Volume 3, Issue 1, January – 2024
PP 1-11

International Journal of Futuristic Innovation in Arts, Humanities and Management (IJFIAHM)

Social Media and Privacy: Understanding the Risks to Personal Data

Omprakash Dewangan, Akanksha Mishra, Jyoti Nainani

Assistant Professor, Department of CS & IT, Kalinga University, Naya Raipur

omprakash.dewangan@kalingauniversity.ac.in

Assistant Professor, Department of CS & IT, Kalinga University Naya Raipur

akanksha.mishra@kalingauniversity.ac.in

Assistant Professor, Department of CS & IT, Kalinga University Naya Raipur

Jyoti.nainani@kalingauniversity.ac.in

ABSTRACT: Social media platforms have largely taken over our daily lives in recent years, giving people a way to communicate with one another and exchange private information. The extensive usage of social media has increased the potential of privacy violations and cybercrime. The increasing use of social media platforms has raised concerns about the protection of personal data and privacy. This research paper examines the threat to private data from social media and the laws and measures in place to address this issue in India.

To examines the possible dangers of using social media, such as data breaches, identity theft, hostile hackingand unauthorized access to private data. There are also about the laws which defend the threat to private data from social media. The Personal Data Protection Bill of 2019 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 are two examples of the legislative framework in India that covers the protection of personal data.I have also drawn attention to the moral and legal issues related to social media corporations' exploitation of users' personal information using previous related cases. I have finishedwith suggestions on how people and organizations might safeguard their private information and uphold their privacy in a connected world.The paper concludes that while India has taken significant steps towards protecting personal data, there is still room for improvement. The Personal Data Protection Bill, 2019, is yet to be passed, and there is a need for greater awareness among citizens about the importance of protecting their personal data. The paper recommends that the government should strengthen the legal framework and increase public education to ensure that the privacy and personal data of Indian citizens are adequately protected. At the end some measures are mentioned which can adapt by users to keep safe their data and themselves.

Keywords: Cyber bullying, Personal Data Protection Bill, 2019, Phishing, Privacy Policy, Scams, Social Media.

I. INTRODUCTION

Social media platforms have become a vital part of our everyday lives, giving a platform for communication, collaboration, and information sharing. However, given the large volume of personal information published on social media, there is a risk that this information may be mistreatedby mischievous actors.The gathering and sharing of personal information by third-party apps and services is another threat to private data from social media. These apps may gain access to your social network account and collect data about you without your knowledge or agreement, which can then be used for targeted advertising or other purposes.

Here are some of the threats to private data from social media:

A. Data breaches:

Social media platforms keep massive amounts of personal data, such as names, email addresses, phone numbers, and other information. If there is a data breach, this information could be accessible to hackers who could use it for identity theft, fraud, or other nefarious purposes.

B. Phishing and scams:

Phishing attacks can target social media users by mimicking a trusted source and tricking them into disclosing personal information. Scams, such as phone gifts or fraudulent investment programmed also be promoted via social media.

C. Cyberstalking and harassment:

Social media may also be a tool for cyber talking and harassment, in which criminals utilize victims' personal information to threaten or harass them online.

D. Social engineering:

Social media gives a lot of personal information about individuals that can be exploited to build targeted social engineering attacks. These attacks might range from phishing efforts to impersonation scams.

E. Online reputation damage:

Individuals social media posts might come back to haunt them in the form of online reputation damage. Employers, future partners, and others might view public social media posts that are potentially embarrassing or damaging to a person's reputation. The potential of data breaches from social media is one of the most serious threats to private data. When a social media site is hacked, users' personal information might be taken and sold on the dark web. Even if you remove your social network account, your data may still be retained on the platform's servers.

The laws which defend the threat to private data from social media are:

In India, the primary law that deals with the protection of personal data is the Personal Data Protection Bill, 2019. The bill was introduced in the Indian Parliament in December 2019, and it is currently under consideration by a parliamentary committee. Once passed, the bill will become

law, and it aims to provide a framework for the protection of personal data and the establishment of a Data Protection Authority.

The Rules for Sensitive Personal Data or Information and Reasonable Security Practises and Procedures in Information Technology of 2011. These rules complement the Personal Data Protection Bill. These guidelines apply to businesses that gather, keep, and handle sensitive personal data or information. Such businesses are required by the regulations to use acceptable security practises and processes, seek data subjects' consent, and declare the reason for data collecting.

Moreover, the Indian government recently announced new guidelines for social media platforms under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules apply to social media platforms, messaging apps, and digital news organizations, among others. The guidelines require social media platforms to establish a grievance redressed mechanism, appoint a compliance officer, and remove objectionable content within 36 hours of receiving a complaint, among other things.

Overall, these laws and guidelines aim to protect the privacy and personal data of Indian citizens and ensure that social media platforms operate responsibly and with accountability.

II. BACKGROUND

The evolution of social media has altered the way we interact, share information, and engage with one another. Social media platforms such as Facebook, Twitter, Instagram, and LinkedIn have become a crucial part of our everyday lives, allowing us to interact with friends and family, share our views and experiences, and stay up to date on the latest news and trends.

However, as social media has become more popular, there has been an increase in worry about the privacy and security of our personal information. Personal information such as names, email addresses, phone numbers, and location data are collected by social media sites from their users. Companies can use this information for targeted advertising, while hackers can exploit it for harmful purposes such as identity theft, fraud, and phishing scams.

There have been several high-profile cases in recent years involving threats to private data from social media platforms. Here are a few examples:

A. Cambridge Analytical :

In 2018, it was discovered that the data analytics company Cambridge Analytical had illegally collected millions of Facebook users' personal data and used it to sway political campaigns, including the 2016 US presidential election. Regulators around the world are now paying more attention to social media sites as a result of the controversy that caused a public outcry over Facebook's management of user data.

B. Twitter hack:

In July 2020, several high-profile Twitter accounts, including those of Barack Obama, Joe Biden, and Elon Musk, were hacked in a coordinated attack that was carried out by a group of hackers

who gained access to Twitter's internal systems. The hackers used their access to the accounts to promote a Bitcoin scam, and were able to steal more than $100,000 before being caught.

C. Facebook data breach:

In September 2018, Facebook revealed it had had a data breach that had impacted around 50 million user accounts. Due to a flaw in Facebook's "View As" feature, hackers were able to collect access tokens that could be used to hijack user accounts, which led to the breach. The incident, which was among the biggest in the business's history, raised questions about Facebook's security procedures.

D. Privacy issues with TikTok:

In 2020, privacy issues with the Chinese-owned social media app TikTok were brought up. It was said that TikTok gathered user data and shared it with the Chinese government. Due to these worries, requests for the app's ban in the US were made, and other Chinese-owned digital firms came under more scrutiny.

Furthermore, using third-party apps and services on social media platforms puts our personal information at risk. These apps may gain access to our social media accounts and collect data without our knowledge or permission, which can then be used for targeted advertising or other purposes.

As a result of these dangers, social media companies have added a variety of safeguards to secure user data, including enhanced privacy settings, two-factor authentication, and data encryption. However, it is critical for users to assume responsibility for their own privacy and security and to take precautions to keep their personal information safe.

III. HYPOTHESIS

Hypothesis 1: The Terms and Conditions of the Apps include Privacy Policies; which can use the personal information of the user to show relevant adds which may threat to user's information.

Hypothesis 2: Revealing themselves by posting minute-to-minute posts and stories shows much more information about the user's to the followed people.

Hypothesis 3: Linked social media accounts with the game applications and other websites, may lead to the data corruption or steal the information of the user.

IV. LITERATURE REVIEW

A. Privacy Threats related to user profiling in online social networks by Fredrik Erslonson.

This paper presents different privacy threat in OSNs. Here the main threat are described as OSN information leakages, Third party interference , Trojan application, public information harvesting , socialbots and Friend-in –the-middle Trojan applications.

B. Report says about the cyber security breach by NBC news.

A cybersecurity firms gave a statement in which it is found that millions of records openly exposed on the internet containing public information from Facebook. Here the passwords are also leaked of about twenty two thousand users.

C. The data which are collected by the India's largest social media application Meta uses the terms and conditions for showing the adds by Facebook.

Under the section of Privacy policy the important ways to collect the public data are describe as :

- The activity and information that you provides,
- Friends followers and other connections,
- Apps browsers and device information,
- Information from partners and third parties apps.

D. Stealing of public information through game by CNN news.

The gamming applications uses the Facebook and google account to log in to the game, which threats the users data by gaining access to their accounts and sells or show to their respective government. Some countries IT acts mention that the companies should give their information of the public data at any required period when the government needed.

V. RATIONALE OF THE STUDY

The rationale for researching the threat to private data from social media is multifaceted. Firstly, social media platforms have become an integral part of many people's lives, with millions of individuals sharing personal information on these platforms daily. However, this information is often stored and processed by third-party companies, which can lead to potential privacy breaches if proper security measures are not in place.

Secondly, the rise of social media has led to an increase in cybercrime, with hackers and cybercriminals targeting social media platforms to steal sensitive information. This information can then be used for various malicious purposes, such as identity theft, fraud, and blackmail.

Thirdly, there is a growing concern among individuals and organizations about the misuse of private data by social media companies. Recent high-profile cases of data breaches and scandals involving social media platforms have highlighted the need for greater transparency and accountability in the way these companies handle personal data.

By researching on the threats to private data from social media, we can better understand the risks and develop strategies to mitigate them. This can help individuals and organizations protect theirsensitive information and maintain their privacy in an increasingly connected world.

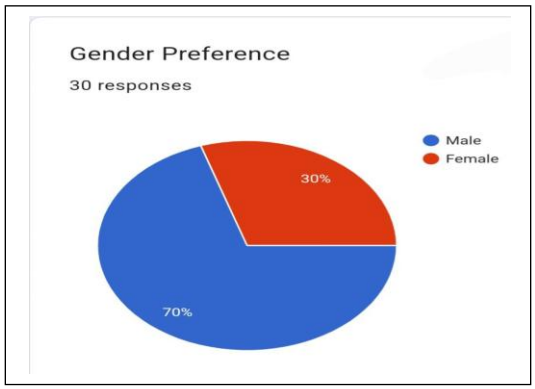
VI. METHODOLOGY

In this research, 'Quantitative Methodology' is used for the study and the data has been gathered via questionnaire. As youth is the leading generation of this nation, the age group between (13 - 50) of 30 people has been selected to analysethe awareness level of social media users regarding the security of their personal information.

Findings

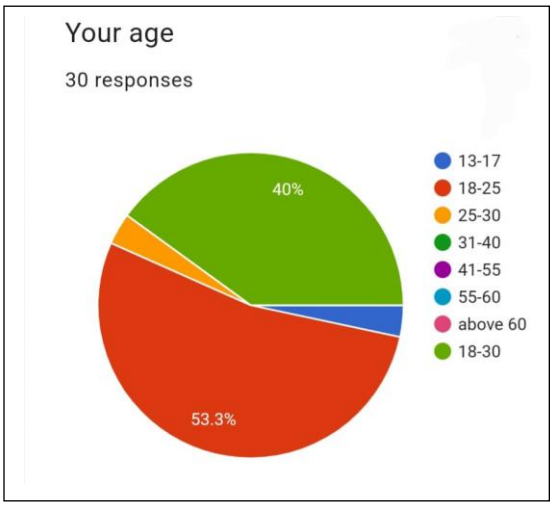
A. Gender:

Male with70 percent of participation has weighted with lead from women in the survey.



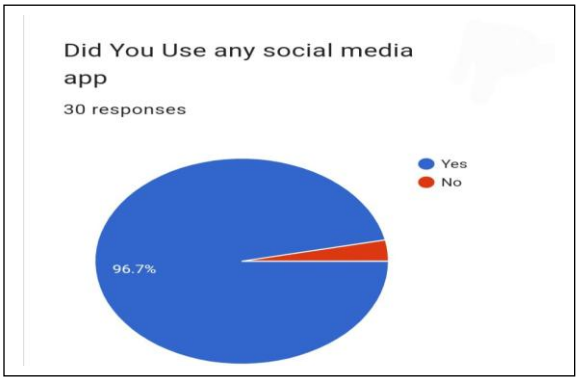
B. Age

Out of 30 people , the maximum age group participated in the survey was of 18 to 30.



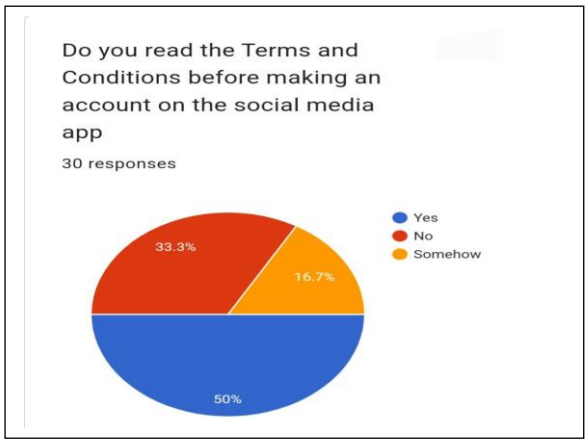
C. Do you use social media?

96.7 percent of the people as huge mass are active on the social media.



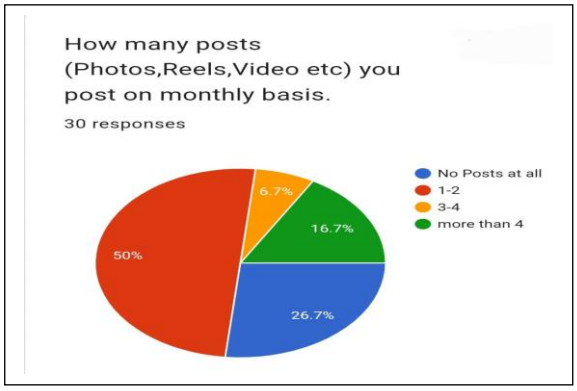
D. Do you read the Terms and conditions before making an account on the social media app?

Only half of the people read the terms and conditions where only 33.3 % people don't even see that.



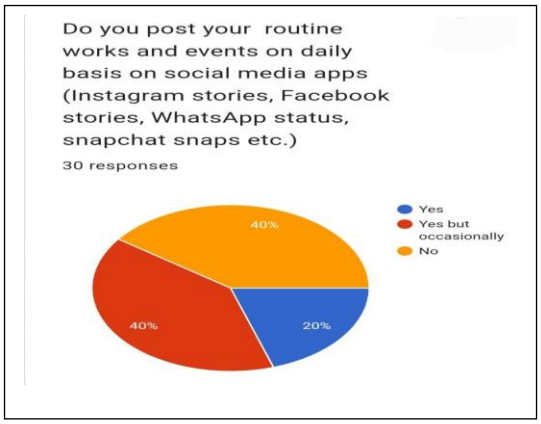
E. How Many posts (photos , Reels , Video, etc.) you post on monthly basis?

As per the responses, 50% of people post atleast couple of post on monthly basis.

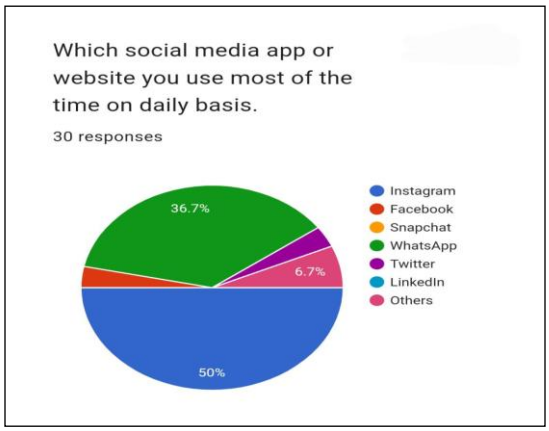


F. Do you post your routine work and events on daily basis on social media apps?

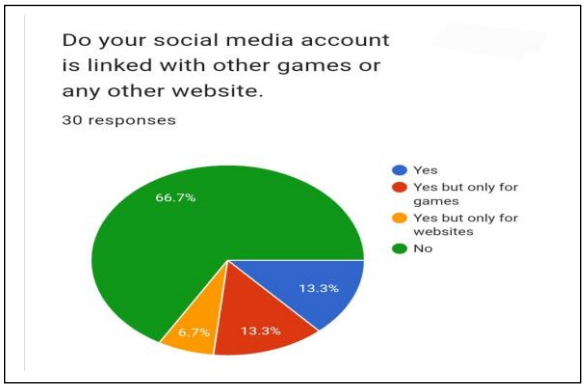
60 % of people post their daily routine of their life on the social media.



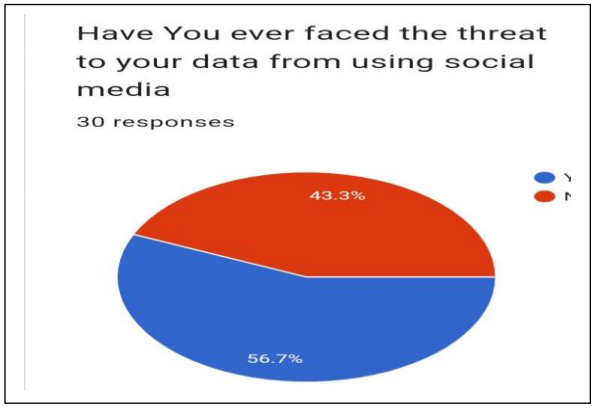
G. Which social media app or website you use the most of the time on daily basis?
Instagram has the half of the active users followed by whatsapp by 36.7%.



H. Do your social media account is linked with other games applications or any other websites?
32.7 % people of the survey has agreed that there social media accounts are linked with other websites.



I. Have you ever faced the threat to your data from using social media application ?
According to the survey, 56.7 %people had faced the threat to their data.



J. What is your opinion on threat to personal data from social media ?

In the people's opinion, it came out that they think if users are not sharing their any personal data then, they are safe. So people should try to use the social media as a social place not a place to share everything private and personal without thinking twice. They also said that private data on social media is very unsecured and can be exploited very easily.There are scammers and phishes waiting every time for your one mistake and negligence so carefully and very precisely share your personal data with only trusted people.

VII. RESULT AND CONCLUSION

There are several threats to private data from social media, which can have serious ramifications for individuals and society as a whole. Data breaches, identity theft, cyberbullying, and the spread of disinformation are all major concerns linked with social media use.

At the point when programmers gain admittance to delicate client information, for example, login passwords, individual data, and confidential interchanges, information breaks can happen. This can bring about data fraud, monetary extortion, and reputational hurt for people and associations.Another important concern is cyberbullying, particularly among young people who may be more prone to online harassment and abuse. Social media platforms can be used to disseminate rumours, harass people, and even inspire violence.

The propagation of disinformation is another key concern associated with social media use. False information can quickly spread via social networks, causing confusion, mistrust, and even harm to individuals and groups. This can be especially difficult during times of crisis, such as public health issues or natural catastrophes.

Only half of the people are aware and read the Terms and Conditions of the Apps includes Privacy Policies, but it is the first step to read the it's terms and conditions consciously. According to the research, posting personal information on social media platforms has some advantages but also having number of hazards too. So that it is not good to reveal yourselves by posting minute-to-minute posts and stories, which shows much more information about the user's to the followed people. Some people even without thinking just share their social media accounts detail with other websites .But People should be alert regarding their linked social media accounts with the game applications and other websites, which may lead to the data corruption or steal the information of the user.

Although India has made significant progress in securing personal data, there is always potential for improvement. The Personal Data Protection Bill, 2019, has yet to be passed, and citizens need to be more aware of the need of securing their personal data. The study suggests that the government tighten the legislative framework and increase public education to ensure that Indian residents' privacy and personal data are effectively protected.

VIII. METHODS TO PREVENT DATA THREAT

i) Many social media platforms support various configurable users' privacy settings that enable users to protect their personal data form other users or applications. Facebook, Instagram and LinkedIn are the widely used applications which provide the user the facility to change their

privacy settings and choose which other person in the network are able to view their details, pictures and posts.

ii) Child monitor applications is a good method to keep an eye on their child activity on the social media application. Parents can also view the followers list in their child friend list and can question about any over aged friend or an unknown person.

iii) Remove third party applications from the device as previous studies shows that the third party applications collect the personal information by suspecting the social media accounts.

iv) Keep updating the apps applications time-to-time, as with every new update the company brings new method to save the data from hackers also they add more security features for better security.

v) By limiting the number of stories that are put on different social media applications on the daily basis reduces the chance of being suspected by other person.

vi) Use the end-to-end encrypted method application for the transfer of files, images, videos, audios, texts. When the first user send any data to other, the data will be first decoded to the server side and then the decoded data is than transfer to the device where it gets encoded by the installed applications.

vii) Use strong passwords and enable two-factor authentication: Strong passwords and two-factor authentication can prevent unauthorized access to social media accounts, reducing the risk of data breaches and identity theft.

viii) Be cautious of phishing scams: Phishing scams can trick individuals into providing sensitive information to cybercriminals. Individuals should be cautious of suspicious messages and links received through social media and report them to the platform's administrators if they appear to be fraudulent.

ix) Use dependable antivirus software to protect your computer and mobile devices against malware infections, which lowers your chance of data breaches and other online risks.

x) Stay informed about the latest threats: Individuals and organizations should stay up-to-date on the latest threats to social media privacy and security and adjust their prevention measures accordingly.

CONCLUSION

To summarise, the risks to private data posed by social media are serious and must be carefully considered by individuals, organisations, and governments. Social media users can protect their private data by using strong passwords, enabling two-factor authentication, being cautious when sharing personal information, and reviewing privacy settings on a frequent basis.While social media has numerous advantages, it is critical to be aware of the hazards and take precautions to preserve personal data and privacy online. This includes being cautious when sharing personal

information, using strong passwords and security settings, and staying up to date on the latest dangers and online safety best practises.

REFERENCES

1. NBC News articles - https://www.nbcnews.com/tech/tech-news/facebook. (2023, January) Facebook terms. [Online]. Available: http://www.facebook.com/legal/terms.
2. CNN news article https://edition.cnn.com/2020/07/28/tech/india-china-apps-ban-hnk-intl/index.html.
3. NBC news -https://www.nbcnews.com/tech/tech-news/facebook-user-data-millions-found exposed-internet-third-party-apps-n990621.
4. Laura F. Bright, Kelty Logan and Hayoung Sally Lim, “Social Media Fatigue and Privacy: An Exploration of Antecedents to Consumers’ Concerns regarding the Security of Their Personal Information on Social Media Platforms”, Journal of Interactive Advertising,volume 22, 2022, https://doi.org/10.1080/15252019.2022.2051097.
5. Baker-Eveleth, L., Stone, R. and Eveleth, D. (2022), "Understanding social media users’ privacy-protection behaviors", Information and Computer Security, Vol. 30 No. 3, pp. 324-345. https://doi.org/10.1108/ICS-07-2021-0099.
6. Aras Alkis, Tekin Kose, “Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe”,Computers in Human Behavior,Volume 137,2022,107412,ISSN 0747-5632, https://doi.org/10.1016/j.chb.2022.107412.
7. Saura, J.R., Palacios-Marqués, D. & Ribeiro-Soriano, D. Privacy concerns in social media UGC communities: Understanding user behavior sentiments in complex networks. Inf Syst E-Bus Manage (2023). https://doi.org/10.1007/s10257-023-00631-5.
8. Marín, V.I., Carpenter, J.P., Tur, G. et al. Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers. J. Comput. Educ. 10, 769–795 (2023). https://doi.org/10.1007/s40692-022-00243-x.