the three important aspects of Internet Behavior as well as preference of using the social media apps, awareness on cyber-attacks and measures to overcome the cyber-attacks in this current situation.

1.3. Research Purpose

1. To analyze the frequency of preference to use various social media applications on theinternet activities during COVID – 19 lockdown and normal period.
2. To know the level of awareness of cyber-attacks through the internet/ applications duringCOVID – 19 Lockdown.
3. To identify the measures to overcome the cyber-attacks by the users during the coronalockdown time at India.

1.4. Research Hypothesis

- There is no association between the age of the respondents over the preference of the usingthe WhatsApp during the lockdown period.
- There is no influence of the educational qualification over the measures to overcome thecyber-attacks at the lockdown time.

2. Methodology of the Study

Study Area: This study is done in India.

1. **Sample Size**: 77.
2. **Sample Technique:** Simple Random and Convenient Sampling Technique. The popular social media app is taken according to the study undertaken in Mobile App usage in lock down. (Madhav Chanchani and Digbhijay Mishra)
3. **Data Collection**: Primary Data and Secondary Data. The Primary Data is collected throughthe well-structured questionnaire created through Google form. The Secondary

Data is collected from the News Article, Journals, Websites and Magazines.

4. **Data Analysis:** The statistical tools applied in this study are Percentage Analysis, Chi-Square, ANOVA, T-Test and Regression.

2.1. Results and Discussions

Table 1: Preference of using the Media Apps during Lockdown

One – Sample Test						
Apps	**Test Value = 0**					
	T	**Df**	**Sig. (2-Tailed)**	**Mean Difference**	**95% Confidence Interval of the Difference**	
					Lower	**Upper**
YouTube	44.309	76	.000	3.818	3.65	3.99
Facebook	25.191	76	.000	3.351	3.09	3.62
Whatsapp	59.341	76	.000	4.468	4.32	4.62
Tiktok	28.921	76	.000	3.299	3.07	3.53
Google Pay	26.331	76	.000	3.182	2.94	3.42
PUBG	22.755	76	.000	2.883	2.63	3.14
ZOOM	21.494	76	.000	3.013	2.73	3.29
Learning Apps	23.803	76	.000	3.584	3.28	3.88
Music Apps	34.434	76	.000	3.857	3.63	4.08
Aarogya Setu	21.926	76	.000	3.247	2.95	3.54

The table 1 reveals that apps 59.34, 44.31, 34.43, 28.92, 26.33, 25.19, 23.80, 22.76,21.93, and 21.49 are statistically significant at the 5 percent level. This indicates that the respondents are always preferred to use Whatsapp (4.468) during the COVID 19 lockdown time and they also frequently prefer to use to YouTube, Music Apps like Wynk, MX Player, Official/ Learning Apps (Byju, Vedanta) and Ellison, N. B., Steinfield, C., Lampe, C. (2007) Facebook.

Further, it reveals that the respondents are occasionally preferred to use Tiktok, Arogya Setu, GPay, and Zoom app. Finally, the respondents rarely prefer to access the PUBG during the COVID 19 lockdown time since 24th March, 2020 till May 1st week. As per the data analyzed by Nielsen and BARC the social media apps user base increased by 25% (Whatsapp tops by +27%). This study also identified that the majority of the respondent preference is Whatsapp.

Table 2: Awareness towards Cyber Attacks in Social Media Apps during Lockdown Period

One – Sample Test					
Cyber Attacks	**Test Value = 0**				
	T	**Df**	**Sig. (2-Tailed)**	**Mean Difference**	**95% Confidence Interval of the Difference**

					Lower	Upper
Phishing/Hacking	43.733	76	.000	2.805	2.68	2.93
Spyware	33.698	76	.000	2.636	2.48	2.79
Malware	33.411	76	.000	2.623	2.47	2.78
Ransom ware	20.61	76	.000	2.169	1.96	2.38
Denial of Service	25.77	76	.000	2.455	2.26	2.64

The table 2 denotes that 43.733, 33.70, 33.41, 25.77, and 20.61 are statistically significant at the 5 percent level. This implies that the respondents are well aware of Phishing/ Hacking in the social media/ Mobile Apps during the lockdown period. Further, it denotes that the respondents are aware of spyware, Malware and Denial of Service attacks in the social media/ Mobile Apps. Finally, the respondents do not have much awareness towards Ransom ware attacks in the social media/ Mobile Apps. Ledbetter, A. M., Mazer, J. P., DeGroot, J. M., Meyer, K. R., Mao, Y., Swafford, B. (2011) The report released in the Times of India dated on 11th April, 2020 also identified that Phishing attacks are increasing during the corona lockdown period in the Banking Transactions.

It has given warning to the customers to protect their CVV/ PIN number against the Phishing. Another report on 4th April, 2020 released by the Times of India has mentioned that Hackers are attacking the employees working from home. Thus, this study has identified that the maximum number of respondents is highly aware of Phishing/ Hacking during the corona lockdown period.

Table 3: Measures to overcome Cyber Attacks during Corona Lockdown Period

One – Sample Test						
Measures	**Test Value = 0**					
	T	**Df**	**Sig. (2-Tailed)**	**Mean Difference**	**95% Confidence Interval of the Difference**	
					Lower	**Upper**
Do not download unknown attachments and files from e- mails	46.247	76	.000	4.494	4.30	4.69
Install known/ authenticated security software's	66.520	76	.000	4.532	4.40	4.67
Don't reveal CVV/ PIN/ Account Number/ anyother bank details to the unknown people	64.951	76	.000	4.636	4.49	4.78
Report to the Bank official immediately regarding the suspicious/ doubtful call	46.870	76	.000	4.468	4.28	4.66
Call to the Toll free/ report to cybercrime official for cyber attacks	41.071	76	.000	4.325	4.11	4.53
Try to avoid downloading mobile apps like any desk, Quick support and etc.	44.709	76	.000	4.377	4.18	4.57

The table 3 indicated that 66.52, 64.95, 46.87, 46.25, 44.71, and 41.07 are statistically significant at the 5 percent level. Hence, the respondents strongly agree that they should install the known/ authenticated security software's in their Computers/ Smartphones, not to reveal their CVV/ PIN/ Account Number/ any other personal details to unknown people and do not download the unknown attachments or files from the e-mails to avoid the cyber-attacks during normal days and especially during a corona lockdown time. Carpenter, J. M., Green, M. C., LaFlam, J. (2011), Vogel, E. A., Rose, J. P., Okdie, B. M., Eckles, K., Franz, B. (2015) It has also indicated that the respondents agree towards reporting to the Bank official immediately about the suspicion/ doubtful calls, calling to the toll-free numbers/ to cybercrime official for the cyber-attacks and avoiding to download unknown apps in the mobile like any desk, quick support and so on to overcome the cyber-attacks during this lockdown time.

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	346[a]	0.12	0.108	1.102

It is found from the above table that R= .346, R Square=.120, Adjusted R Square=.108, Std. Error=1.102. This shows that the awareness of Phishing/ Hacking by the respondents created a variance of 10.8%. This leads to the following ANOVA table.

Table 5: ANOVA (b)

Model	Variables	Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	12.372	1	12.372	10.179	.002b
	Residual	91.16	75	1.215		
	Total	103.532	76			

From the above table it is observed that F=10.179; P=.002 is statistically significant at the 5 percent level. It indicates that the respondents are aware of the Phishing/ Hacking attacks. This leads to following coefficient table.

Table 6: Coefficients (a)

Model	Variables	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta	B	Std. Error
1	(Constant)	1.340	0.643		2.085	0.04
	Hacking	0.717	0.225	0.346	3.19	0.002

It is inferred from the above table that the level of awareness towards Phishing/ hacking attack (Beta=.346; B=3.190; P=.002) is statistically significant at the 5 percent level. This indicates the respondents always accessing the Facebook are highly aware towards the Phishing/ Hacking attacks during the corona lockdown period. Bessière, K., Kiesler, S., Kraut, R., Boneva, B. S. (2008) The level of Phishing/ Hacking awareness varies according to the respondent preference towards access the Facebook.

3. Suggestions

These are suggested recommendations from this study:

- More awareness has to be created regarding the ransom ware attacks and Denial of Service(DOS) for those who are working from home.
- The customers must be educated to approach Bank officials in case of any suspicious call/ doubtful call regarding inquiry of account details.
- The cybercrime cell has to frequently announce its toll-free numbers/ helpline numbers in case of any cyber-attacks. The customers must be encouraged to report to the cybercrime toll numbers/ websites immediately regarding the cyber-attacks.
- The customers must be constantly informed about the various mobile apps being attacked by the hackers.

4. Conclusion

The cybercrime and cyber-attacks are started increasing in the last decade due to the entrance of technology like computer, internet, automation, online payments, and so on. This paved the way to increase in the user rate of the technology and utilization of automated/ digital products. Hence, the cyber-attacks are started increasing as the penetration of internet, smartphone, social media apps users rate are increasing. The people are also started to work from home during the COVID 19 lock down period, so the hackers/ phishing, ransom ware increased and they started focusing on people who are working from home as well as operating banking transactions through online/ mobile. Thus, this study focus is to analyze the internet behaviours of India consumers and creates awareness of various cyber-attacks. Finally, this study suggests few measures to overcome these attacks during this pandemic lockdown and normal period.

The profile of the India internet users consists of the female. Most of the consumers were in between the age group of 21-30 years, possessing an educational qualification of post-Graduation. They are working in the Private Organizations/ Sector/ Banks in the area of Finance, Research Analyst, and Travels and so on. Their annual income is less than Rs. 5,00,000 and marital status is single.

The internet behaviours of India people are spending more than 4 hours per day; they are accessing the internet through their smartphones/ mobile phones and the main reason for the using theinternet is entertainment. The respondents always prefer to use the Whatsapp. White, J. B., Langer, E. J., Yariv, L., Welch, J. C. (2006) They are highly aware of phishing/ hacking attacks of the social media app. Moreover, the respondents strongly agree to install the known/ authenticated security software's in their Smartphones/ Tablets/ Laptop/ Computers. The Facebook users are aware of the phishing/ hacking attacks. Chou, H.-T. G., Edge, N. (2012) There is no association between the respondents age over the usage of Whatsapp. There is no influence of educational qualification over the measures to overcome the cyber-attacks.

5. Scope for Future Research

- The similar research of cyber-attacks can be carried in the Banking Sector.
- The Cyber Crime research can be done in the future as an individual study on social media, Mobile Apps, and e-mails.

6. References

[1] Baumeister, R. F., Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. Psychological Bulletin, 117, 497–529. doi:

https://doi.org/10.1037/0033- 2909.117.3.497
[2] Bessière, K., Kiesler, S., Kraut, R., Boneva, B. S. (2008). Effects of Internet use and social resources on changes in depression. Information, Communication & Society, 11, 47–70. doi: https://doi.org/10.1080/13691180701858851 .
[3] Carpenter, J. M., Green, M. C., LaFlam, J. (2011). People or profiles: Individual differences in online social networking use. Personality and Individual Differences, 50, 538–541. doi: https://doi.org/10.1016/j.paid.2010.11.006
[4] Shrilatha S., Aruna K., Bhagavathy S., Chellaiah G., Gupta A. Future of electric vehicles with reference to national electric mobility mission plan at Tamil Nadu (2021) AIP Conference Proceedings, doi: https://doi.org/10.1063/5.0066282
[5] Kasinathan, A., Kasthurirangan, D., & Bhagavathy, S. (2022). The Prevalence and Predominance of Artificial Intelligence in YouTube Advertisements in Shaping the Lifestyle of the Budding Generation. In S. Iyer, A. Jain, & J. Wang (Ed.), *Handbook of Research on Lifestyle Sustainability and Management Solutions Using AI, Big Data Analytics, and Visualization* (pp. 206-220). IGI Global. Doi: https://doi.org/10.4018/978-1-7998-8786-7.ch013
[6] Chou, H.-T. G., Edge, N. (2012). "They are happier and having better lives than I am": The impact of using Facebook on perceptions of others' lives. Cyberpsychology, Behavior, and Social Networking, 15, 117–121. doi: https://doi.org/10.1089/cyber.2011.0324
[7] Ellison, N. B., Steinfield, C., Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12, 1143–1168. doi: https://doi.org/10.1111/j.1083-6101.2007.00367.x
[8] Ledbetter, A. M., Mazer, J. P., DeGroot, J. M., Meyer, K. R., Mao, Y., Swafford, B. (2011). Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness. Communication Research, 38, 27–53. doi: https://doi.org/10.1177/0093650210365537
[9] Lee, K.-T., Noh, M.-J., Koo, D.-M. (2013). Lonely people are no longer lonely on social networking sites: The mediating role of self-disclosure and social support. Cyberpsychology, Behavior, and Social Networking, 16, 413–418. doi: https://doi.org/10.1089/cyber.2012.0553
[10] Morahan-Martin, J., Schumacher, P. (2003). Loneliness and social uses of the Internet. Computers in Human Behavior, 19, 659–671. doi: https://doi.org/10.1016/S0747-5632(03)00040-2 .
[11] Nie, N. H. (2001). Sociability, interpersonal relations, and the Internet: Reconciling conflicting findings. American Behavioral Scientist, 45, 420–435. doi: https://doi.org/10.1177/00027640121957277
[12] Teppers, E., Luyckx, K. A., Klimstra, T., Goossens, L. (2014). Loneliness and Facebook motives in adolescence: A longitudinal inquiry into directionality of effect. Journal of Adolescence, 37, 691–699. doi: https://doi.org/10.1016/j.adolescence.2013.11.003
[13] Vogel, E. A., Rose, J. P., Okdie, B. M., Eckles, K., Franz, B. (2015). Who compares and despairs? The effect of social comparison orientation on social media use and its outcomes. Personality and Individual Differences, 86, 249–256. doi: https://doi.org/10.1016/j.paid.2015.06.026
[14] White, J. B., Langer, E. J., Yariv, L., Welch, J. C. (2006). Frequent social comparisons and destructive emotions and behaviors: The dark side of social comparisons. Journal of Adult Development, 13, 36–44. doi: https://doi.org/10.1007/s10804-006-9005-0