A Comprehensive Study on Privacy and Security on Social Media

https://doi.org/10.3991/ijim.v16i01.27761

Mohammed S. Albulayhi(✉), Salim El Khediri
Department of Information Technology, College of Computer,
Qassim University, Buraydah, Saudi Arabia
mohmad199077@gmail.com

Abstract—In many aspects of healthy, science, educational, functional, and social life, social media networks today are part of the human lifestyle. Social media has more impact on human life and introduced significant changes in the way people's way of communication. People exchange a lot of information across social media networks, starting with the sharing of information with the growth of information sharing at the moment, and the advancement of technology Users create overt networks to reflect their current or new social connections. Users also upload and post a plethora of personal details. Maintaining the privacy and security of the user is a main challenge in social media. Users should feel the importance of preserving the privacy of their data and how valuable information such as banking details and confidential data should be kept away from social media. Users can also post personal information about others without their permission. The problem is exacerbated by users' lack of familiarity and knowledge, as well as the lack of appropriate resources and architecture of social media networks. This paper provides study on many privacy and security challenges encountered by social media networks and the privacy threats they pose, as well as current studies into possible solutions.

Keywords—social media networks, security information, privacy, policy enforcement

1 Introduction

The key idea of social media is to connect people of different societies and establishments. It has also created many business opportunities for enterprises and individuals. But this innovative and influential social media leads to a lot of issues in both personal and public critical security concerns. For the new promotion on their business the enterprises can analyze the users of social media like Facebook and twitter and find the pattern of their reactions for the several postings. And the HR managers review the social accounts of their career candidates to conclude the final selection for their recruitment. even more than previous forms of web applicants [1].

Even after the chain of recruitment process like online application, written examinations, group discussion, and the final personal interview, the analysis of the social accounts (Facebook, Twitter, LinkedIn etc.) of the applicants are also plays a key role on the recruitment process, at the final decision-making process of the recruitment [1]; Police departments are using social media platforms to gather information in order to prosecute crimes [2]; practices on public social sites are changing political regimes [2] and swinging election results [2]. Since social media users are usually linked to peers, families, and associates, there is a widespread belief that social media networks offer a safer, confidential, and trusting Internet-mediated atmosphere for online interaction.

In the short span of the last ten years the usage of social media has exploded to a steeply rise and its impacts and effects are not expected for a such a level in every aspects of human life. People across the globe, irrespective of sex, race, and culture are using social media networks to communicate with known and unknown persons, relatives, and non-relatives, working and non-working peoples, in ways that were previously impossible in the earlier days. The arrival of social media drastically improved the approach of the communication and the presentation of the information among themselves. The impact of social media not only enhance the personal communications but also gives the way to promote the business among their customers by the companies and enterprises with the help of internet and networking facilities. Because of the widespread use of social media, it is worth considering if users are relinquishing their concealment of human and civil rights. Users are increasingly inclined to trust social media networks with individual data, such as personal contacts and location, without questioning what type of attacks on their data once it is gathered by the social media companies [3]. Once the personal information of the individual users could have stored on the server of the social media through the common internet, it is apparently assumed that only those users would have access to it. But it is a big danger without the knowledge of the security attacks and the hackers of the social media networks. Figure 1 shows the main reasons for using social media networks.

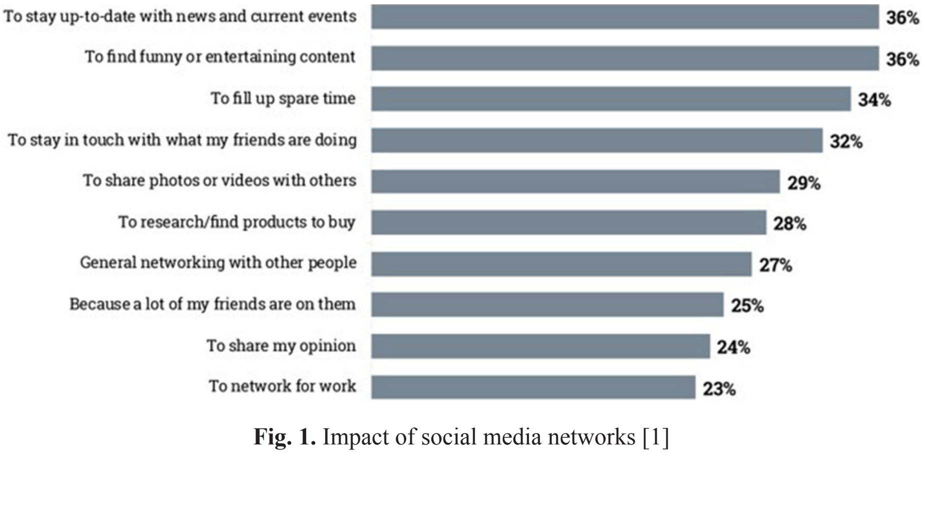

Fig. 1. Impact of social media networks [1]

People are incented to overshare classified details on social media, which offers a major insecure outlet for data breaches, it provides the sufficient information to the data breached to steal the user's personal information and allows them to spread the data over the network or to sell the data to the rival companies for a huge money. Figure 2 shows the history of social media network users. More than 4.5 billion people throughout the world have access to the internet, and about 3800 million people use social media. According to the current statistics by the middle percent of 2021, approximately more than 50 percent of the global population will be connected through any one of social network, while 65 percent of people are the using the online networks for any purpose. The total number of persons accessing internet across the world will be raised to 4500 million, a tremendous growth of 8 percent compared to the month of September 2020. The total number of social network account holders is 3800 million worldwide, which is more than 9 percent compared to the previous year 2019.

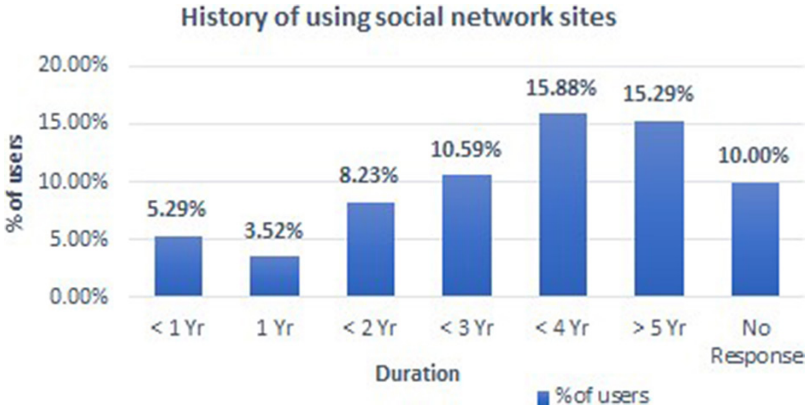

Fig. 2. The history of social media network user

Irrespective of the tremendous effects of social media facilities on both personal and business life of people, the big problem of using them is preserving the confidentiality of protecting personal data of the customer. The major distinctive of the privacy and security matters of the social media network is the malware detection. The nature of the malware is the spreading from the reliable sources and if the user clicks the link came from the trusted user contacts [4]. The large amount of benefits from the social media is directly proportional to the privacy issues relied on the social media network. So normally the social media network is a wide and good platform the hackers whose major income is the data breaches mechanism. The benefits and the privacy issues are the two sides of a coin. The latest survey conducted by the EY Global information security reiterated that 60 percent people were of the global business enterprises experienced a great set back of such data breaches that occurred during the last year.

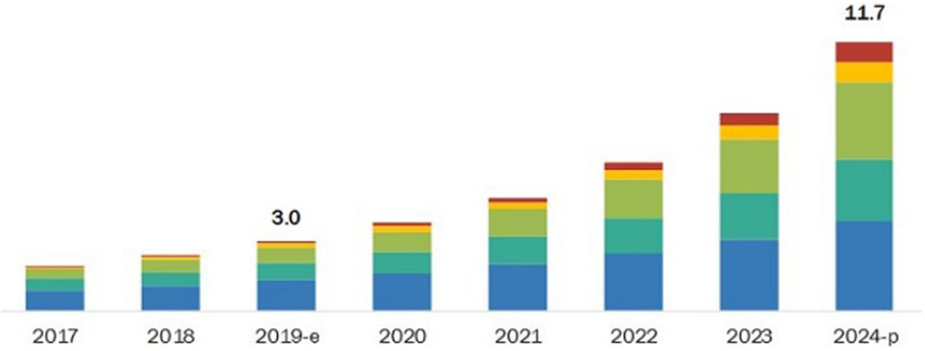

Fig. 3. The total malware growth rate in millions [5]

A global cyber-attack in 2012 by a hacker known as "Peace" exposed the passwords of over 200 million LinkedIn account holders. After these cyber-attacks, the management of LinkedIn started to implement a new protocol. Even after five years the same hacker "Peace" started revealing the compromised password details from the previously attacked LinkedIn account holders [4]. Since billions of social media users' credentials and personal data are circulating across the internet, social media sites must have tight protection. Every day, Facebook reports collecting as many as 600,000 security hack attempts. Every day, the National Security Agency (NSA) reports 300 million attempted hacks. Figure 3 shows the total malware growth rate in millions.

Misuse of identity, threats from third-party applications, trusting operators of social media networking sites, phishing attacks, viruses, and malwares, legal difficulties, tracking users and privacy of data are all important challenges in social media networks. The safety of social media.

In the broader framework of data mining, advanced recordings of human conduct in interpersonal organizations can be identified with a significant amount of productive analyzing in order to learn without invading users' privacy. As a result, information should be made available in such a way that privacy is protected and security is closely monitored. Contrary to popular belief; however, it is exceedingly improbable that any outsider interested in deciphering information can be relied upon, because gatherings may desire to use all information, even sensitive and identifying information. Because interpersonal organizations are so distinct, the best course of action is to guarantee the unflinching quality of privacy for the person who expresses affiliation with them.

The rest of the paper is structured into another three sections. The related work on the security and privacy of social media networks is analyzed in Section 2. The Probable Hazards with its confidentiality risk in Social media network Sites are explained in Section 3. The trust management and their corresponding issues are given in the fourth section. The last part summarizes the results of our investigations and the proposed methodology to adopt security and privacy on social media networks with the conclusion.

2 Related work

Online social media networks have been an inevitable feature associated with the everyday breathes in most of the people over the globe in recent years. Social network users can create their own exclusive network for the purpose of establishing their personal and social communication links with the help of the social media service providers. All the users associated with this explicit link will share a lot of personal data by uploading them continuously. Such personal privacy threats associated with these actions were habitually overlooked and disregarded. Users, some time, also reveal sensitive information to a wider public than they expected. Users may also share personal information on other people ignoring the consent of others. This problem is exacerbated by users' lack of expertise and understanding, as well as the absence of appropriate tools and structure of social media networks.

Open and unstructured methods were employed in this exploratory study to better understand and know what people think they're talking about friendships, privacy, and privacy abuses. Unstructured interviews were conducted with an opportunistic group of eight persons, who were given an introductory question and a topic of discussion to have the conversation going. Three of the eight were guys, while the other five were women. They ranged in age from 23 to 32. Even though everyone in the group had at least a bachelor's degree, they came from a wide range of academic backgrounds. In a similar manner, participants were questioned at their convenience and in quiet areas. To record each interview, we used free open-source software (Audacity) and an inexpensive PC microphone. Interviews ranged in length from 10 to 26 minutes. The interviewer avoided leading questions and suggestive body language to make the subject feel at ease, open to debate, and unbiased.

Participants were asked about the importance of friendship before being quizzed about an instance of privacy invasion in their lives. In order to better understand how privacy breaches, affect friendships both before and after they occur, this research was carried out to gather data. The inquiries into friendships and their advantages were broader, but the inquiries into privacy violations were narrower.

While ethical issues were minor, they were taken into account, and actions were taken to lessen the danger. Consent was granted with full knowledge. Participants were made aware of their right to request the removal of their personal data at any time. Interviewees were assured they could give however much or how little information they wanted, and this was reaffirmed when concerns about privacy were expressed. The interviewer instructed not to prod the interviewee for more details if the subject matter sounded distressing or sensitive. And last, if any unintended consequences occur, the subject might address them with their interviewer, which would allow the interviewer to give them appropriate assistance and refer them to experts in the field concerned (using the NHS Direct Web site).

In the eight interviews conducted, none of the subjects voiced any concern or desire to have their information deleted. In order to discover modal concerns and motifs, the transcriptions were subsequently subjected to thematic analyses.

Privacy and Security issues on Social media network: Table 1 provides the consolidated data of the various categories of "privacy and security" issues encountered in the social media services' aggregator.

Table 1. Different types of privacy and security topics in social media networks

Type of Data Leakages	Issues on the Social Media Networks
Data breeches with other customer	Sybil attacks
Data breeches within social apps	Compromised accounts
Data breeches within networks	Social spam and malware
Data breeches within the group	DDoS

Leaks and linkages to consumer knowledge and content concerns are related to the possibility of information leakage. We consider a variety of organizations that are involved in the leaking and linking of users' information and content. Conversing with other users may put users in danger, particularly if any of them are strangers or just acquaintances.

Data leakages associated with the social media services leads to the several misuse of internet users including phishing scam as described in [6]. This fraud of misusing internet touched a level of 16 percentages. User credentials are similar to a social contract inside which individuals share their own data for monetary or nonmonetary rewards, which is the only drawback of privacy concerns. It goes without saying that as long as the advantages of a very social contract outweigh the current and foreseeable hazards of publicity, responsible consumers will remain interested in it. Notion says that people make choices that maximize their benefits while minimizing their expenditures. This idea supports that theory. It's been developed to exploit the interests of the users in order to reveal the information that they've shared on social media sites like Facebook and Twitter.

The major source for the occurrence of these threats are the hike in the social media accounts holder, the usage of social network by the enterprises and the increase of explicit communication link within the persons through the social media network. Figures 4 and 5 show that the statistics of the internet frauds [7].

The recent detailed survey conducted by the popular security software company Webfoot [6] shows that the major setback on using the social media networks is the easy possibility of the attack on the user's confidential information about their financial status. These attacks will steal the log in credentials like user Id, Login password and Transaction password of the social media network users. Their digital devices are also affected by the malware, which was intestinally spread by the trusted user, while accessing the social media networks. As per the new regulations and laws enforced by the local government on the social media network service providers, the user's confidential data and the financial transactions must be shared with government agencies whenever required. Both the data breeches by the cyber attacker and the intervention of the government will in future be forcefully damage the relationship between users and the service providers.

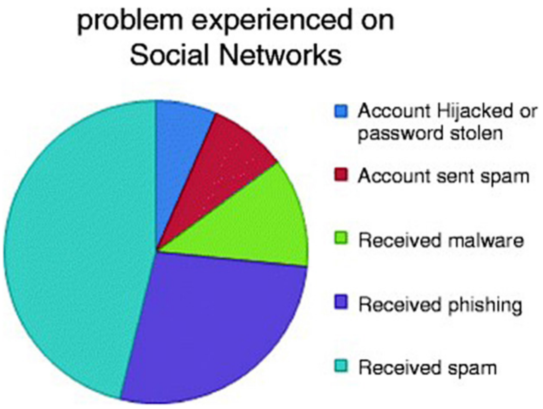

Fig. 4. Internet fraud statistics [7]

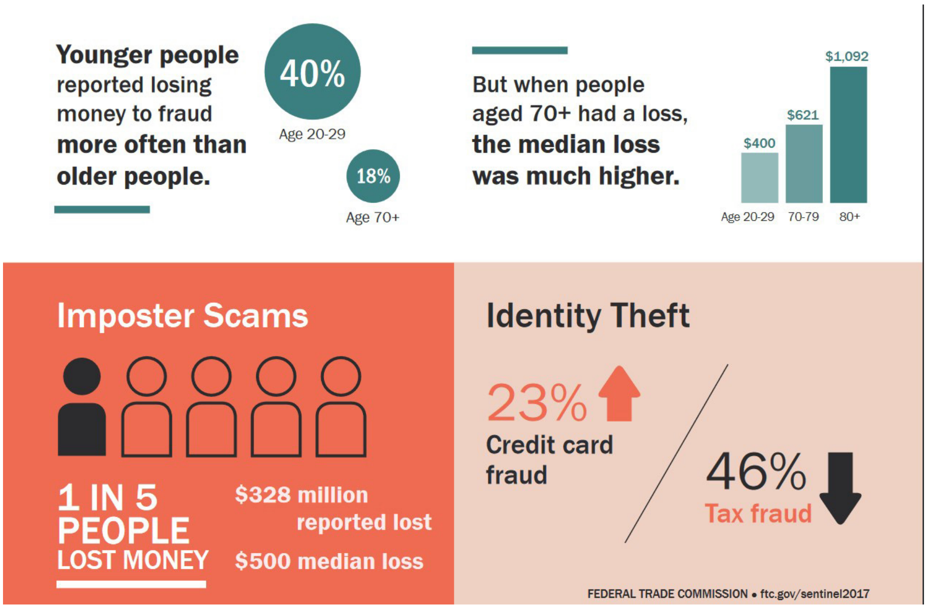

Fig. 5. Internet fraud statistics [7]

A big scam on the attack of the Facebook user's personal information was reported on 2016 in the united states of America. The Cambridge Analytical [7] illegally helped the presidential candidate by providing nearly 50 million FB users account information and this indirectly influence the result of the presidential election in favor of that candidate's victory. According to the studies conducted by Pew Trust, every year nearly 85 percent of social media network users lodged complained that their personal information is steeled and given to the many advertising companies by the attackers. They intervened without their permission on their social media posts and provide the statistics to their advertising agents and gained more and more. Unwanted leakage of user information, along with the blurring of the technical and personal sides of users' lives caused by social media networks, allows for serious accidents. The destinations of social media network pages' act to enhance privacy settings. As a big feature of their default design structure many large-scale social media service providers, restrict security. Clients must go into their account configuration and change their security preferences.

Furthermore, the large amount of individual information is collected with the help of both technically impaired ordinary consumer and because of social media networks' inability to have modern confidentiality devices, has drawn many numbers of companies to extract and provide that data to their business collaborators. Figure 6 displays that the shadow profile problem, in which SPP system encompasses a portion 'm' which is the total magnitude of the users and 'n' is total size of the user who share their contact details [8].

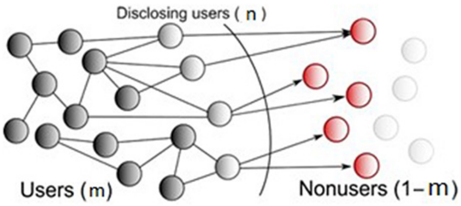

Fig. 6. Shadow profile [8]

The spread of malware relevant data through the social media network is another inevitable and unwanted effect. Even though the rumor was already existed in the society in the ancient days, its spreading has less effect and slow spreading among the people. But nowadays the fake news can spread as the speed of light propagation through the social media network as virus. Since the last March 2020, the news about the "corona Virus" both in the sense of good awareness and bad afraid, spread in the rocket speed through the social media network [9].

One more attack on the social media network is called as "Botnet". Automated accounts known as botnets create messages or follow new users on social media sites when a certain word is typed in. There are many bots in a botnet, which acts as a network. Data is stolen, spam is propagated, and distributed denial-of-service (DDoS) attacks are carried out with the help of bots and botnets on social media [10]. Botnet structures usually take one of two forms, and each structure is designed to give the botmaster as much control as possible. Figure 7 shows the Propaganda Botnets on Social Media.

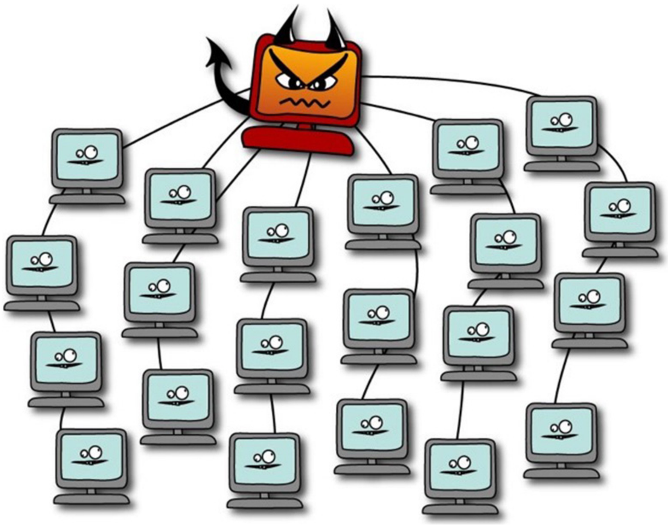

Fig. 7. Propaganda botnets on social media [9]

Creating harmful group events on social media networks is simple thanks to the networks' well-known mobilization function. Social media networking sites, micro-blogs, and other forms of social communication, which take advantage of the powerful new media features, can be easily abused by those who wish to propagate misinformation and encourage violence.

Attacks on social media networks are aimed in targeting to attack the service provider directly, posing a threat to its main market. Social media network is using the attacks named as Distributed Denial-of-Service (DDoS) attacks which was targeted to create a forum to spread fake news in the form of spam and malware.

This type assaults are carried out in different variety of methods. Like Sybil attach which is a method of subverting a reputation system by generating many identities, intruders may generate many identities to spread malware or spam content. Attackers may also illegally make use of the credentials built by unknown person to conduct coordinated attacks. It's worth noting that the attacks on social media networks have an impact on platform consumers as well. Attacks on social media networks, on the other hand, take advantage of the social graph of the network to victimize additional people by spreading quickly. As a result, the service provider's highest priority was the detection and interrupt the dissemination [11] [12] [13]. The groups and protection issues are summarized in Table 2.

Table 2. Comparisons of privacy and security od social media networks among reference papers

Reference	Advantages	Disadvantages	Comments
[1] Joshi, P. & Kuo, C.-C.	Examine the mathematical formulations and simulation methods for social media network integrity and confidentiality.	There are no feasible methods for an intruder to perform an attack.	Algorithms should be created to infer confidence in social media networks as vulnerabilities and security breaches grow more context aware.
[2] Ricard Fogues, et al.	offer a list of privacy dangers that may impact users of social media network services, as well as the requirements that privacy procedures should meet to avoid this threat.	The suggested paradigm and terminology must be adaptable enough to allow for multiple social media network solutions that cover a wide range social feature.	Current techniques must be examined to see how well they meet the criteria.
[3] S. Kumari, et al.	A detailed Evaluation of Data security on Social Media, as well as the dynamics of intersecting organizations in the real world are presented.	No multiple regression analysis to ignore the growth of the organization including the network backbone.	To be deployed, more developed theoretical models describing the link among the expertise mechanism and community membership.
[4] M. Ismailov, et al.	given a summary of typical state-of-the-art outcomes on detecting identity trick, as identified by the authors.	Not identified common methodological weaknesses.	It is better to identify the weakness and some recommendations to be proposed.
[5] Hossain, et al.	present PriMa (Privacy Manager), a confidential system that provides development of access restrictions for users' profile information, bridging the gap between SN users' privacy management demands and the privacy protection methods of existing social media networks.	There aren't any examples of how an attacker may attack.	The scientific interpretation may be considered into account.

3 Proposed methodology for social media privacy problems

This study's sole aim focusing on connecting a measurable scheme associating a particular outcome of specious investigating the public data of prospective customers. This system retrieves the personal credentials, residential details and so on. To help with this, we created a survey method that would be extensively used and disseminated to over 200 social media participants, with the population determined with the help of special technique. As a result, this thorough research has concentrated more on privacy issues related to social networks and has essentially jolted out privacy violations.

We defined some of the privacy issues that Facebook users should address before using social media and incorporated them into the site's privacy settings to avoid any violations.

For a long time, privacy concerns about e-commerce transactions were the main focus of attention because of credit card theft and the misuse of personal information by vendors. But now that people are more concerned about the content they share online, the focus has shifted. Individuals putting personal information on their pages or the SNS allowing unrestricted "default" access are the two most common ways that identity fraud is perpetrated on social media. Aside from obvious issues such as credit card fraud, identity theft, and data storage problems, users' own behaviors, such as youths' tendency to "sext," cyberbullying, and the difficulty controlling personal information can all put privacy at risk.

Privacy can be viewed from the perspective of having control. Keep control over personal data, decision to release data, physical interaction of others, number of people participating in disclosure or decision about who you chat and discuss issues with is crucial to maintaining privacy. Control. With a focus on social relationship with our surroundings, Altman developed the concept of personal, dyadic, and collective borders to limit privacy and transparency. On a day-to-day basis, these restrictions are readily apparent. The person we are speaking with is aware of our body language and vocalizations; the person we are writing to is aware of our posture and movements; how much we have heard and from whom we have heard it; who can see us as we walk down the street; that see us choose restroom; if cameras are keep pointing at us; if someone or something has touched us; and if we have touched someone or something is aware (whether friendly or unfriendly). In an SNS setting, controlling these barriers and the information flow across them can be difficult due to the ambiguous meaning attached to the word "friend." The term "friend" is frequently used on social media to refer to a variety of prospective interpersonal ties.

3.1 Social media user's behavior prediction

This research aims to find out how social media users perceive anonymity and confidentiality in social networking sites [7]. A sample of 200 respondent's understudies was selected at random from various parts of the globe. A total of 185 surveys were successfully filled and returned. Males made up about 78 percent of the respondents, while females made up about 22 percent. On the other hand, about 72 percent of respondents were between the ages of 20 and 35. However, the number of populations comprises groups "between 28 and 41" was almost 19 percent, while the number of populations comprises groups "50 and up" was close to zero. The educational standard has a significant effect, with four-year certification accounting for 58 percent and progress grades accounting for 30 percentages. An increased usage of network reflects some similarities in of social association, with 56 percent of those who have been using the site for more than 10 years, and if we link the use with the essence of SN, we get 51 percent for moderately well-known and 49 percent for extremely well-known.

3.2 Confidentiality problems and troubles

As seen in Table 3, when asked about protection, the knowledge on the security awareness provided by the social media network service provider, only 50 percentage of the user only somewhat familiar. Many service providers change their security setting in such a way cannot be changed or accessed by the user itself on their personal information. They did not allow the user to change their profile without proper and well-defined authenticated process. Nowadays three stages of authentication process are carried out carried out by the social network platforms to access the profile of the user. However, when it comes to changing security settings, 43 regression coefficient their privacy configuration every so often, which means only if anything happens, and 47 percent modify their protection setting on a regular basis, which is the same for security and record setting. We listed the various privacy controls provided by the service provider to their customers during login process in Table 3 below. There is a vast spectrum of sexism that exists in social media sets when it comes to providing privacy policies to consumers, and based on the results of the poll, many users of social networking sites have not given any thought to their security settings and have left their privacy data as they are.

Table 3. The comparison of secrecy concerns in social media networks

Secrecy choices	Facebook	Twitter	LinkedIn	Google+
Active users' visibility Restriction	Allowed	Not Allowed	Not Allowed	Not Allowed
Control on locating the users	Allowed	Allowed	Allowed	Not Allowed
Blocking facility with image	Allowed	Not Allowed	Not Allowed	Allowed
Login Alerts	Allowed	Not Allowed	Not Allowed	Allowed
Blocking facility with spam	Allowed	Allowed	Allowed	Allowed
Restriction on the new message	Allowed	Not Allowed	Allowed	Allowed

3.3 Privacy setup on social networking sites

The privacy settings on social networking sites are reinforced. As part of their basic settings, Facebook and other long-distance social networking sites minimize protection. To change their protection options, clients must go into their client settings. Clients can choose not to display personal data such as their date of birth, phone number, email address, or company status on sites like Facebook. For those who choose to include this information, Facebook allows users to restrict access to their profile to just those they identify as “companions.” Regardless, even this level of anonymity isn't enough to prevent one of those companions from downloading a snapshot to their own computer and uploading it elsewhere. Nonetheless, fewer social networking site users have restricted their profiles recently.

Take, for example, how individuals can limit the display of their profiles to others on various social media sites If you're on Facebook, for example, you can choose to hide your profile from other users. xFacebook: The default privacy setting for new users on Facebook is Friends Only. To make this adjustment, navigate to Settings > Privacy > Who can see your future postings. Protect my Tweets in Twitter's Security and Privacy Settings: Twitter: Security and privacy settings > Privacy > Tweet privacy If you'd like to update anything about your public profile, go to xLinkedIn:Settings xTwitter and edit it there. to change this setting, write the name of a Circle in the "To" box under your article before you publish it.

Facebook may clearly state that they cannot guarantee the privacy of their users' information, and that if users make their profiles public, all information included within may be viewed by job interviewers and school board members. Remember that most long-distance informal communication destinations encourage you to close applications, hide your buddy list, and hide your interests. As a matter of course, much of the data is still open. It is critical that all clients of long-distance interpersonal communication sites limit access to their profiles, do not submit data on illegal or arrangement-breaking behaviors to their profiles, and be cautious of the information they make available.

4 Types of relationship tie

We live in a social context where managing the flow of personal information to various connection links is critical. We release more information about ourselves with those whom we have an intimate relationship since it is part of the private tie of intimacy. With an intimate relationship, we may convey different information than with parents. According to Reiman, "we can only give out personal information to friends and/or strangers because we can hide it from the rest of the world—and limit inti-mate observation of ourselves" (1976). Intimate partners and parents, for example, may have different information needs. There are no close connections between friends and/or lovers unless we are able to share personal information regarding ourselves with others, and disallow intimate views of ourselves, according to Reiman (1976). A person's personality and personal information are important since it helps determine how private or detailed the information is when determining which parts of one's personality and personal information to expose to various kinds of partnerships. This is important. As per Altman and Taylor (1973), the different and evolving layers of an onion represent the primacy of personality. Some researchers believe that the importance of individuals inside a social network is linked to their expectations of privacy. Personal information is considered a violation of privacy if it is acquired by another party and made available to connections above what the individual's own implies and close buddy circle would reasonably expect [14].

Whenever we connect online, either on a social media platform, the line between who can see our data or images blurs. Virtually [15] exacerbates the difficulty of managing people. By adding multiple "ties" to our friends list on sites like Facebook [11], it becomes difficult to control access and sharing with a variety of different people and "friend" category members. For example, photos of intoxicated trips may be swiftly shared with friends, but can they be readily discussed with family, colleagues, or even potential employers? Unless the photos are restricted and governed by frequently sophisticated privacy settings, anyone on the "friends" list can see them online. To make matters worse [11], it's becoming increasingly difficult to maintain control over social spheres, which might lead to privacy intrusions.

Concerns about privacy on social media platforms can differ depending on the site being used and the user's privacy options and site settings. As an illustration, Facebook enables users to create a public profile that contains information such as photographs, home town, date of birth, relationship status, and e-mail address [16]. The information is then made available to the whole public, including those who may not know you. As a result, until the privacy settings are changed, users may not be aware of the recipients of the information they're sharing. Additionally, releasing personal and private information may cause security difficulties including phishing, leakage of information and stalking [17].

Personal information shared by default across all social networking sites, such as a user's photo, is not immune to privacy concerns on such sites, even if it is not publicly shared [17]. In the wake of the recent changes to Facebook's privacy settings, many users' information (such as images and lists of "friends") are now exposed to everyone by default, further aggravating the problem.

Outside access, such as identifying profile images, demographic data, or distinct interests from other SNS, has tended to dominate discussions of privacy and social networking sites [18]. Other external concerns could stem from SNS's widespread usage of unsecured login connections, which provide simple access to other parties including hackers, identity thieves, and the government [18]. Even if private information is willingly shared by a site user, there are additional privacy concerns inside the SNS and the network of contacts [18]. Some instances include the sharing and tagging of photographs that identify other users, disclosing demographic information, and disclosing personal information on profile websites that involves other users [19].

Furthermore, it has been demonstrated that having information about one's hometown and date of birth makes it easier to calculate Social Security numbers (SSN) in the United States [19].

Bonneau & Preibusch (2009) found a wide range of privacy control options on the 45 social networking sites they visited. Privacy rules, privacy controls, and informational measures, according to Bonneau and Preibusch (2009), are frequently cumbersome and fall short of expectations. Even if privacy-enhancing features are available, sites rarely publicize them when it comes to maintaining privacy on social media platforms [20]. As a result, if users are uninformed that privacy dangers exist, they are unlikely to be prompted by a social media platform that does not market such features, and therefore unidentified data sharing may persist. For this reason, it is possible that SNS will not publicize their features: even for users who aren't concerned about privacy, growing attention to privacy controls may cause users to become more careful and share fewer information [20], minimizing the richness of content and thus the experience of the users and their contributions [21].

Today's Internet use raises several questions about one's right to privacy. There is an increase in the number of SNS and SNS users, making it increasingly difficult to control how information is shared and concealed [11]. In social networking sites, the "friends" umbrella's cumulative nature of social spheres, or connection types, exacerbates issues. It is common for users to be unaware that their data is being gathered and stored on a large scale [22]. Often, they're unaware of the perils of hanging out with a bunch of "pals" Online and SNS privacy issues like credit card fraud, identity theft, and what kind of information people put on their SNS pages are frequently discussed [23]. Despite the validity of these worries, it's not clear what participants consider a violation of their privacy or whether researchers share their concerns.

Many people were interviewed about their personal experiences and friendships to have a better understanding of the difficulties and impacts of dealing with and being the victim of a privacy invasion [24][25]. We queried about privacy violations in general, rather than especially online, but it became evident that the majority of participants' privacy was infringed because they used Facebook. Due of privacy's potential role as a method of control for limiting detailed info flows to certain kinds of relationships, we questioned interviewees whether friends and friendship signified to them in order examine these links between privacy and friendship [26][27][28].

5 Solutions for social media network privacy and security issues

The general method for shielding information from social media networks is focused on the observation that false data can be used to operate them. Users will also access social media networks without offering actual evidence if the operations that social media networks run on fake information can be traced once again with back to initial information.

FB service provider introduced a feature named as Fly-by-night to their account holders, which allows the customer to connect in online without giving the recordable conversation on platform. During the set-up Fly-by-night Facebook app produces a confidential password with a pair of private keys. Then the app perform encryption on the private keys with the use of confidential password and the output of the encryption process was saved in local computer. During the installation process of a client-side JavaScript is downloaded, which was available on the server of Fly-by-night facility. A key was generated and used for the decryption to find the password. This process was the combinational in nature with the integration of the attribute-based encryption (ABE) and the cryptography public key.

An application named as Persona masks user data from the social network. Persona implements the key functionalities of existing social media networks as apps, such as accounts, walls, notes, and so on. Persona makes use of the request "Loading" which allow the account holder for saving their confidential data and felicitates the sharing them over the network. The Facebook Persona app is equivalent to every other third-party Facebook app except that user's log in by authenticating via the browser extension. Persona's exclusive markup language is translated by the browser extension. Persona databases provide its all the available information with the help of cloud technology with high level of security.

6 Conclusion

The privacy and security on the social media network are an inevitable mechanism to be employed, because of its impact on the revolutionary usage of internet globally and locally. The entire community using the social network comprises of two type of groups based on the acceptance on providing their personal and confidential data over the media. One group of people willing to share their information with others without hesitation. But most of the user have no willingness to share their data with social media service provider. So, the greatest success on the development of social network is solely depends on the security mechanism provided by them to secure the users sensitive data. Rally in future, there is no life without social media network. So, it is the responsibility of both the user and service provider to adhere the privacy and security mechanism in order to save their confidential data. The existence of the cyber attacker cannot be avoided but their operability can be surely restricted with the help of the most complicated security mechanism, which are clearly given and analyzed in this paper.

It has been found that privacy issues in social media websites are very weak, and users' efforts to make effective improvements to their social media privacy are much lower than in other modes of security operations. Furthermore, many social media consumers lack technological skills, resulting in low privacy issues about their own posts. Many of the flaws and hiccups on the technological side of privacy and security controls on social media platforms were found in the statistics collected. As a result, we identified the potential source of the issues and recommended reforms to address the social media networking site's privacy concerns. We might protect social media networks against more attacks and bugs if we enforced a multilevel authenticated strategy while creating login credential with any social media networks. It includes creating unbreakable keys, modifying passwords often, becoming mindful of information leakage, knowing the intent of antivirus or similar applications, and proprietary apps, among other things.

7 References

[1] Joshi, P., and Kuo, C.-C. (2011). Security and privacy in online social networks: A survey. 2011 IEEE International Conference on Multimedia and Expo, 1–6. https://doi.org/10.1109/ICME.2011.6012166

[2] Ricard, F., Jose, M. Such, Agustin, E., and Ana, G.-F. (2015). Open Challenges in Relationship-Based Privacy Mechanisms for Social Network Services, International Journal of Human–Computer Interaction, 31:5: 350–370. https://doi.org/10.1080/10447318.2014.1001300

[3] Kumari, S., and Singh, S. A Critical Analysis of Privacy and Security on Social Media. 5th International Conference on Communication Systems and Network Technologies, 2015, pp. 602–608, doi: https://doi.org/10.1109/CSNT.2015.21

[4] Ismailov, M., Tsikerdekis, M., and Zeadally, S. Vulnerabilities to Online Social Network Identity Deception Detection Research and Recommendations for Mitigation. Future Internet 2020, 12: 148–152. https://doi.org/10.3390/fi12090148

[5] Humayun, M., Jhanjhi, N. Z., Alsayat, A., and Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal, 22(1): 105–117. https://doi.org/10.1016/j.eij.2020.05.003

[6] Hossain A. A., and Zhang, W. Privacy and security concern of online social networks from user perspective. International Conference on Information Systems Security and Privacy (ICISSP), 2015, pp. 246–253.

[7] Zhiyong, Z., and Brij, B. G, (2018). Social media security and trustworthiness: Overview and new direction. Future Generation Computer Systems, 86: 914–92. https://doi.org/10.1016/j.future.2016.10.007

[8] Newton, M., and Kalman, G. Peer-to-Peer-Based Social Networks: A Comprehensive Survey. SN Computer Science, vol. 1, 2020. https://doi.org/10.1007/s42979-020-00315-8

[9] Sun, Y. Yin, L., and Liu, W. Defending sybil attacks in mobile social networks. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, 2014, pp. 163–164. https://doi.org/10.1109/INFCOMW.2014.6849206

[10] Gail-Joon, A., Mohamed, S., and Anna, S. Security and Privacy in Social Networks. IEEE Internet Computing; 2011; 15(3): 10–12. https://doi.org/10.1109/MIC.2011.66

[11] Shaikh, A., Soomro, A., Ali, S., and Memon, N. (2009, July). The security aspects in web-based architectural design using service oriented architecture. In 2009 13th International Conference Information Visualisation (pp. 461–466). IEEE. https://doi.org/10.1109/IV.2009.83

[12] Fire, M., Goldschmidt, R., and Elovici, Y. (2014). Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, 16(4): 2019–2036. https://doi.org/10.1109/COMST.2014.2321628

[13] Houghton, D. J., and Joinson, A. N. (2010). Privacy, social network sites, and social relations. Journal of technology in human services, 28(1–2): 74–94. https://doi.org/10.1080/15228831003770775

[14] Garbarino, E., and Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. Journal of Business Research, 57(7): 768–775. https://doi.org/10.1016/S0148-2963(02)00363-6

[15] Saeed, S., Shaikh, A., and Memon, M. A. (2018). Impact of Social Networking Sites on Personality & Attitude of Young Adults (Research covering the young adults lives within Korangi, Karachi). International Research Journal of Arts & Humanities (IRJAH), 46(46).

[16] Johnson, B. K., and Knobloch-Westerwick, S. (2014). Glancing up or down: Mood management and selective social comparisons on social networking sites. Computers in Human Behavior, 41: 33–39. https://doi.org/10.1016/j.chb.2014.09.009

[17] Joinson, A. N., Houghton, D. J., Vasalou, A., and Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In Privacy online Springer, Berlin, Heidelberg, (pp. 33–45). https://doi.org/10.1007/978-3-642-21521-6_4

[18] Gross, R., and Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, (pp. 71–80). https://doi.org/10.1145/1102199.1102214

[19] Trepte, S., and Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In Privacy online Springer, Berlin, Heidelberg, (pp. 61–73). https://doi.org/10.1007/978-3-642-21521-6_6

[20] Bonneau, J., Preibusch, S., Anderson, J., Clayton, R., and Anderson, R. (2009). Democracy Theatre: Comments on Facebook's Proposed Governance Scheme. Report from Cambridge University Computer Science Lab (http://www. cl. cam. ac. uk/~ jcb82/2009-03-29-facebook-comments. pdf).

[21] Burke, M., Marlow, C., and Lento, T. (2009, April). Feed me: motivating newcomer contribution in social network sites. In Proceedings of the SIGCHI conference on human factors in computing systems: (pp. 945–954). https://doi.org/10.1145/1518701.1518847

[22] Acquisti, A., and Gross, R. (2009). Predicting social security numbers from public data. Proceedings of the National academy of sciences, 106(27): 10975-10980. https://doi.org/10.1073/pnas.0904891106

[23] Jones, K. S. (2003). Privacy: what's different now? Interdisciplinary Science Reviews, 28(4): 287–292. https://doi.org/10.1179/030801803225008677

[24] Rajan, M. S., Arunkumar, J. R., Ramasamy, A., and Sisay, B. (2021, July). A comprehensive study of the Design and Security of the IoT layer Attacks. In 2021 6th International Conference on Communication and Electronics Systems (ICCES), IEEE, (pp. 538–543). https://doi.org/10.1109/ICCES51350.2021.9489235

[25] Oladepo, A. G., Bajeh, A. O., Balogun, A. O., Mojeed, H. A., Salman, A. A., & Bako, A. I. (2021). Heterogeneous Ensemble with Combined Dimensionality Reduction for Social Spam Detection. International Journal of Interactive Mobile Technologies (iJIM), 15(17): 84–103. https://doi.org/10.3991/ijim.v15i17.19915

[26] Salloum, S. A., Al-Emran, M., Khalaf, R., Habes, M., and Shaalan, K. (2019). An Innovative Study of E-Payment Systems Adoption in Higher Education: Theoretical Constructs and Empirical Analysis. International Journal of Interactive Mobile Technologies(iJIM), 13(6): 68–83. https://doi.org/10.3991/ijim.v13i06.9875

[27] Shaikh, A., Ali, S., Memon, N., and Karampelas, P. (2010). SOA security aspects in web-based architectural design. In From Sociology to Computing in Social Networks (pp. 415–430). Springer, Vienna. https://doi.org/10.1007/978-3-7091-0294-7_22

[28] Al-Dalahmeh, M., Al-Shamaileh, O., Aloudat, A., and Obeidat, B. (2018). The Viability of Mobile Services (SMS and Cell Broadcast) in Emergency Management Solutions: An Exploratory Study. International Journal of Interactive Mobile Technologies (iJIM), 12(1) 95–115. https://doi.org/10.3991/ijim.v12i1.7677

8 Authors

Mohammed S. Albulayhi is an Master thesis student in cybersecurity at Department of Information Technology, College of Computer, Qassim University, Buraydah 51941, Saudi Arabia. ORCID: 0000-0002-1296-4742; Email: 421100196@qu.edu.sa and mohmad199077@gmail.com

Salim El Khediri is an Assistant professor at Department of Information Technology, College of Computer, Qassim University, Buraydah 51941, Saudi Arabia. Email: S.ELKHEDIRI@qu.edu.sa

Article submitted 2021-10-22. Resubmitted 2021-12-06. Final acceptance 2021-12-17. Final version published as submitted by the authors.