



---

## Impact of user awareness about privacy concerns of sharing personal information on social media: Facebook, Instagram

*Amita Gerg<sup>1</sup>, Dhruv Pushpavadan<sup>2</sup>, Tanya Dineshpal Singh<sup>2</sup>*

<sup>1</sup>Assistant Professor, Parul University

<sup>2</sup>Student, Parul University

---

### ABSTRACT

Popular social-media platforms in the country, particularly in Indonesia, include Facebook, Twitter, and Instagram (which is now owned by Facebook). Risks associated with social media usage are rising as the number of users grows. In 2018, Facebook had a user-data breach, which illustrates one of the dangers to users' security and privacy. These challenges prompted the authors to undertake study on the impact of privacy concerns, trust, and user knowledge on the willingness to reveal personal information through social media. It was decided to build a research model around a number of different assumptions. An online survey of 340 social media users was performed over a two-month period using the model's validated questionnaires. A reliability and validity study was carried out to verify the structural model that was used in this study. An SEM analysis was utilised to discover the correlations between the study model's components. The findings of this study reveal that user knowledge, trust, and privacy concerns have a favourable and substantial influence on sharing personal data on social media. We next explored the significance of our findings for policymaking, practise, and future research.

---

### INTRODUCTION

Social media has evolved into one of the most important aspects of everyone's life. One cannot picture a day without social media in his or her life. Some well-known social networking websites include Facebook, Twitter, Gmail, WhatsApp, Snapchat, Instagram, and LinkedIn. They have over 100 million users around the world.

While you are using your social media accounts, someone is watching you and your accounts. These are social media hackers who get access to your accounts by obtaining your login credentials. There are numerous more dangers and risks associated with social networking in addition to this one. Having a thorough understanding of all of these risks.

Social networking websites have grown in popularity in the era of Internet technologies. The laws of social interaction and communication have been altered by computer-mediated communication. Most social networking sites, such as Facebook, Google+, and Twitter, Instagram, provide users with features such as online engagement, information sharing, and the development of new relationships. New privacy problems have arisen as a result of online interaction and sharing of personal information on social networking sites. As a result, it necessitates an investigative understanding of the user's behavioural purpose to provide information.

The bounds of social communication have been pushed farther by online social networking. Everyone can now disclose their personal items, sentiments, and relationships over the internet. Although it facilitates communication, internet contact has also resulted in the creation of a vast pool of information that may be easily accessed and misused. These Online Social Networks have security and privacy features to safeguard users' sensitive information from unauthorised access, yet these rules are still broken since users are unaware of the hazards and how to avoid them.

The number of social-media users is increasing every year, accompanied by increased risks. One of those risks is to the security and privacy of users, as shown by the user-data leak experienced by Facebook in 2018.

---

## FACEBOOK

Personal information from over 533 million Facebook users from 106 countries was discovered to have been leaked online earlier this year. Alon Gal, CTO of cyber intelligence firm Hudson Rock, was the first to warn in January that a Telegram bot was being used to sell free phone numbers. The bot took advantage of a flaw in a Facebook function that allowed everyone's phone numbers to be accessed for free.

This isn't the first time a data leak from Facebook has been reported — there have been a number of them in the past, the most infamous of which in recent memory was the Cambridge Analytica scandal in 2018, when it was revealed that a political consulting firm used Facebook data to influence elections.

## INSTAGRAM

Instagram is one of the most widely used social media sites, with users from all over the world using it. It's a platform for all types of artists, from those who want to provide unique beauty tips to those who want to make money by uploading short videos, IGTV, etc. This platform outperforms all other major apps in terms of user engagement.

In the event that a user forgets their password, the "password reset or recovery" option allows them to restore access to their account. In order to verify their identity, Instagram users must validate a six-digit secret code given to their selected phones or email accounts that expires after 10 minutes.

Laxman Muthiyah, an Indian bug bounty hunter, recently uncovered a vulnerability in the password recovery step of Instagram's mobile app. Instagram's rate-limiting function, according to Laxman, may be circumvented by sending a large number of requests from numerous IP addresses, as well as submitting multiple requests to process at the same time.

---

## OBJECTIVES OF THE STUDY

- To investigate the security concerns that customers have when using social media
- To find out the various preventive measures taken by the users to avoid leakage of personal information.
- To Study the awareness amongst the customers about the various security features available on various social media.

---

## PROBLEM STATEMENT OF THE STUDY

Today all social media offers a wide range of security services to their users. Despite the fact all social media provides security. It is critical to investigate whether all social media platform aware of security policies. A user should have thorough knowledge and awareness of various social media platform to avoid the disclosure of their personal information.

A social media platform owner should be able to figure out what kind of security policy user needs, as a result the projects goal is to discover a study on the impact of user understanding of trust & privacy on sharing personal information social media.

---

## HYPOTHESIS OF THE STUDY

H0:Differences in impact between user concerns about privacy when submitting personal information to social media and user awareness are significant social networks such as facebook, instagram, and twitter

H1:User awareness of privacy concerns in sharing personal information on social media: there is no significant and distinct difference in the impact of user awareness of privacy concerns in sharing personal information on social media. Instagram, facebook.

---

## REVIEW OF LITERATURE

Facebook and Instagram are the most often and most widely used social-media sites, especially in Indonesia. The number of social-media users is increasing every year, accompanied by increased risks. One of those risks is to the security and privacy of users, as shown by the user-data leak experienced by Facebook in 2018. These issues led the authors to conduct research relating to the influence of privacy concerns, trust, and user awareness on the readiness to share personal information via social-media sites. A research model was developed based on several hypotheses. The research model was confirmed, and experiment was conducted from 340 social-media users through a questionnaire-based online survey over a period of 2 months. To confirm the structural model used in this research, reliability and validity analyses were performed. Structural equation model (SEM) analysis was used to detect relationships among constructs in the research model. The results of this research show that user awareness, trust, and privacy concerns have a positive and significant effect on sharing personal data on social media. Then we discussed the implications of our results for policy-making, practice, and future research.

Harvested social media data has the potential to enhance emergency response decision support if its reliability can be assessed. Slándáil aims to develop a prototype system which automates social media data analysis for emergency response. This paper considers some of the ethical concerns that may arise with such alternate use of data. It offers technical (hardware and software) and operational measures intended to improve the security of data and information flow to mitigate those risks.

To deliver personalized services to users, recommendations systems are highly important. Despite the numerous advantages, implementing personalized recommendation systems usually necessitates the collection of users' personal data, especially online usage, which unnecessarily exposes users to significant privacy concerns. As a result, developing a functional privacy-preserving framework to prevent sensitive information from being inferred against inference attacks is critical. The main idea is to mask the users' information such that the original data is transformed with data anonymization to comply with data security and privacy regulation. As a result, using different entropy-based metrics, our system will quantify privacy leakage, which provides effective privacy protection for individuals.

A social network is a public structure made up of people or associations called nodes, which are associated by at least one particular sorts of interdependency, for example, friendship, normal interest, and interchange of fund, connections of convictions, information or notoriety. A cyber threat can be unexpected and purposeful, directed or nontargeted, and it can originate from an assortment of sources, including outside countries occupied with secret activities and data fighting, criminals, programmers, hackers, virus code writer, displeased representatives and contractual workers working inside an association. Social networking destinations are not only communicated with other individuals all inclusive, yet additionally one successful route for business promotion.

Social networks have become a part of human life. Starting from sharing information like text, photos, messages, many have started share latest news, and news related pictures in the Media domain, question papers, assignments, and workshops in Education domain, online survey, marketing, and targeting customers in Business domain, and jokes, music, and videos in Entertainment domain. Because of its usage by Internet surfers in all possible ways, even we would mention the social networking media as the current Internet culture. While enjoying the information sharing on Social Medias, yet it requires a great deal for security and privacy. The users' information that are to be kept undisclosed, should be made private.

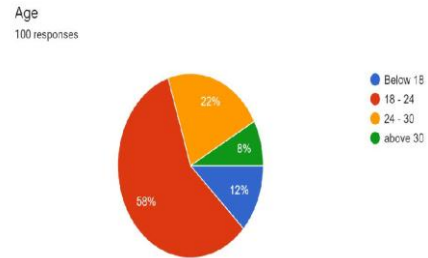
---

## RESEARCH METHODOLOGY

Research is based on primary data that is collected through questionnaire and secondary data is collected from websites, journals and previous studies. The sample size for this research was 100.

**DATA ANALYSIS AND INTERPRETATION**

**1.AGE WISE**

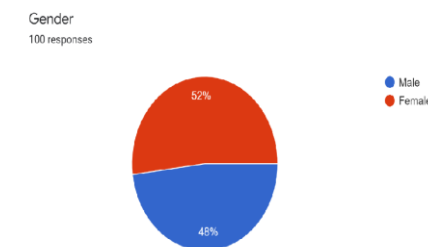


**INTERPRETATION:**

The first interpretation of the chart shows that Out of 100 respondents, 58% respondents are between the age of 18-24, 22% respondents are between 24-30, 12% respondents are below 18 and 8% respondents are above age 30.

**2.GENDER WISE**

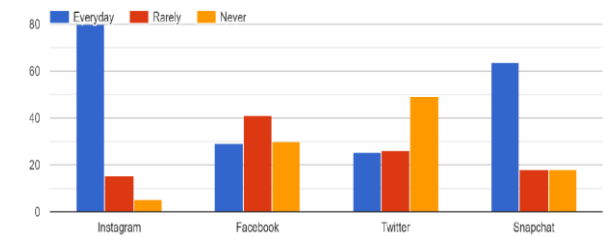
INTERPRETATION: The second interpretation of the chart shows the gender wise distribution of the sample survey. From the data collected it can be



analysed that there is 52% female and 48% male.

3.

Which Social Media platform will you prefer the most ?



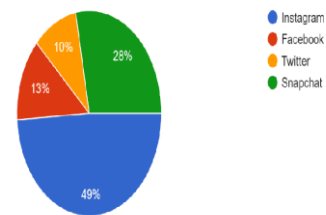
**INTERPRETATION:**

The third interpretation of the chart shows the preference of the social media platform which is used on daily basis, rarely, or never. From the data collected it can be analyzed that most of the respondents prefer Instagram on day-to-day basis, Facebook and Snapchat are rarely used by the respondents.

4.

Which Social media platform is more secure according to you ?

100 responses

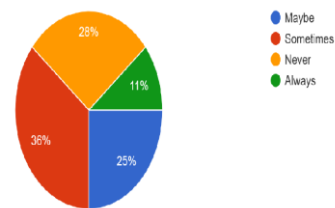
**INTERPRETATION:**

The fourth interpretation of the chart shows that which social media platform is more secure according to the users. From the data collected it can be analysed that there are 49% respondents who think that Instagram is more secure, 28% respondents who think Snapchat is secure, 13% respondents think Facebook is secure and 10% respondents think Twitter is secure.

5.

Have you ever share or post your personal information such as your phone numbers, home/work address in your profile ?

100 responses

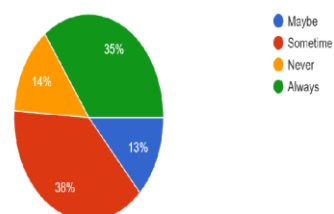
**INTERPRETATION:**

The fifth interpretation of the chart shows that how many respondents share or post their personal information on social media. From the data collected it can be analysed that 11% respondents always share their personal information, 25% respondents maybe share, 36% respondents sometimes share their information and 28% respondents never share or post their personal information on social media platform.

6.

Do you think before posting your photos (to avoid it from being exploited )

100 responses

**INTERPRETATION:**

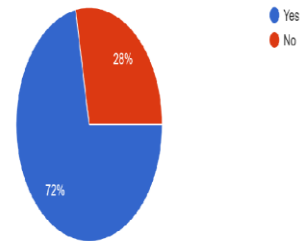
The sixth interpretation of the chart shows that how many respondents think before posting their photos (to avoid it from being exploited) on social media. From the data collected it can be analysed that 13% people will maybe think before posting, 35% always think, 14% sometimes think and 38%

never thinks before posting photos on the social media

7.

Do you Enable privacy setting to restricted who can post and access information on your children websites.

100 responses



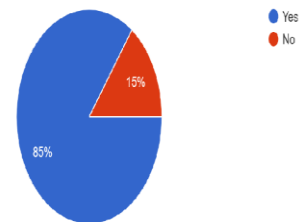
#### INTERPRETATION:

The seventh interpretation of the chart shows that how many respondents enable privacy settings to restricted that who can access the information on your children website. From the data collected it can be analysed that 72% of respondents have enabled the privacy settings to restricted and 28% of the respondents have not enabled the privacy settings.

8.

Are you aware what information should be kept private and not shared.

100 responses



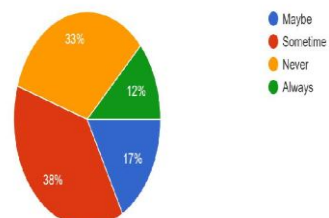
#### INTERPRETATION:

The eighth interpretation of the chart shows that how many respondents are aware that what information should be kept private and not shared. From the data collected it can be analysed that 85% of respondents are aware and 15% of the respondents are not aware.

9.

Do you respond to harassing or threatening comment posted on your profile.

100 responses



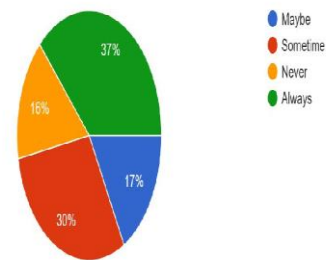
**INTERPRETATION:**

The ninth interpretation of the chart shows that do you respond to harassing or threatening comment posted on your profile. From the data collected it can be analysed that 12% people responds, 17% will respond when something related to that happens with them, 33% never responds and 38% people sometimes responds.

10.

Do you add people as friends to your site only if you know them ?

100 responses

**INTERPRETATION:**

The tenth interpretation of the chart shows that do you add people as friends to your site only if you know them. From the data collected it can be analysed that 16% people never add, 17% maybe add, 30% will sometime add and 37% people always add people as friends only if they know them.

**FINDINGS**

- From The Above Research It Has Been Seen That Instagram Is Used On Daily Basis And The Most Secure App Used On Daily Basis And The Most Secure App With All The Privacy
- 36% Of Respondents Say They Share Their Information On Occasion.
- 13% Of Population Will Perhaps Think Twice Before Posting Or Uploading Images On Social Media.
- 72% Of Respondents Have Restricted Privacy Options Enabled While 28% Have Not Enabled Privacy Settings.
- 85% Of Those Polled Are Aware Of The Types Of Information That Should Be Kept Private And Not Shared.
- For Security Reasons 56 % Respondents Have Installed Monitoring Software While 43% Have Not
- 44% Of Respondents Believe That If They Submit A Photo To A Social Networking Platform, It Will Be Misused And 56 % Of People Never Worried About It.

**SUGGESTIONS**

The number of people using social networking sites is growing rapidly, as is the amount of personal information that is shared. The social networking world is full of both useful and worthless information. It is equally critical for users to be aware of potential security concerns and to learn how to take actions to protect themselves and their data. Before releasing or sharing any sensitive information, one must exercise extreme caution and be aware of the potential implications. So, before you do anything on social networking sites, be cautious and consider your options. It is recommended that you study the privacy policies, terms of service, and other important papers on social networking sites. If the user is not convinced or at ease, they have the option to terminate.

---

## CONCLUSIONS

This study has revealed that Users often publish sensitive data that can be exploited to track their whereabouts and activities, according to one study. The majority of users are unaware that their posts and updates are public and easily accessible. To safeguard consumers from probable loss of property or surveillance, it is vital to enhance their privacy awareness. Facebook's and Instagram privacy settings should be made easier to comprehend and more prominent so that they are used. Regulators must also ensure that rules protecting users' data are followed. According to our findings, more user training on how to use Facebook's and Instagram privacy settings could increase privacy awareness. Users must be taught how to secure themselves in various ways.

According to research on user knowledge and consciousness of personal information on social media, participants as social media users already understand what personal information implies in their own words. They can also provide explanations and examples for a variety of personal data facts. Users frequently use personal data information for multiple purposes when communicating on social media. When interacting with social media, the engagement of this information is recognised to have a relationship at the stage of individual consciousness. Individual awareness phases can be distinguished from critical thinking stages that participants engage in while adding personal information and data to their social media pages. This stage explains why it was decided to incorporate personal data in the first place.

---

## WEBSITES

- [https://www.researchgate.net/publication/286851196\\_User\\_awareness\\_of\\_social\\_media\\_security\\_The\\_public\\_sector\\_framework](https://www.researchgate.net/publication/286851196_User_awareness_of_social_media_security_The_public_sector_framework)
- <https://ieeexplore.ieee.org/document/8618220>
- <https://scholar.ui.ac.id/en/publications/impact-of-user-awareness-trust-and-privacy-concerns-on-sharing-pe>
- [http://www.scielo.org.za/scielo.php?script=sci\\_arttext&pid=S0038-23532018000300009](http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0038-23532018000300009)

---

## REFERENCES

- .2018 , V Paramarta, M Jihad, A Dharma , International Conference on Advanced Computer Science and Information Systems (ICACSIS)
- Damian Jackson; Paul Hayes , 2016 11th International Conference on Availability, Reliability and Security (ARES)
- J.Fenila Naomi; A. Vasanthageethan; G. Roshini; J.Sathish Kumar ,2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)
- S Kumar, V Somani , International Journal of Advance Research in ... , 2018- researchgate.net
- Senthil Kumar , Saravanakumar Kandasamy , 2016 Elsevier B.V. Peer-review under responsibility of organizing committee of the ICISP