International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 05, ISSN No. 2455-2143, Pages 38-54
Published Online September 2023 in IJEAST (http://www.ijeast.com)

USER AWARENESS OF SECURITY AND PRIVACY IN SOCIAL NETWORKING SITES

Triveni Krishnappa
School of Computing and Digital Media
London Metropolitan University, London
Engalnd, United Kingdom

Abstract— **The rapid expansion and widespread adoption of social networking sites have created new security and privacy challenges for individuals. This study will assess users' awareness of the security and privacy measures and their understanding of potential risks and vulnerabilities. The study uses a quantitative survey to collect data on users' perceptions, understandings, and experiences about security and privacy on social sites. The results will be analyzed to identify trends, knowledge gaps, and user perceptions, providing insight into the current landscape of user perceptions and insights. The outcome of this study will be useful in formulating plans and recommendations to improve security measures and promote responsible online behavior among social network administrators, policymakers, and users. This study aims to provide users with the necessary knowledge to adequately protect themselves in the digital age by highlighting their awareness and understanding of security and privacy on social networks.**

Keywords— **Security, Privacy, Attacks, Social Networking Sites (SNSs), Cybersecurity, Phishing**

I. INTRODUCTION

Technological advancements in recent years have led to the widespread use of social networking sites and fundamentally changed the way people connect, communicate, and share information. These platforms have seamlessly integrated into people's daily lives and offer many benefits and opportunities for social interaction and content sharing. However, the growing reliance on social media has led to serious security and privacy problems. Over the past decade, these platforms have experienced unprecedented growth, attracting billions of users worldwide. Platforms like Facebook, Twitter, and Instagram have revolutionized human-to-human interaction by fostering connectivity across geographic boundaries and facilitating the exchange of ideas, opinions, and personal information (AlMudahi et al., 2022). These websites provide a convenient and accessible way for individuals to stay in touch with friends, family, and acquaintances, improve social relationships, and facilitate the exchange of life experiences. Although social networks offer valuable opportunities for social interaction, they also raise significant security and privacy concerns (Hameed and Nafeesa Shameem Rahman, 2017). Users are willing to share large amounts of personal information, including interests, photos, location, and even sensitive data, without being fully aware of the potential risks involved. This growing digital footprint and the huge amount of personal information being shared on social media have increased the need to effectively address security and privacy issues. Main challenges in ensuring strong security and privacy on social networking sites is the lack of user awareness and understanding (Paramarta et al., 2018). Many users are unaware of the potential risks associated with sharing personal information on these platforms, as well as the impact of their privacy settings and data handling methods. Users' limited knowledge and understanding leaves them vulnerable to various security threats such as identity theft, phishing attacks, and unauthorized data access. Users' lack of awareness and understanding of security and privacy on social networks exposes individuals to significant risks and consequences (Alotaibi et al., 2021). Unauthorized entry of personal information can lead to identity theft, financial fraud, reputational damage, and potential personal security risks. In addition, the misuse of user data for personalized advertising and data analysis raises concerns about privacy violations and undermines individual autonomy. This study aims to expand users' knowledge and understanding of security and privacy on social networks. The results will help identify knowledge gaps, uncover factors that influence user behavior, and inform the development of strategies to improve user education and promote responsible safe, and confidential operations. The research is carried out with the following objectives:

- Assess users' understanding of security and privacy precautions on social networking sites.
- Examine user understanding of potential risks and consequences associated with inadequate security practices.
- Examine factors that influence user behavior and decision-making regarding security and privacy on social networking sites.
- Identify gaps and challenges in existing security and privacy education initiatives in social networking environments.

II. LITERATURE REVIEW

Social networking sites have grown in popularity in recent years, providing individuals with unprecedented opportunities to connect and communicate. However, this widespread adoption also leads to many security and privacy issues. Many studies have been done to test users' awareness and understanding of security and privacy on social networks. These studies have shown how important it is for users to be aware of the privacy settings available on these platforms and the potential risks associated with sharing personal information online. The results show that a significant percentage of social media users lack in-depth knowledge of the privacy options available, leading to the inadvertent disclosure of sensitive data. Data breaches pose a significant threat to the security and privacy of social media users. Data breaches and unauthorized access incidents have raised serious concerns about the protection of user data. Studies have looked at the impact of data breaches on popular social media sites and found a decline in user trust and engagement. The study emphasizes the need for strong authentication measures and security best practices to prevent unauthorized access and data breaches. Attackers attack vulnerabilities in these platforms and gain unauthorized access to user accounts and personal information (Baatarjav and Dantu, 2011). Such breaches can result in the disclosure of sensitive data, which can lead to identity theft, financial fraud, and reputational damage. The consequences of poor security practices on social networking sites are a matter of great concern. Weak passwords and lack of two-factor authentication have been identified as potential risk factors for unauthorized access and data breaches. Social networking sites often use unclear and ambiguous privacy policies and data sharing methods, leaving users unaware of how their personal information is collected, stored, and shared (Srilakshmi Voddelli, Sastry and Prasad, 2022). Data-sharing practices between social media platforms and third-party apps were analyzed, revealing instances of data sharing without explicit user consent. These regulatory loopholes can allow third-party programs or advertisers to access user data without explicit permission, which can lead to privacy and security data management issues. To better understand users' knowledge, attitudes, and behaviors, several studies have examined their perceptions and understandings of security and privacy on social networks. Users' understanding of privacy settings, security precautions, and the impact of personal information disclosure on social networking sites were examined in the study (Chen and Yamamoto, 2021). The results showed varying degrees of awareness, with some users not understanding the potential risks associated with their actions. Various factors influence user behavior regarding privacy on social networking sites. These include personal characteristics such as age, education, and technical knowledge, as well as contextual factors such as perceived benefits and risks of sharing personal data (Huang and Leu, 2020). Understanding these factors can aid in the development of effective interventions to increase user awareness and encourage responsible behavior online.

The social media environment is vulnerable to various threats and vulnerabilities that compromise user security and privacy. Studies have analyzed common security risks and vulnerabilities on social networks. These vulnerabilities include cross-site scripting (XSS), SQL injection, and poor coding practices. In addition, the integration of third-party applications into social media platforms has been identified as a potential risk as it can lead to data breaches and unauthorized access. Phishing attacks continue to pose a widespread threat to social networking sites, with attackers using phishing techniques to trick users into revealing sensitive information (Adil, Khan and Nawaz Ul Ghani, 2020). Social engineering tactics exploit users' trust and familiarity with their social networks, making them more vulnerable to such attacks. Malicious actors use social media as a middleman to spread malware and clickjacking attacks (Pal, Ghosh and Kar, 2023). By tricking users into clicking seemingly malicious links or downloading malicious content, an attacker can compromise a user's device and gain unauthorized access to personal information. Social networking sites provide a variety of privacy features and options to allow users to manage personal information and enhance security. These privacy settings allow users to adjust the visibility of their personal information and decide who can see their profiles, posts, and other shared content (Alan et al., 2022). By adjusting these settings, users can adjust their privacy settings to their comfort level. To increase security, social media platforms provide additional authentication measures, such as two-factor authentication (2FA) (Talwar, Chaudhary and Kumar, 2022). Encryption options are equally important for protecting user data from unauthorized access. User attitudes and actions have a significant impact on their approach to privacy and security on social media platforms. They should carefully consider the potential benefits and risks associated with sharing their personal information on these sites. The perceived benefits such as social connection and information sharing often outweigh the perceived risks (Dhawan, Singh and Goel, 2014). The effectiveness of security and privacy education initiatives in social media environments has been studied. The researchers evaluated in-app privacy guidelines and privacy-related notices as a method of informing users about privacy settings. These initiatives have shown promising results in positively influencing user privacy decisions and raising their awareness of privacy concerns. Understanding this insight can help develop interventions that emphasize the importance of responsible information sharing. Social norms and beliefs in social media platforms influence user privacy behavior. Users are more likely to follow applicable social norms regarding information disclosure and privacy protections (Miyaji, Hsu and Miyaji, 2022). The perceived reliability of a platform affects a user's willingness to share personal information. These studies highlight the importance of improving user training, implementing robust security measures, and ensuring transparent data handling policies. Addressing data breaches, unauthorized access, and loopholes in the privacy policy is critical to protecting users' data and their privacy in the digital age.

Security in Social Networking Sites

The security of social networking sites is essential because of the large amount of personal information shared and the potential for misuse. This is an important aspect that has a direct impact on user privacy, data protection, and online security in general (Knowledge Rusere et al., 2022). These platforms are now an integral part of our lives and facilitate communication, exchange, and collaboration with others. However, they also present a few security challenges that users and website operators must overcome to ensure a safe and enjoyable online experience. These platforms connect millions of users around the world, making them attractive targets for cybercriminals (Halder and Kule, 2023). Effective security measures are needed to protect user data, privacy, and overall online security. Some important aspects of security on social networking sites:

1. User Authentication and Access Control: Effective authentication methods such as two-factor authentication (2FA) play an important role in ensuring that only authorized people have access to user accounts. Social media platforms must have robust access control systems in place to prevent unauthorized login attempts.
2. Data Encryption: The implementation of encryption protocols such as HTTPS and SSL/TLS ensures that the data transmitted between the user and the social networking site remains confidential and cannot be easily intercepted by attackers.
3. Privacy Settings and Controls: Social networking sites must provide detailed privacy settings that allow users to customize who can see their posts, profile information, and other personal information. By providing clear and easy-to-use privacy controls, users can manage their security.
4. Secure Password Policies: Enforcing strict password policies and providing a password strength indicator can encourage users to choose complex and unique passwords, reducing the risk of unauthorized access.
5. Regular Software Updates and Patching: Social media platforms must regularly update their underlying software and systems with the latest security patches. This practice is key to patching vulnerabilities and preventing exploitation by malicious attackers.
6. User Education: Providing users with information about common security threats such as phishing and fraud can help them identify and avoid potential risks.
7. Fraud Prevention: Social networking sites should have mechanisms in place to detect and prevent fraudulent activity such as fake accounts or spam, and act quickly on suspicious behavior.
8. Third-Party App Permissions: When integrating third-party apps, social media sites must ensure that users know what data the app can access and provide clear options for revoking permissions.
9. Data Minimization: Collecting only necessary data from users and minimizing the amount of personal information stored can reduce the potential impact of a data breach.
10. Incident Response: A clearly defined incident response plan allows social media sites to quickly address security vulnerabilities, notify affected users, and take appropriate action to minimize the impact.
11. Transparency: Social networking sites should be transparent about their data collection, data sharing with third parties, and how user information is used.
12. User Reporting and Support: Providing an easy way to quickly report suspicious or abusive behavior. Responding to their concerns demonstrates a commitment to user safety (Nakerekanti and Narasimha, 2019).

Data Privacy in Social Networking Sites

Privacy on social networking sites is a significant concern due to the widespread collection, storage, and sharing of personal information on these platforms. This issue is of great importance because users reveal a lot of personal information on these platforms. Although social networks provide many tools for connecting and interacting with others, they also collect and store a significant amount of user data (Dhannuri et al., 2019). Privacy is of prime importance to protect users from potential threats such as identity theft, data breaches, and various forms of exploitation of their personal information. Users share various data including personal information, photos, messages, location information, etc. Ensuring data protection is essential to protecting user interests, maintaining trust, and preventing misuse of sensitive information. The most important aspects to consider when protecting data on social networks (Schubert and Marinica, 2019):

1. Data Collection and Consent: Social networking sites must be transparent about the types of data collected and how it is used. Users must give explicit consent before their data is collected, and they must have clear options to control the information they share.
2. Privacy Settings: Strong and easy-to-use privacy settings should be provided to allow users to customize who can access their profile. The default setting should prioritize privacy and limit public disclosure.
3. Data Usage and Sharing: User data should not be used beyond what they have consented to. Social networking sites should avoid sharing user data with third parties without explicit consent and the user must be able to revoke that permission.
4. Data Security: Robust security measures need to be implemented to protect user data from unauthorized access, data breaches, and hacking attempts. Encryption practices and secure storage are fundamental elements of data security.

5. User Control: Users must be able to access, modify, and delete their data. Explicit protocols must be provided for data access and data deletion requests.
6. Data Minimization: Social networking sites should only collect the minimum data necessary for their service. Unnecessary data should be avoided to limit the potential impact of a data breach.
7. Children's Privacy: Special safeguards must be taken to protect the privacy of minors. Parental consent is required to process children's data.
8. Cookie Policy: A clear and comprehensive cookie policy must be provided to inform users about the use of cookies for tracking and analytics purposes.
9. Data Breach Response: In the event of a data breach, the social network needs a clearly defined plan to notify affected users and authorities and take appropriate action to mitigate the impact.
10. Education and Transparency: Users must be made aware of privacy risks and best practices. Social networking sites should communicate their privacy guidelines to users.
11. Global Compliance: Taking into account worldwide user presence on social networking platforms, as well as adhering to numerous privacy rules and regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act).

Common threats and vulnerabilities in social networking environments

It is important to understand the common threats and vulnerabilities of social media platforms. This literature review is on common threats and vulnerabilities faced by users when using social media platforms. Cyber attackers are increasingly focusing on social media platforms as users reveal a lot of personal information. Common threats and vulnerabilities are (Tabassam et al., 2019):

- Phishing Attacks: Attackers use phishing tactics to trick users into revealing their login credentials or sensitive information, often through fake login pages or messages.
- Social Engineering: Social engineering techniques involve manipulating users into revealing sensitive information such as passwords or personal information by exploiting psychological vulnerabilities. Social networking sites provide a wealth of personal information that attackers can use to launch targeted social engineering attacks.
- Identity Theft: The abundance of personal information available on social media profiles leaves users vulnerable to identity theft. Cybercriminals can gather enough details to impersonate individuals or use their information for fraudulent purposes.
- Clickjacking: Clickjacking involves hiding malicious content behind legitimate links or ads. Users may unknowingly interact with these links, which may result in unintended actions such as sharing sensitive information.
- Unauthorized Access: Weak passwords and lax security practices can lead to unauthorized access to user accounts, resulting in potential misuse of personal information.
- Third-Party Application Risks: Users often grant permission to third-party apps to access their social media accounts. These apps may misuse or mishandle user data, posing a privacy risk.

Investigating common threats and vulnerabilities in the social media environment is key to increasing user awareness and understanding of potential risks. Knowledge of these risks can guide the development of targeted safety awareness and education campaigns. By educating users about these threats and providing actionable security measures, social media platforms can enable
users to protect their personal information, apply safer online practices, and contribute to a safer digital environment.

Common Threats (Brute force and Phishing attacks) on Social Networking Sites with the prevention methods

A brute force attack is a type of cyber-attack in which an attacker attempts to guess the correct credentials (username and password) to gain unauthorized access to a user's account on a social networking site. This attack method assumes that an attacker can eventually guess the correct credential combination by trying all combinations (Chapple and Seidl, 2021).

The process of a brute force attack on social networking sites typically includes the following steps:

- Target Selection: The attacker selects a specific user account on the social networking site that he wants to compromise.
- Username enumeration: An attacker can try to get the username of the target user in a variety of ways, such as through publicly available information in the user profile or by trying out common usernames.
- Password guessing: An attacker uses automated software or scripts to systematically try all possible password combinations to gain access to user accounts. These efforts may involve trying out common passwords, dictionary words, or alphanumeric combinations.
- Bypassing Rate Limiting: Many social networking sites implement a rate-limiting mechanism to block repeated login attempts after a certain number of failed attempts. To get around this, an attacker can use techniques such as a distributed network of compromised computers (botnets) to spread the attack to multiple sources.
- Successful Login: If an attacker can guess the username and password combination correctly, they will gain access to the targeted user account.

Preventing Brute Force Attacks:

Social networking sites implement various security measures to protect against brute force attacks. Some common strategies include:

- Account Lockout: After a certain threshold of unsuccessful login attempts, the account may be temporarily locked, preventing further login attempts for a certain period.
- CAPTCHA: Using CAPTCHA queries during login attempts can help distinguish between legitimate users and automated bots used in brute force attacks.
- Two-factor authentication (2FA): Enabling 2FA requires users to provide an additional factor of authentication (such as a one-time code sent to their mobile device) when entering a password, adding an extra layer of security.
- Strong password policies: Encouraging users to create strong, unique passwords can make brute force attacks more difficult.

Brute force attacks pose a significant threat to the security of user accounts on social networking sites. To mitigate this risk, social networking platforms must implement robust security measures, including account suspensions, CAPTCHA challenges, two-factor authentication, and strict password policies (Shetty et al., 2017). Educating users about the importance of using strong passwords and recognizing suspicious login attempts is essential for protection from brute force attacks.

A phishing attack is a form of cyber-attack in which an attacker attempts to trick users into revealing their sensitive information, including login credentials, personal information, or financial information. They achieve this by posing as a real entity or service on social networking platforms. Phishing attacks often use deceptive techniques to trick users into thinking they are interacting with a trustworthy source (Alharbi et al., 2022).

The process of a phishing attack on social networking sites typically includes the following steps:

- Creation of a Fake Page or Message: The attacker creates a fake login page or message that closely resembles the legitimate login page of the social networking site. This fake page can be hosted on a malicious website that the attacker controls, or it can be sent via phishing emails, direct messages, or social media posts.
- Deceptive message or email: The attacker creates a message or email -Mail that prompts the user to take an action, such as a claim that your account needs to be verified or there has been suspicious activity on your account. The message often contains a link to the fake login page.
- User Interaction: The attacker sends the phishing email or message to many users in the hope that some will click on the provided link. When users click on the link, they are redirected to the fake login page.
- Information Disclosure: Unsuspecting users may enter their login credentials on the fake login page thinking it is an authentic social networking site. However, your credentials will be captured by the attacker.
- Unauthorized Access: Using the user's credentials, the attacker gains unauthorized access to the user's social networking account.

Preventing Phishing Attacks:

Social networking sites implement various security measures to prevent phishing attacks and protect their users. Common prevention strategies include (Jamil et al., 2018):

- Phishing Detection: Social networking platforms use algorithms and machine learning techniques to detect and block malicious links and messages related to phishing attacks.
- Account recovery protocols: If a user's account is compromised, such as through phishing, the platform may have account recovery processes in place to help users regain control of their accounts. User education: Platforms often provide users with education and guidance about the risks of phishing attacks and how to recognize and avoid them.
- Multi-Factor Authentication: Implementation of Multi-factor authentication (MFA) increases security by requiring users to provide an additional authentication element in addition to their password. This measure reduces the likelihood of unauthorized access, even in cases where credentials have been compromised.
- Report and flag: Social networking sites encourage users to report suspicious messages or accounts so platforms can crack down on potential phishing attempts.

Phishing attacks pose a significant threat to social network users as attackers attempt to trick them into revealing sensitive information. To combat phishing, social networking platforms implement security measures such as phishing detection, account recovery protocols, user training, multi-factor authentication, and reporting mechanisms. User awareness and vigilance are also crucial to detect and prevent falling victim to phishing attacks on social networking sites.

Understanding Users' Perceptions and Behaviors

Understanding users' perceptions of privacy risks is key to determining their awareness and understanding of security and privacy on social networks. Several studies have examined users' perceptions of the risks associated with sharing personal information on these platforms. Zheng and Ariyo surveyed to examine users' perceptions of privacy risks on social networking sites. The study revealed that a significant number of users were aware of potential risks such as unauthorized access, data breaches, and identity theft. However, there are differences in risk perception among different user demographics, with younger users having a lower level of concern. The privacy settings and controls provided by social networks play an important role in allowing users to manage their privacy. A study by Chen and Li looked at users' use of privacy settings on social networking sites. The results show that while most users are aware of privacy settings, their understanding of how to configure and customize these settings is limited. Users often rely on default settings without fully understanding the impact on their privacy. The practices of sharing and disclosing information on social networking sites affect user privacy. Hideaki examined users' information sharing practices on social networking sites. Research shows that users are more likely to share personal information due to factors such as social connections, perceived benefits of sharing, and the influence of friends. However, users' understanding of the potential risks associated with information disclosure is different and some users show a lack of awareness.

Studying users' privacy behavior provides insight into proactive measures to protect their privacy on social networking sites. A study conducted by M. Singh examined the privacy behavior of social media users. Research has identified factors such as privacy concerns, perceived control over personal information, and knowledge of privacy settings as factors that influence user behavior. The study also highlights the importance of educational initiatives and user-friendly interfaces to promote privacy-respecting behaviors. Overall, the study emphasizes the importance of understanding users' perceptions of privacy risks, use of privacy settings and controls, information sharing practices, and privacy behavior. These factors contribute to an understanding of user perception and understanding of security and privacy on social networks.

Strategies for Enhancing Security and Data Privacy Awareness

Existing policies and initiatives provide valuable insight into efforts to increase user awareness and understanding of security and privacy on social networks. The researchers examined different approaches taken by organizations, policymakers, and industry players to address privacy issues. A review was conducted of existing policies and initiatives implemented by the social network to raise privacy awareness. Research has identified measures such as improved privacy settings, user training resources, and transparency reports as common strategies used by platforms to empower users and promote a culture of privacy. Education and awareness campaigns play an important role in promoting user understanding and awareness about security and privacy on social networks. In a study by Ben Salamah, the impact of an education campaign on social media users' data protection awareness was examined. The results showed that targeted educational interventions significantly improved users' understanding of privacy risks, their ability to navigate privacy settings, and their adoption of privacy practices. The look and design of social networking sites can influence users' awareness and understanding of privacy. The research found that clear and intuitive privacy settings, simplified privacy settings, and visual cues within the interface positively influence users' awareness and control over their data.

Regulatory interventions play a crucial role in protecting data privacy on social networks. A study by Layton and Elaluf-Calderwood analyzed the influence of regulatory interventions on users' privacy awareness. The research highlighted the importance of strong privacy regulations, transparency requirements, and enforcement mechanisms to promote user awareness and hold social networks accountable for privacy practices. Collaboration between social networking sites and users is key to promoting a culture of privacy and increasing user awareness. Cengiz, Kalem, and Boluk examined collaborative efforts between social networking sites and users to improve privacy. The study highlights the importance of user feedback mechanisms, bug bounty programs, and user-driven feature development to promote transparency, trust, and user empowerment. A literature review of existing policies and initiatives, education and awareness campaigns, user interface and design considerations, policy interventions, and regulatory as well as collaborative efforts provide valuable insights to improve user awareness and understanding of security and privacy in social networks.

User Comprehension of Risks and Consequences

To improve privacy and security on social networking sites, users must understand the potential risks and consequences associated with poor security practices (Yadagiri Vamsi Krishna et al., 2023). The study determines how well users understand the risks and consequences associated with poor security practices on social networking sites. This helps to find out if users are aware of security vulnerabilities that could lead to data breaches or unauthorized access to their accounts (Zboil, Syrovtkov, and Pavlicek, 2022). Some users may not fully understand the impact of using weak passwords or underestimate the importance of regularly updating their privacy settings. Others may have misconceptions about the level of security offered by social media platforms, assuming that their personal information is fully protected without additional precautions. Recognizing these misconceptions or gaps in understanding is critical to designing targeted educational interventions to address knowledge gaps. By eliminating these misconceptions, social media platforms can enable users to take more proactive steps to protect their data and improve their overall online safety (Nuchitprasitchai, Kilanurak and Porrawatpreyakorn, 2020). Identifying common misconceptions and gaps in understanding underpins the development of appropriate educational initiatives that enable users to make more informed decisions about their safety online. By improving users' understanding of risks and consequences, social media platforms can create a safer online environment and foster a more privacy-conscious user community.

Factors Influencing User Behavior and Decision-Making

Understanding the various factors that influence user behavior and decision-making on social networking sites is key to developing effective strategies to improve privacy and data security. Personal factors play an important role in shaping user behavior and decision-making on social networking sites (Dimitrios Amanatidis, Ifigeneia Mylona, and Dossis, 2022). Studies have examined how personality traits such as openness to experience, and conscientiousness affect users' willingness to share personal information online. Cognitive biases such as optimism or the illusion of control can lead users to underestimate the potential risks associated with their online activities. Understanding the impact of individual characteristics on user behavior can help develop tailored education and intervention programs to meet specific needs and promote better security practices.

Social factors also have a significant influence on user behavior on social networking sites. Studies have looked at how social norms, peer influence, and social comparison influence users' privacy and security decisions. Social norms can determine what behavior is considered acceptable in a social network and influence users' decisions about sharing personal information and adjusting privacy settings. Peer influence and social comparison play a role in shaping user behavior, as individuals tend to adapt their actions to behavior in their social environment, including privacy options and security measures (Elistina Abu Bakar, Nur Jannah Draman and Aznan Zuhid Saidin, 2018). Contextual factors in the online environment also influence user behavior and decision-making. User interface design and usability of privacy settings can significantly affect how users manage their privacy settings. An intuitive and user-friendly interface can empower users to make informed decisions. Default settings on social media platforms can greatly affect users' privacy practices, as many users tend to keep the default options without actively adjusting their privacy settings. Understanding the influence of contextual factors can help platform designers and policymakers create an environment that supports better security and privacy practices. Personal characteristics, social influences, and contextual factors all play a role in shaping user privacy and security decisions and practices. With these factors, platforms can design appropriate interventions and user-friendly interfaces to enable users to make informed decisions about their privacy, thereby creating a safer online environment.

Factors Influencing Data Privacy Awareness

The factors that influence the privacy perception of social media users are very important in determining their awareness and understanding of security and privacy. Several studies have looked at different factors influencing user awareness in this context. Sutarno conducted a comprehensive analysis of the factors influencing the privacy awareness of social network users. The study identified factors such as personal experience with data breaches, education, and perceived trustworthiness of social media platforms as key drivers of awareness. These findings highlight the importance of considering these factors to raise awareness about privacy. Demographic factors play a role in users' awareness and understanding of privacy on social networks. The relationship between demographics and privacy awareness has been established to identify possible variations and trends. In a study by Alotaibi, the link between demographics and data protection awareness of social network users was examined. Research has found that factors such as age, gender, and education level are associated with varying degrees of privacy awareness. Younger users and more educated users tend to exhibit higher levels of awareness and understanding. Media literacy and digital skills are essential factors contributing to increasing users' awareness and understanding of data protection in the context of social networks. Alobaid and Ramachandran examined the influence of media literacy and digital skills on social media users' privacy perceptions. The results show that people with a higher level of media and digital literacy are more likely to exhibit greater awareness of privacy issues and engage in privacy-protective behaviors. The transparency of the privacy policy and the complexity of the user agreement are important factors affecting users' awareness and understanding of privacy on social networks. A study by Yang, Yu Jie Ng, and Vishwanath analyzed the transparency of privacy policies and the complexity of user agreements concerning users' privacy awareness. The study shows that clear and transparent privacy policies, combined with simplified user agreements positively influence users' understanding of privacy and the ability to make informed decisions about their data. Understanding the factors that influence privacy awareness, the relationship between demographics and awareness, the influence of social network usage patterns, the impact of media literacy and digital skills, as well as the role of privacy policy transparency and user agreement complexity contributes to a comprehensive understanding of user awareness and understanding of security and privacy in social networks.

User Experiences and Incidents

User experience related to a security breach, or a social data breach is key to understanding the true impact of inadequate data protection. Studies are conducted to investigate user incidents related to security or data breaches on social networking sites. These incidents may include data breaches, unauthorized access to user accounts, identity theft, cyberbullying, or disclosure of sensitive personal information. By real-world incidents, we can gain valuable insights into the vulnerabilities and risks of social media platforms and provide insights into areas of concern. User experience analysis allows us to understand the emotional and psychological impact of security and privacy incidents. Studies look at how these incidents affect users' feelings of vulnerability, their distrust of social media platforms, and their general attitudes toward privacy private. These responses provide valuable insights into users' resilience and adaptability to security and privacy challenges (Winter et al., 2020). User experience also affects their perception of accountability and the responsiveness of social media platforms to security and privacy issues. Studies examine users' trust in the platform's ability to protect their data and how these experiences affect future user interactions and willingness to share information online. The role of the media and communication channels in disseminating information about these incidents is crucial as it can significantly affect public perception of safety measures. Investigating user incidents involving security breaches or social media breaches helps to better understand the true impact of inadequate data protection. By analyzing user experiences, we gain insight into the emotional impact of security incidents and the factors that influence users' perceptions of security and privacy. Understanding users' reactions to incidents and their trust in social media platforms can help develop effective incident response protocols and proactive measures to improve data protection. In addition, considering the role of media in shaping public awareness helps create a safer and more transparent online environment, thereby increasing users' trust in media platforms. society and their engagement with their private lives.

Evaluation of Existing Security and Privacy Education Initiatives

Ensuring users' awareness and understanding of security and privacy on social networks is crucial to protecting personal data and mitigating potential risks. The initiatives may include in-app tutorials, privacy notifications, interactive quizzes, and privacy educational resources. Studies have evaluated the availability and accessibility of these educational initiatives within the platforms. They also examine the level of integration and visibility of privacy and security resources to determine whether users can easily access and interact with them. Evaluating the effectiveness of educational materials in teaching essential security and privacy concepts is critical to understanding their impact on user awareness (Ivaschenko et al., 2018). By assessing existing security and privacy education initiatives, the reviewers identified various gaps and challenges that need to be addressed to improve user awareness and understanding. A common challenge is the lack of exposure to educational resources. Users may ignore or opt out of in-app tutorials or privacy notifications, resulting in limited access to important information. Studies have highlighted the need for more user-friendly and interactive teaching materials. Static or overly complex resources may not capture users' attention and may not effectively convey important security and privacy concepts. For example, users may receive guidance on basic privacy settings but lack information on how to recognize and respond to phishing attempts or identify potential data breaches. Another identified gap is the limited adaptation of educational content to the diverse user base (Patil and Arra, 2022). Adapting educational materials to different user demographics and user levels can increase their relevance and effectiveness. Additionally, studies have shown the importance of reinforcing educational messages over time. A single guide or notification may not be enough to create lasting changes in user behavior. Assessing the effectiveness and identifying gaps and challenges of these initiatives can guide the development of more robust and user-centered educational resources. These identified challenges on social networking platforms can improve users' overall awareness of security and privacy, empower users to make informed decisions and improve their online security.

User Practices

Understanding common user practices and behaviors that can contribute to security and privacy risks on social networks is critical to improving user security and privacy. The studies focus on examining prevailing user practices and identifying areas for improvement in user behavior and security practices (Mccloskey and Herbert, 2019). Some common practices include:

- Oversharing of Personal Information: Users may accidentally share excessive personal information on social media platforms, such as their full name, address, phone number, or date of birth, which can increase the risk of identity theft and targeted attacks.
- Weak passwords: Many users still use passwords that are weak or easy to guess, making it easier for attackers to gain unauthorized access to user accounts.
- Failure to adjust privacy settings: Failure to adjust privacy settings or understand the impact of default settings may expose user information to a wider audience than intended.
- Interaction with suspicious links: By clicking on malicious links or downloading files from dubious sources Users can fall victim to phishing scams.
- Trust unknown contacts: Accepting friend requests or interacting with unknown contacts can lead to unauthorized access to personal information or targeted social media attacks.
- Third-party app permissions: Users may grant excessive permissions to third-party apps without fully understanding the scope of data access they provide.

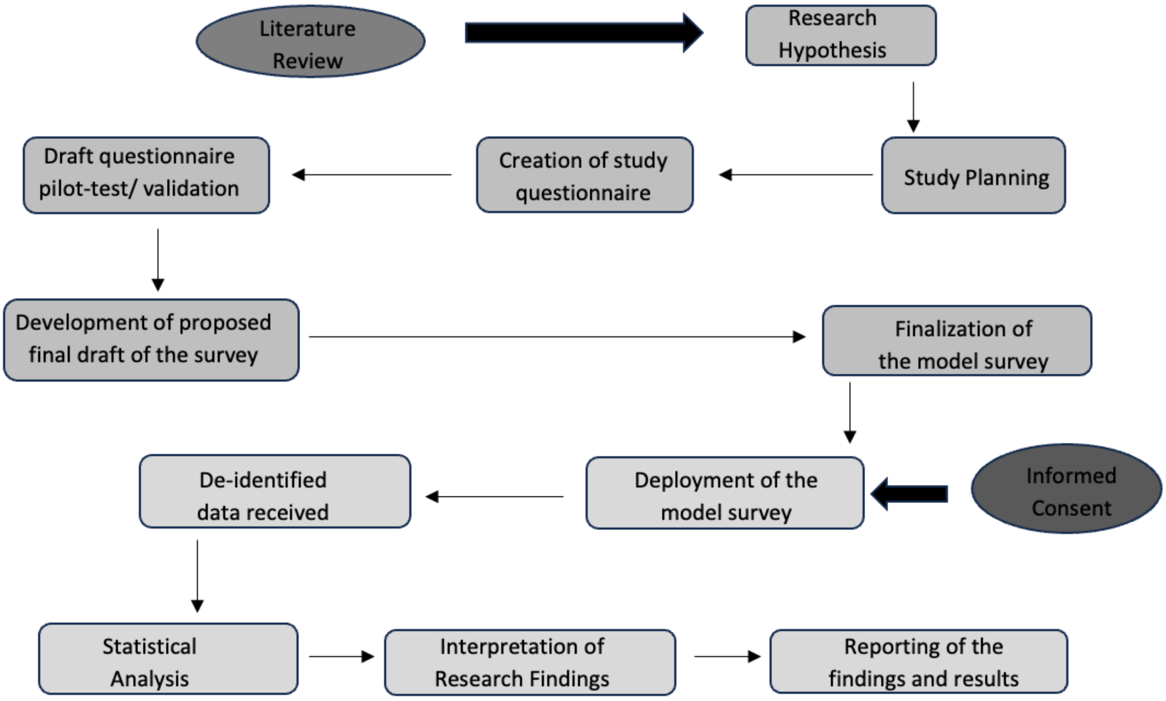
Based on the research, several areas of improvement have been identified to improve user privacy and security practices (Kurniawan et al., 2021):

- Security Education: An increased focus on user education and awareness campaigns is needed to inform users about the risks involved in common practices and how to adopt safer behaviors.
- Password policies: Platforms can implement stricter password policies and provide password strength indicators to encourage users to create stronger passwords.

- Privacy Settings: Social networks can improve the clarity and usability of privacy settings interfaces, helping users manage their information more effectively.
- Improved phishing detection: Implementing advanced phishing detection mechanisms can prevent users from interacting with suspicious links and messages.
- Two-Factor Authentication (2FA): Encouraging users to enable 2FA can significantly improve the security of their accounts and protect against unauthorized access.
- Data access transparency: By providing clear and understandable explanations of third-party app permissions, users can make more informed decisions about granting access to their data.

Strengthening security education, implementing robust password policies, and improving privacy settings customization can empower users to take proactive steps in safeguarding their personal information online.

III. METHODOLOGY


Literature Review
Research Hypothesis
Study Planning
Creation of study questionnaire
Draft questionnaire pilot-test/ validation
Development of proposed final draft of the survey
Finalization of the model survey
Informed Consent
Deployment of the model survey
De-identified data received
Statistical Analysis
Interpretation of Research Findings
Reporting of the findings and results

This study will use mixed methods that integrate both quantitative and qualitative techniques for literature review and data collection. It will consist of two main components - assessing user awareness and understanding through surveys, and interviews. The study is aimed at a diverse group of social media users. A sample size of 100 participants was recruited. Participants were selected based on demographic factors such as age, gender, and level of social media usage to ensure that different user profiles are represented.

Data Collection: A structured questionnaire was developed to assess user awareness and understanding of security and data privacy measures in social networking sites. The survey will include questions about knowledge of security features, privacy settings, password strength, and responses to potential risks. The survey was administered electronically using online survey platforms and through in-person data collection.

Ethical Considerations: Informed consent from participants was obtained providing a thorough explanation of the research objectives, processes, possible risks, and confidentiality safeguards. The protection of participant's personal data and maintenance of anonymity in reporting and data analysis was ensured. Ethical approval was obtained from the research supervisor of the University ensuring compliance with ethical guidelines and principles.

Limitations: Limitations may include potential biases in participants' self-reporting, generalizability of findings to a broader population.

IV. RESULTS AND FINDINGS

- Overview of demographic characteristics of participants:

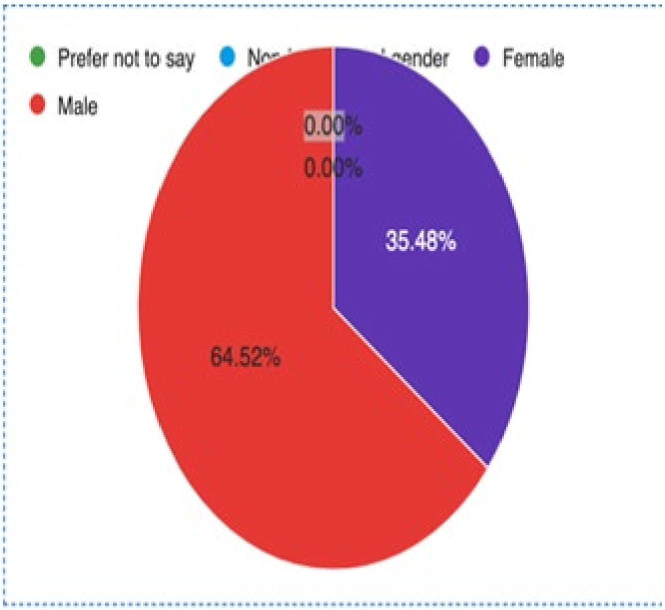


Figure: What is your gender?

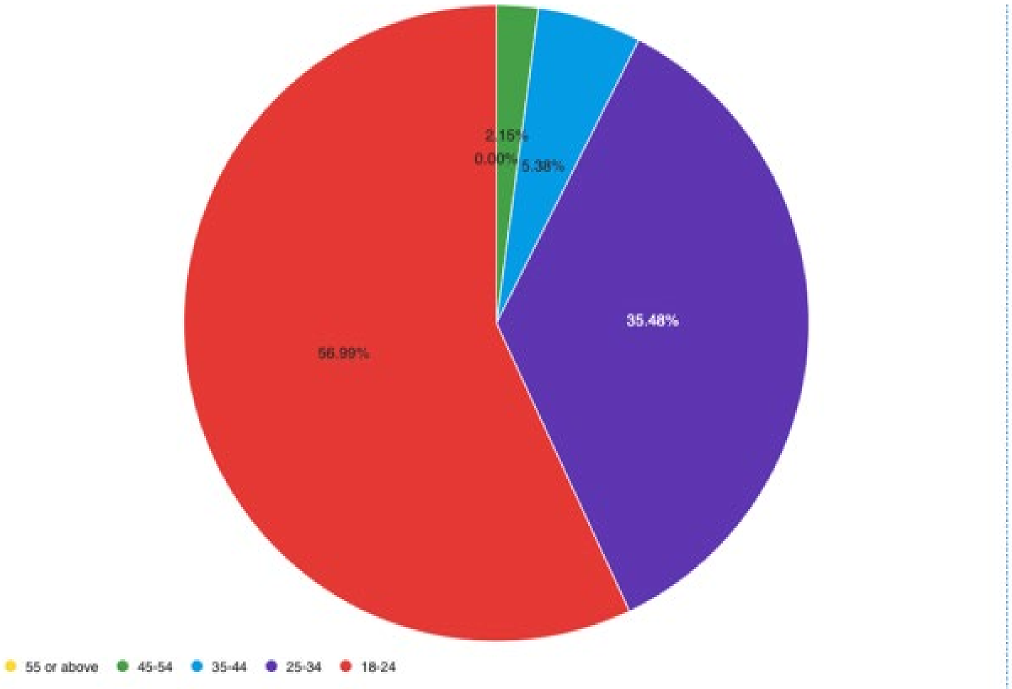


Figure: What is your age?

The survey was completed by a diverse group of participants. Out of the total respondents (100), 64.52% were male, and 35.48% were female. The age distribution was as follows: 18-24 years (56.99%), 25-34 years (35.48%), 35-44 years (5.38%), and 45+ years (2.15%). The participants represented various educational backgrounds.

- Summary of responses related to security and data privacy awareness:

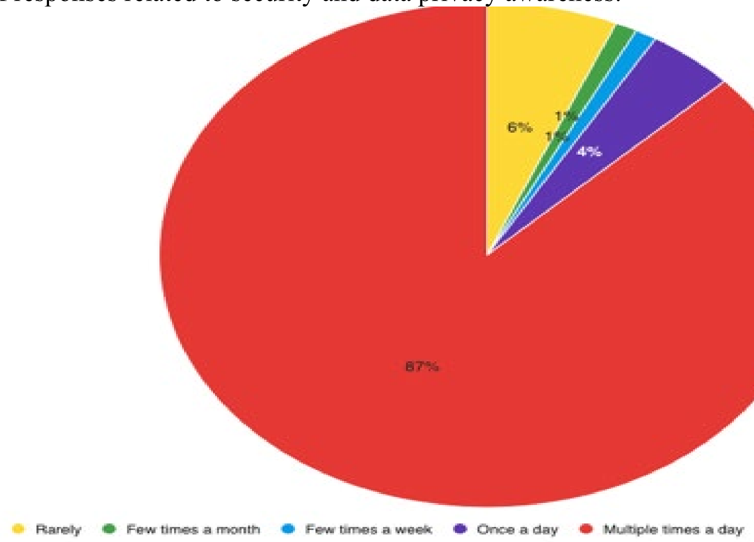


Figure: How often do you use social networking sites?

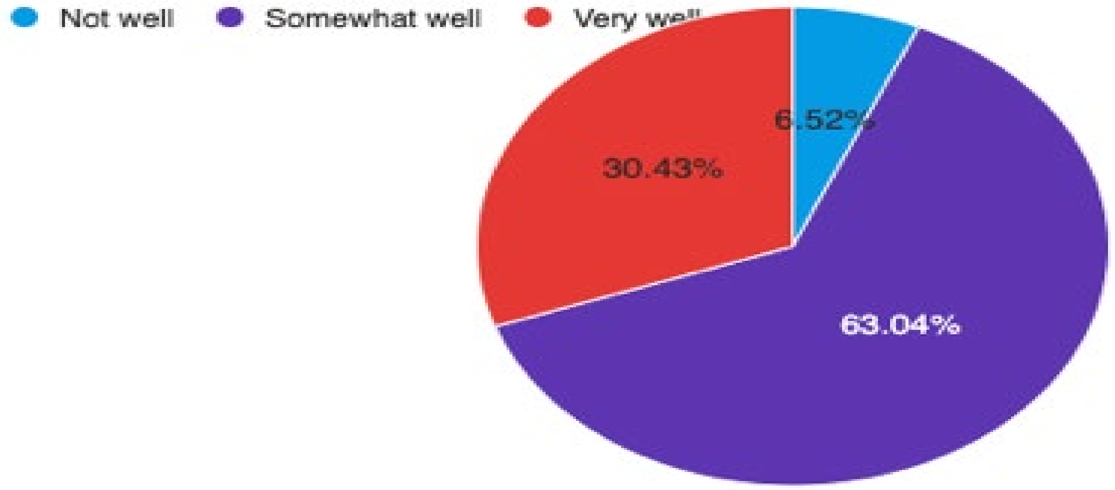


Figure: How well do you understand the privacy settings?

The survey included questions to assess participants' awareness of security and data privacy in social networking sites. The results indicated that 87% of respondents use social networking sites often. However, only 30.43% of participants reported having a good understanding of data privacy settings and how to manage them effectively.

- Frequency and impact of different types of attacks

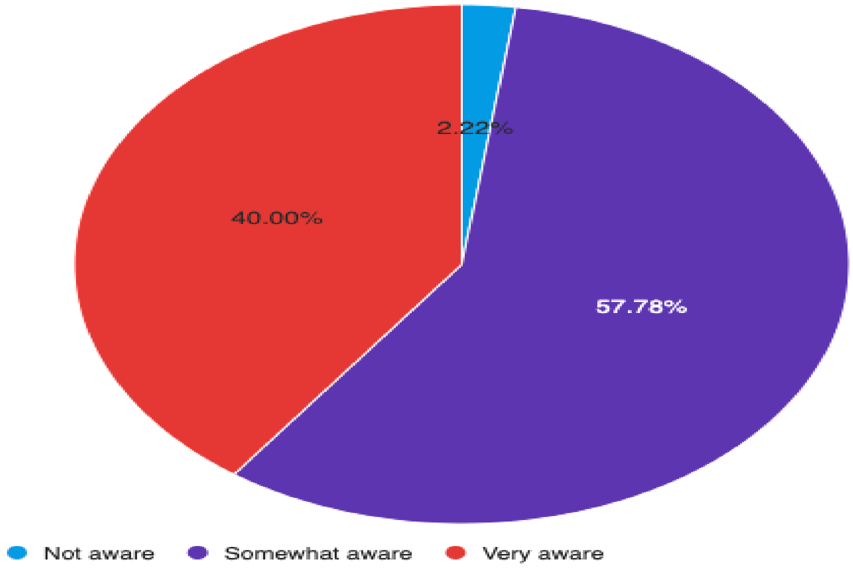


Figure: How aware are you of the security and privacy issues?

Participants were asked about their experiences with various security threats on social networking sites. The most reported types of attacks were phishing attempts, followed by malware infections and account hacking incidents. These attacks had varying levels of impact, with only 40% of respondents stating that they are aware of the incidents and risks taking place on social networking sites.

- Users' experiences with security incidents

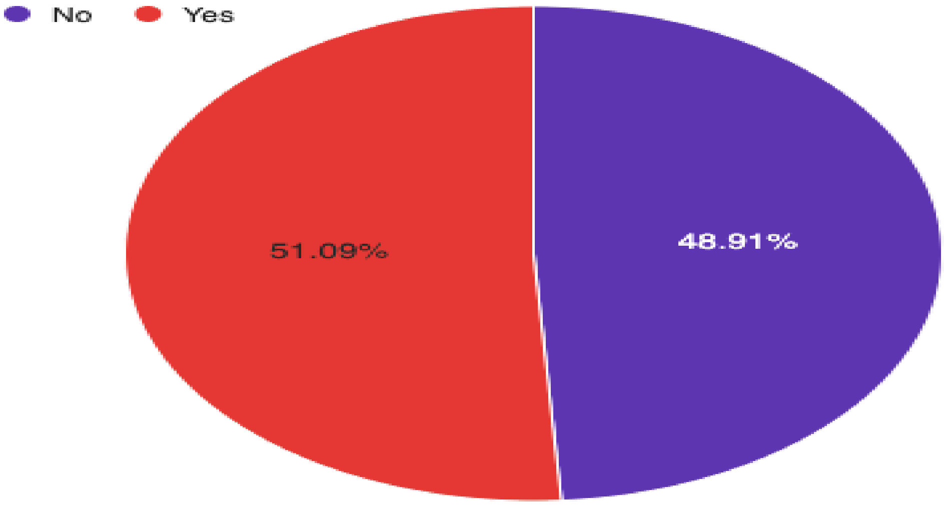


Figure: Have you encountered privacy or security incidents while using SNSs?

A significant portion of the respondents reported experiencing at least one security incident on social networking sites. Among them, 51.09% have encountered one or the other kind of incident. These incidents had a significant impact on users' trust in the platforms and their overall perception of data privacy.

- Evaluation of participants' comprehension to control the visibility of personal data

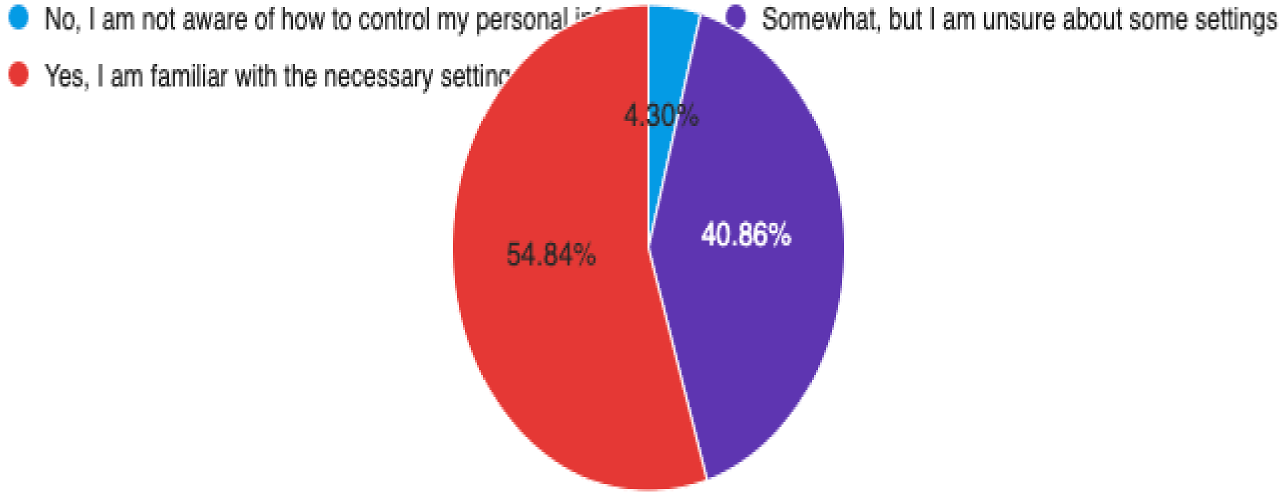


Figure: Do you know how to control the visibility of your personal information and limit access to your data on SNSs?

The survey included questions to evaluate participants' knowledge of privacy settings available on social networking sites. The findings revealed that 54.84% of respondents were familiar with the basic privacy settings, such as controlling the visibility of posts and profile information. However, 40.86% of participants were not aware of more advanced privacy features, such as two-factor authentication and encryption options.

- Exploration of motivations and concerns related to data sharing

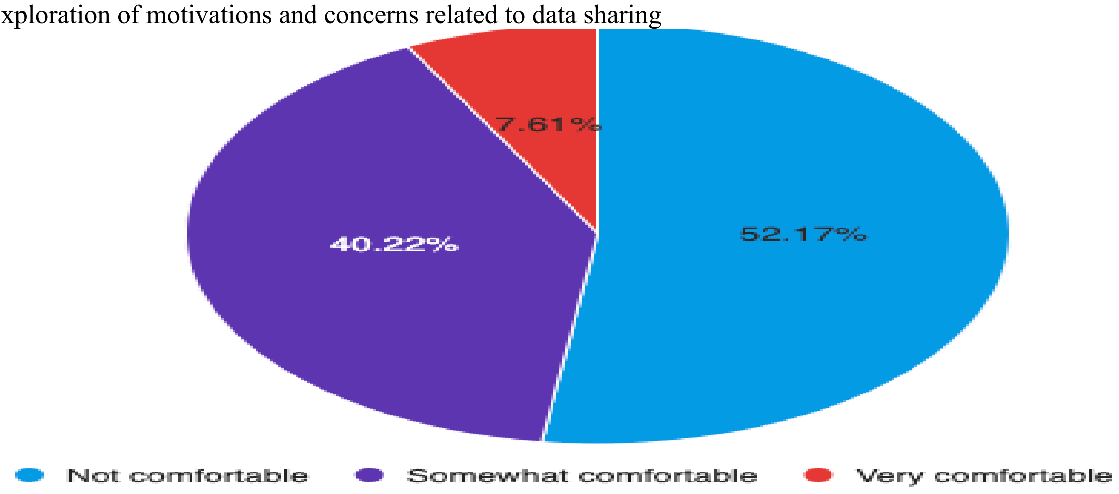


Figure: How comfortable are you with collection, use and sharing your personal data by SNSs?

Participants were asked about their motivations and concerns when sharing personal information on social networking sites. The analysis showed that while 40.22% of respondents were comfortable sharing their information to connect with friends and family, 52.17% expressed concerns about potential misuse of their data and privacy violations by third parties.

- Investigation of password management and privacy-enhancing actions

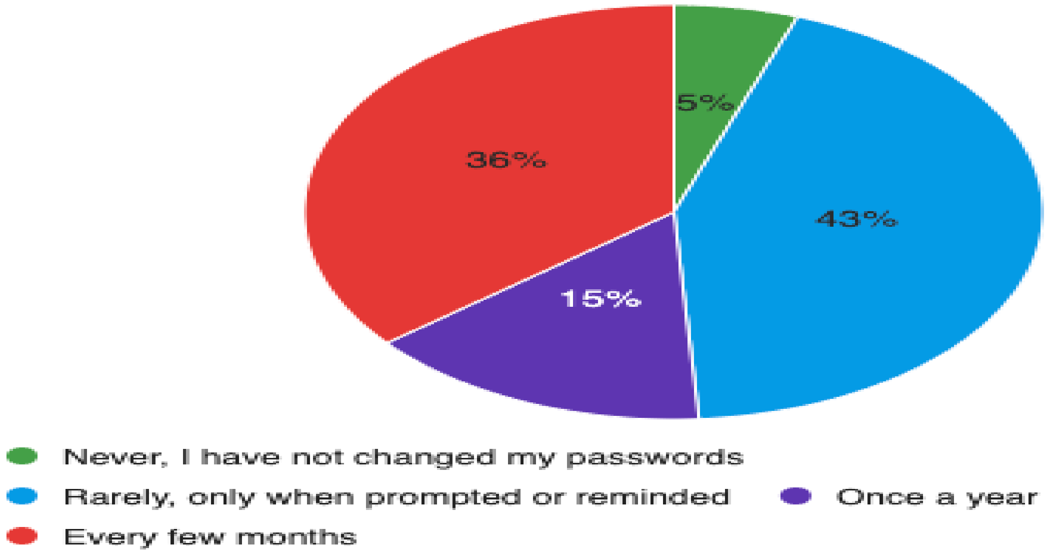


Figure: How often do you change your passwords for SNSs?

The survey included questions regarding participants' password management practices and actions taken to enhance their privacy on social networking sites. The results indicated that 36% of respondents used unique, strong passwords and changed them every few months while 43% of respondents changed passwords only when prompted.

- Analysis of responses related to trust in platforms and social norms.

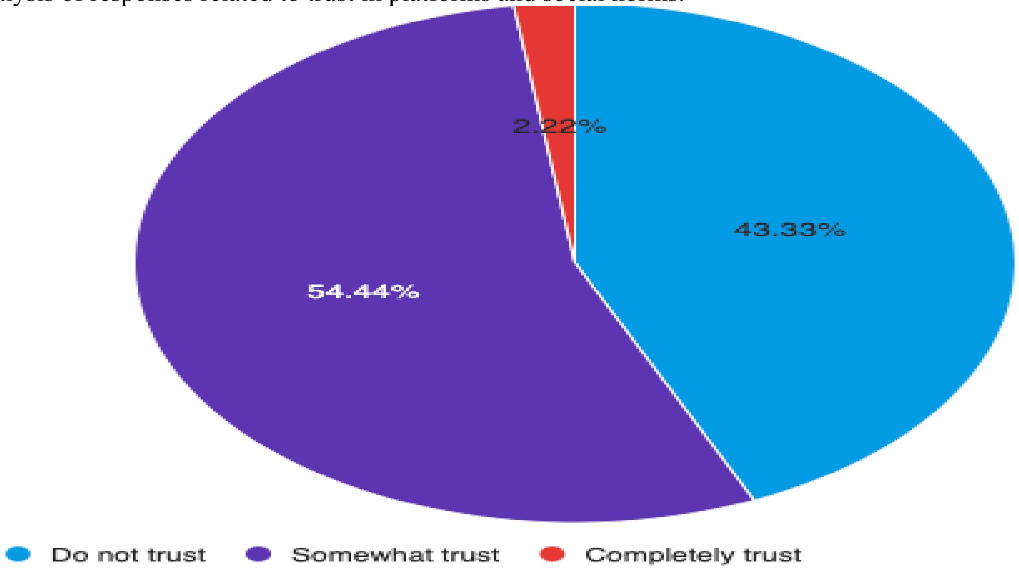


Figure: How much do you trust SNSs to protect your personal data?

Participants' responses regarding trust in social networking platforms and adherence to social norms were examined. The findings revealed that 54.44% of respondents expressed a moderate level of trust in platforms' data privacy practices, while 43.33% reported a low level of trust. However, only 2.22 % of participants indicated that their privacy decisions were influenced by social norms and the behavior of their peers on these platforms.

The survey findings highlighted the need for improved security and data privacy awareness among users of social networking sites. The results revealed gaps in knowledge, awareness, and understanding, as well as the prevalence of security incidents and privacy concerns. Understanding the factors influencing user behavior and addressing these issues can contribute to the development of effective strategies and interventions to enhance users' awareness and understanding of security and data privacy in social networking sites.

V. CONCLUSION

This study's findings confirm and extend previous research in the field. Researchers have found similar results regarding the lack of user awareness and understanding of security and data privacy on social networking sites, supporting the confirmation of previous research results (Erfan Aghasian, Garg and Montgomery, 2019). However, the current study also brings novel insights by identifying gaps in knowledge and understanding that have not been extensively explored in the literature.

The results of this study hold considerable significance for the different parties involved. To begin with, it underscores the critical need to address user awareness and comprehension concerning security and data privacy when using social networking platforms. Users should be empowered with the requisite knowledge and abilities to make informed choices and safeguard their personal information. Secondly, the study highlights the potential consequences of inadequate security measures, such as data breaches and unauthorized access. These consequences can have severe impacts on users, ranging from identity theft to financial loss. This underscores the urgency for social networking platforms to prioritize robust security measures and protect user data. Policymakers should consider these findings when formulating regulations and guidelines to protect user privacy and promote data security on social networking sites. The evaluation of existing privacy and security education initiatives reveals valuable insights regarding users' engagement with educational resources. The study identifies several shortcomings and areas for improvement, including the need for more comprehensive educational campaigns that address advanced data privacy topics.

VI. REFERENCE

[1] Adil, M., Khan, R. and Nawaz Ul Ghani, M.A. (2020). Preventive Techniques of Phishing Attacks in Networks. 2020 3rd International Conference on Advancements in Computational Sciences (ICACS). doi:https://doi.org/10.1109/icacs47775.2020.9055943.

[2] Alan, A., Al-Arnaout, Z., Topcu, A., Zaki, C., Shdefat, A. and Elbasi, E. (2022). How Do Default Privacy Settings on Social Media Apps Match People's Actual Preferences? 2022 International Conference on Electrical and Computing Technologies and Applications (ICECTA). doi:https://doi.org/10.1109/icecta57148.2022.9990282.

[3] Alharbi, A., Alotaibi, A., Alghofaili, L., Alsalamah, M., Alwasil, N. and Elkhediri, S. (2022). Security in Social-Media: Awareness of Phishing Attacks Techniques and Countermeasures. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICCIT52419.2022.9711640.

[4] AlMudahi, G.F., AlSwayeh, L.K., AlAnsary, S.A. and Latif, R. (2022). Social Media Privacy Issues, Threats, and Risks. [online] IEEE Xplore. doi:https://doi.org/10.1109/WiDS-PSU54548.2022.00043.

[5] Alobaid, M. and Ramachandran, R. (2021). A Social Media Case Study on the Impact of Disinformation on Business and Consumers. [online] IEEE Xplore. doi:https://doi.org/10.1109/CONISOFT52520.2021.00035.

[6] Alotaibi, S., Alharbi, K., Alwabli, H., Aljoaey, H., Abaalkhail, B. and Khediri, S.E. (2021). Threats, crimes and issues of privacy of users' information shared on online social networks. [online] IEEE Xplore. doi:https://doi.org/10.1109/ISNCC52172.2021.9615815.

[7] Baatarjav, E.-A. and Dantu, R. (2011). Current and Future Trends in Social Media. 2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing. doi:https://doi.org/10.1109/passat/socialcom.2011.125.

[8] Ben Salamah, F., Palomino, M.A., Papadaki, M. and Furnell, S. (2022). The Importance of the Job Role in Social Media Cybersecurity Training. 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). doi:https://doi.org/10.1109/eurospw55150.2022.00054.

[9] Cengiz, A.B., Kalem, G. and Boluk, P.S. (2022). The Effect of Social Media User Behaviors on Security and Privacy Threats. IEEE Access, 10, pp.57674–57684. doi:https://doi.org/10.1109/access.2022.3177652.

[10] Chapple, M. and Seidl, D. (2021). CompTIA Security+ deluxe study guide : exam SY0-601. Indianapolis: Sybex.

[11] Chen, H. and Yamamoto, Y. (2021). Task-based Assessment to Evaluate Instagram Users' Capabilities for Personal Information Leakage Prevention. 10th International Congress on Advanced Applied Informatics (IIAI-AAI). doi:https://doi.org/10.1109/iiai-aai53430.2021.00005.

[12] Chen, H.-Y. and Li, C.-T. (2022). Predicting and Analyzing Privacy Settings and Categories for Posts on Social Media. IEEE International Conference on Big Data (Big Data). doi:https://doi.org/10.1109/bigdata55660.2022.10020677.

[13] Dhannuri, S.P., Sonbhadra, S.K., Agarwal, S., Nagabhushan, P., Syafrullah, M. and Adivarta, K. (2019). Privacy Control In Social Networks By Trust Aware Link Prediction. [online] IEEE Xplore. doi:https://doi.org/10.23919/EECSI48112.2019.8977087.

[14] Dhawan, S., Singh, K. and Goel, S. (2014). Impact of privacy attitude, concern and awareness on use of online social networking. [online] IEEE Xplore. doi:https://doi.org/10.1109/CONFLUENCE.2014.6949226.

[15] Dimitrios Amanatidis, Ifigeneia Mylona and Dossis, M. (2022). Social Media and Consumer Behaviour: Exploratory Factor Analysis. doi:https://doi.org/10.1109/seeda-cecnsm57760.2022.9932979.

[16] Elistina Abu Bakar, Nur Jannah Draman and Aznan Zuhid Saidin (2018). Value, Religiosity and Behaviour in Social Media. doi:https://doi.org/10.1109/ict4m.2018.00017.

[17] Erfan Aghasian, Garg, S. and Montgomery, J. (2019). User's privacy in recommendation systems applying online social network data: a survey and taxonomy. pp.259–282. doi:https://doi.org/10.1049/pbpc035f_ch12.

[18] Halder, P. and Kule, M. (2023). Security Attacks on Social Networking: A Review. doi:https://doi.org/10.1109/isdcs58735.2023.10153551.

[19] Hameed, K. and Nafeesa Shameem Rahman (2017). Today's social network sites: An analysis of emerging security risks and their counter measures. 2017 International Conference on Communication Technologies (ComTech). doi:https://doi.org/10.1109/comtech.2017.8065764.

[20] Huang, L. and Leu, J.-D. (2020). Relative Importance of Determinants Towards Users' Privacy Disclosure on Social Network Sites by Privacy Invasion Experience Based on Construal Level Theory. IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). doi:https://doi.org/10.1109/ieem45057.2020.9309833.

[21] Huber, M., Mulazzani, M., Weippl, E., Kitzler, G. and Goluch, S. (2011). Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam. IEEE Internet Computing, 15(3), pp.28–34. doi:https://doi.org/10.1109/mic.2011.24.

[22] ico.org.uk. (2023). Data Protection and the EU. [online] Available at: https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/.

[23] ISO (2022). ISO/IEC 27001 standard – information security management systems. [online] ISO. Available at: https://www.iso.org/standard/27001.

[24] Ivaschenko, A., Anastasiya Khorina, Vladislav Isayko, Krupin, D., Viktor Bolotsky and Pavel Sitnikov (2018). Modeling of user behavior for social media analysis. 2018 Moscow Workshop on Electronic and Networking Technologies (MWENT). doi:https://doi.org/10.1109/mwent.2018.8337258.

[25] Jamil, A., Asif, K., Ghulam, Z., Nazir, M.K., Mudassar Alam, S. and Ashraf, R. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. 2018 IEEE International Conference on Big Data (Big Data). doi:https://doi.org/10.1109/bigdata.2018.8622505.

[26] Knowledge Rusere, Musarurwa, S., Fungai Bhunu Shava and Munyaradzi Maravanyika (2022). Security Concerns on Social Media Customer-to-Customer Online Transactions. A Case of Namibia Facebook Users. doi:https://doi.org/10.23919/ist-africa56635.2022.9845558.

[27] Kurniawan, Y., Cornelia, V., Langitiska, C., Young, W., Anwar, N. and Johan (2021). Analysis of The Effectiveness Of Social Media Instagram (A Case Study at Pom-Pom Café). [online] IEEE Xplore. doi:https://doi.org/10.1109/ICIMTech53080.2021.9535018.

[28] Layton, R. and Elaluf-Calderwood, S. (2019). A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices. [online] IEEE Xplore. doi:https://doi.org/10.1109/CMI48017.2019.8962288.

[29] Legg, P. and Blackman, T. (2019). Tools and Techniques for Improving Cyber Situational Awareness of Targeted Phishing Attacks. [online] IEEE Xplore. doi:https://doi.org/10.1109/CyberSA.2019.8899406.

[30] Mccloskey, S. and Herbert, J. (2019). User Behaviour-Based Access Control for Social Media with Qualitative Research and Bayesian Modelling. [online] IEEE Xplore. doi:https://doi.org/10.1109/COMPSAC.2019.10269.

[31] Miyaji, H., Hsu, P.-C. and Miyaji, A. (2022). Privacy-Preserving Social Media with a Disclosure. Tenth International Symposium on Computing and Networking Workshops (CANDARW). doi:https://doi.org/10.1109/candarw57323.2022.00010.

[32] Nakerekanti, M. and Narasimha, V.B. (2019). Analysis on Malware Issues in Online Social Networking Sites (SNS). [online] IEEE Xplore. doi:https://doi.org/10.1109/ICACCS.2019.8728536.

[33] NIST (2019). Cybersecurity Framework. [online] National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework.

[34] Nuchitprasitchai, S., Kilanurak, N. and Porrawatpreyakorn, N. (2020). Guidelines for Reducing Risk of Social Media Usage for Thai Elderly. [online] IEEE Xplore. doi:https://doi.org/10.1109/ECTI-CON49241.2020.9158321.

[35] Pal, P., Ghosh, S. and Kar, N. (2023). Attacks on Social Media Networks and Prevention Measures. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICONAT57137.2023.10080106.

[36] Paramarta, V., Jihad, M., Dharma, A., Hapsari, I.C., Sandhyaduhita, P.I. and Hidayanto, A.N. (2018). Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social

Media: Facebook, Twitter, and Instagram. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICACSIS.2018.8618220.

[37] Patil, K. and Arra, S.R. (2022). Detection of Phishing and User Awareness Training in Information Security: A Systematic Literature Review. 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). doi:https://doi.org/10.1109/iciptm54933.2022.9753912.

[38] S Suresh Kumar, B Swarnagowri, R Susmitha and R Sujitha (2023). Exploring Techniques for Web Phishing Detection: A Comprehensive Survey. doi:https://doi.org/10.1109/iciccs56967.2023.10142655.

[39] Schubert, R. and Marinica, I. (2019). Facebook Data: Sharing, Caring, and Selling. 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). doi:https://doi.org/10.1109/cybersa.2019.8899743.

[40] Shetty, S.S., Shetty, R.R., Shetty, T.G. and D'Souza, D.J. (2017). Survey of hacking techniques and it's prevention. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICPCSI.2017.8392053.

[41] Singh, M. (2021). Privacy Preservation Techniques for Social Networks Users. 2nd International Conference on Computational Methods in Science & Technology (ICCMST). doi:https://doi.org/10.1109/iccmst54943.2021.00036.

[42] Srilakshmi Voddelli, Sastry, S. and Prasad, R. (2022). Deep Learning (DL) Algorithms for Privacy in Online Social Networking Sites (OSNS). 6th International Conference on Computing Methodologies and Communication (ICCMC). doi:https://doi.org/10.1109/iccmc53470.2022.9753695.

[43] Sutarno, K., Estadimas, B., Taliya, A., Wardoyo, D., Hapsari, I.C., Hidayanto, A.N. and Nazief, B.A.A. (2020). Factors Influencing User Intention in Opening Personal Data on Social Media. 2020 Fifth International Conference on Informatics and Computing (ICIC). doi:https://doi.org/10.1109/icic50835.2020.9288614.

[44] Tabassam, S., Shah, H., Alghamdi, K. and Badshah, A. (2019). Social Netwoks and Digital Security. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICECCE47252.2019.8940808.

[45] Talwar, A., Chaudhary, A. and Kumar, A. (2022). Encryption Policies of Social Media Apps and Its Effect on User's Privacy. 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). doi:https://doi.org/10.1109/icrito56286.2022.9964730.

[46] Trustwave. (n.d.). Meta-Phish: Facebook Infrastructure Used in Phishing Attack Chain. [online] Available at: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/meta-phish-facebook-infrastructure-used-in-phishing-attack-chain/.

[47] Winter, R., Scheinert, S., Stanfill, M., Salter, A., Newton, O.B., Song, J., Fiore, S.M., Rand, W. and Garibay, I. (2020). A Taxonomy of User Actions on Social Networking Sites. doi:https://doi.org/10.1145/3372923.3404808.

[48] Yadagiri Vamsi Krishna, Gudipudi Jahnavi, Medam Tharun, Sravya Geethika Yegineti, Raja, G. and B. Suneetha (2023). Survey: Analysis of Security Issues on Social Media using Data Science techniques. doi:https://doi.org/10.1109/icict57646.2023.10134391.

[49] Yang, R., Yu Jie Ng and Vishwanath, A. (2015). Do Social Media Privacy Policies Matter? Evaluating the Effects of Familiarity and Privacy Seals on Cognitive Processing. 48th Hawaii International Conference on System Sciences. doi:https://doi.org/10.1109/hicss.2015.417.

[50] Zbořil, M., Syrovátková, J. and Pavlicek, A. (2022). Social Login Usage for Third-Party Cloud Services — Relation of Security Risks and Configuration. doi:https://doi.org/10.1109/snams58071.2022.10062712.

[51] Zheng, J. and Ariyo, O. (2022). A Study On Security and Privacy Risks of Self-Disclosure On Social Networking Sites During COVID-19 Pandemic. IEEE International Conference on Big Data (Big Data). doi:https://doi.org/10.1109/bigdata55660.2022.10021102.