Advanced Engineering Technology and Application
An International Journal

http://dx.doi.org/10.1857/aeta/110301

Public Attitudes Towards Data Privacy on Social Networking Sites Towards Individuals and Organizations: A Review

H. Hussien

Faculty of Mass Communication, Ain Shams University, Cairo City, Egypt

Received: 12 Jun. 2022, Revised: 12 Jul. 2022, Accepted: 12 Aug. 2022.
Published online: 1 Sep. 2022.

Abstract: The emergence of Online Social Networking (OSN) has transformed the audience from passive subscriber readers to a contributor to content. It has allowed users to share information and exchange opinions, as well as express themselves in virtual online communities to interact with other users with similar interests. But in return, it has become an ideal platform for hacking and information leakage. It may be important to understand whether social networks represent an information security threat to individuals and organizations. So far, research has not addressed this common problem, but it focuses on one aspect of it, and this represents a clear research gap. The current research attempts to bridge this gap, which in turn raises several important questions, including What is the nature of the factors that enhance the role of social media? What is the nature of its impact on the formation and formation of public opinion? And electronic public opinion monitoring of information security challenges related to social media for individuals and organizations? By reviewing the literature relevant to this study.

Keywords: Public attitudes, security, Information, social networks.

1 Introduction

In light of the information movement and the tremendous technological development in the field of information and communication technology and the knowledge economy, in light of information openness and digital globalization, and the emergence of the techniques of the Fifth Industrial Revolution and artificial intelligence in various sectors, and in light of the digital transformation of countries and the multiplication of reliance on social networks and their means of communication, both in education and work medical consultations, conferences, and other fields; As a result of the isolation and social distancing imposed by the Corona pandemic (Covid 19), which has already contributed to an increase in the rate of hacking and information leakage in recent periods, and an increase in the rate of spread of rumors, as several forms of electronic risks have emerged and their framework has expanded in the modern era [1], weapons employee Digital in all its forms that fit the nature of the context of the digital age such as e-mail, social networking sites and artificial intelligence techniques Employing advanced technical programs, cloud computing technologies (I-Cloud), Internet of things technology, big data, and algorithms of all kinds in the design of malicious code (Malicious Code) , to strike the information security of countries, organizations and individuals, so that controlling them individually has become a very important matter to not keep pace with the digital transformations of the continuous dynamic of the nature of the risks and threats of this type of risk[2].

All countries of the world are now witnessing a prominent interest in information security due to the escalation of security breaches to infrastructure, networks and information[3], for example, the United States of America established 4 specialized bodies in the field of information security, while France established a center to confront risks[4].

Social networks are one of these types of communications that have negative and positive effects on their users. OSN makes sharing information easier and faster than real-time communication.

It makes globalization a reality and provides an opportunity for its users to express themselves. It is also a new way of international relations, both work-related and social interactions[5].

It is easy for people to interact with each other using OSNs anytime and anywhere in the world. Besides these advantages, social networks have disadvantages, the most important of which is information security.

2 Literature Review:

1. Statistics of online social media.

In the early 2000s, social networking sites provided personalized service for sharing information over the Internet and it was embraced by the masses. It can also be used for personal and business reasons[6].

*Corresponding author-mail: hanaa.hussen@women.asu.edu.eg

It brings people together to talk, exchange ideas and interests, and make new friends. Basically, it helps people from different geographic areas to collaborate [7].

Social networking platforms have always been found to be easy to use. Therefore, social media sites are growing exponentially in terms of popularity and numbers. Social networks can also be used for entertainment, job building, getting a job, improving one's social skills, and forging relationships with other individuals.

Many individuals and organizations have begun to realize the importance of social networking as a valuable resource, as it is one of the most widespread and widespread applications of new media on the Internet, and the popularity of social networking sites such as Facebook and Twitter LinkedIn have increased over the past few years, due to its technological capacity in connected and offline communication Online and offline connections.

These resources provide online organizations and institutions with the ability to take advantage of current social networks to achieve positive results for their customers, including providing social support, enhancing sales and profits, enhancing knowledge, enhancing knowledge, and generating innovation[8].

Social networking is defined as: “A set of internet-based technologies that allow users to easily create/modify/link content to other websites, in preparation. They are increasingly used by local governments and have the potential to involve stakeholders in future engagement projects. Where social media encourages dialogue between citizens and the government”[9] social media is also defined as: “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content,” and characterized by interactive participation by users. User-generated content refers to “ The ways people might use social media”[10]Global statistics show the increasing use of social networks around the world, with unprecedented diversity in their public and private content, and also the increase in Internet use, and there are nearly 4 billion (4 billion users) users of the Internet, and there are 2.7 billion (2.7 billion) users Monthly on Facebook[11], 330 million active users on Twitter, 320 million active users on Pinterest.

Figure 1 shows the number of users on different social networking platforms according to a report from Zephoria[12], and there is an increase (16%) year-on-year in monthly active users of Facebook and seven new accounts are created every second. Users upload a total of 350 million photos per day, on average 510,000 comments are posted on Facebook every 60 seconds, 298,000 statuses are updated, and 136,000 photos are uploaded[13].

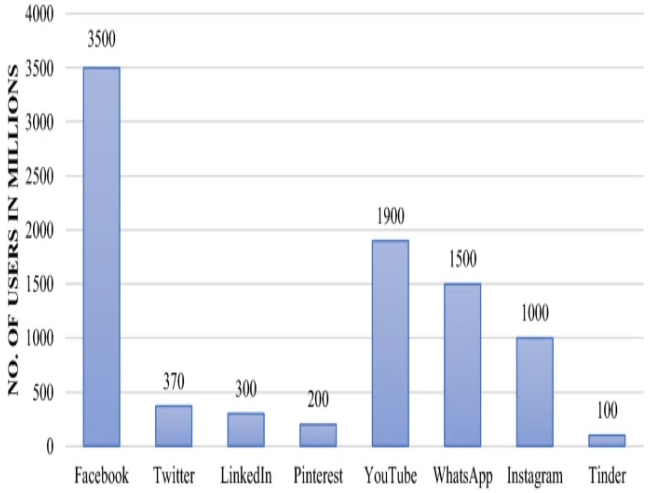

Fig. 1: Social Networking Platforms [11]

Since a huge amount of information and data is uploaded to Facebook, there is a high possibility of a greater security risk inside it, as well as the use of all social networking sites to a large extent so that there is a large amount of data and information available on these sites, which increased the risks of information leakage and opening doors For many electronic crimes such as data breach, privacy spying, copyright infringement [14], and information fraud. Although some social networking sites such as Twitter do not allow disclosure of users' private information, some experienced attackers can infer information by relying on the analysis of user posts and information they share online. The personal information we share through these social networks may provide cybercriminals with enough to obtain our email and passwords[15].

2. *Positive and negative effects of online social networks*

Social networking has changed the way people see the world. It has helped with near-universal accessibility through little effort, for example, Facebook and Twitter have helped millions stay in touch with family and friends. Like many technological revolutions, social networking also has a downside. And we monitor some positive and negative effects of social networks based on public opinion perceptions.

Positive factors of OSN

Various positive factors that drive users to create accounts and use social networking sites to maintain social relationships, marketing of products and platforms, rescue efforts, finding common interest groups of people to connect and share ideas: -

(1) Maintaining Social Relationships Social networking sites have proven to be convenient in keeping pace with the lives of others who matter to us and help to establish friendships and other social relationships[16].

(2) Marketing platform specialists can post work experience and build a network of career-oriented people on sites like LinkedIn or Plaxo that build social networks, help discover better job opportunities, and marketers can influence their audience by posting ads on social media[17].

(3) Social media plays a large role in rescue and recovery efforts during disasters and disasters. Posts are easily managed by social media sites that can reunite missing family members. The public can be kept informed by using the facilities offered by the primary service providers through online social networks and by posting real-time local updates on social media sites. It also helps government officials understand conditions better and make more informed decisions [18].

(4) Finding common groups social networking sites help people find groups of common interest. The audience shares their likes and dislikes, interests, obsessions, ideas, and perspectives for these groups that contribute to creating an open society (2).

Negative factors of OSN

When the public uses social networking platforms, it faces a lot of problems, which many researchers have identified based on information security:

1- **Online bullying:** While making friends is easier on social media, harassers can also easily find victims, the anonymity provided by social networks is a constant problem for social media users, and now any individual can bully someone via these Networks anonymously[19].

2- **Exploiting private information:** Although creating an account on social media sites is free, they mostly earn their money from the ads they display on their websites. The collected data is sold to intermediaries in relationships without the consent of social media users. Moreover, adversaries can also extract confidential information about their targets from these locations using different attack techniques[20].

3- **Isolation:** social media has certainly improved communication between users but on the contrary, it has also avoided real social interaction. And people find it easier to follow the posted comments of people they know than to visit or contact them in person [21].

4- **General addiction:** From records, we can confirm that social media is more addictive than cigarettes and alcohol. People often feel empty and depressed if they do not check their social media accounts for an entire day [22].

3. The role of social networks in creating and shaping Public attitudes:

The importance of electronic Public attitudes has increased in recent years as a result of a group of developments, the most important of which is in communication technology, and the emergence of social networks has played a prominent role in this development, as these sites have become arenas where people with common interests meet about an issue or group of issues of interest to public opinion, and recently appeared New concepts related to a new form of public opinion, which is electronic public opinion as a result of the electronic technical means used in communication in general, and it can be said that there is a new term that expresses the trends of social media users: electronic public opinion, which can be defined that opinion that expresses the largest possible segment of the masses in this vast space on the Internet [23]. Social media plays an active role in creating and shaping public opinion, as it contributes to the promotion of ideas espoused by the elite in society, to become recognized social value and spread among ordinary people, thus influencing their behavior, and shaping their attitudes towards certain issues[24].

This effect is mainly due to the ability of social media, and new media in general, to influence quantitatively through repetition, as social media present similar and recurring media messages about an issue, so this cumulative presentation leads to the conviction of community members. in the long term. In any case, social media has become a major partner in creating electronic public opinion[25].

4. The Sources of Public attitudes formation through social networks:

In social media, different types of messages may serve as potential sources for users to infer public opinion. Walther & Jang have identified three types of messages available in social media technologies, though these can appear in different ways: owner content, overall user representation, and content user-generated [26].

The proprietor content refers to the main messages, such as online news articles, or Facebook status updates including text, images, or videos created or posted by one major author or organization. Aggregate user representations are numerical screens, describing the number of people who performed a particular action on the message[27].

Walther and Jang differentiate between (a) intentional aggregate user representations in the sense of numbers that represent users' intentional actions, such as: liking a post, sharing a message, or rating it. and (b) accidental aggregated displays of descriptive statistics of user behavior that are not turned on for the purpose of indicating anything to others, such as the number of times a video has been viewed on YouTube[28].

Therefore, User-generated content as a third type refers to reactions to online messages by non-owner users, for example, writing text comments regarding the main message or another user-generated comment, and all these

message types may include capabilities different to deliver an atmosphere of opinion to viewers[29].

Regarding inferring public opinion from digital information in social media, studies have shown that messages viewed on SNS with many likes have more general support for this opinion than recipients of viewed messages, which are displayed alongside a small number of likes. User-generated Comments have become a popular way for citizens to express their views on issues discussed publicly. Comments are usually created by a single user, and thus represent an individual's personal situation by presenting someone's personal and narrative experiences and giving vivid examples. and concrete problem or issue. Accordingly, people are expected to make judgments about the way people infer the prevailing opinion climate [30].

5. *Monitoring electronic Public attitudes for threats in social networks towards individuals and organizations*

The term "Information Security" is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity (which means protection against improper modification or destruction of information, ensuring that information is not criticized and credible) confidentiality (which means maintaining authorized restrictions on access and disclosure, including protections for personal privacy and proprietary information), and availability or integrity (which means ensuring timely and reliable access and use of information)[31].

Information security is required because the application of technology to information creates risks. Information may be incorrectly disclosed, inappropriately modified, destroyed, or loss which may result in financial losses and reputational damage [32], and in the context of social networks, particularly improper disclosure of information, i.e., confidentiality, is a risk to individuals and organizations. The researchers found that large-scale social networks pose privacy challenges due to the large amount of sensitive and private information stored in those networks. They argued that the disclosure of personal information in social networks is double-edged. On the one hand, disclosure is a plus or even a must if people want to participate in social networks. On the other hand, disclosure of personal information can lead to hacking and malicious attacks such as phishing, sending spam, distributing malware, facilitating identity theft, and scams [33].

6. *Information security challenges and threats for individuals related to social media:*

With the fast-growing technology, online social networking has grown exponentially over the past few years. The central reason behind this phenomenon is the ability of these networks to provide a platform for users to communicate with their families, friends, and colleagues. The main objective of using them is to share content with the maximum number of users. Individuals use Facebook, Twitter, and LinkedIn to publish their routine activities. Sometimes, they share information about themselves and their lives with friends, colleagues, and at work through status updates or sharing live photos and videos [34].

Currently, many OSN users use smartphones to take photos and create videos to share across OSNs. This data can contain location information and some metadata embedded in it. This was confirmed by a study[1]that the most way to obtain information around the world in 2021 came through identities exposed, and that 91.6% of data penetration led to identity theft or identity theft. As shown in Figure 2.

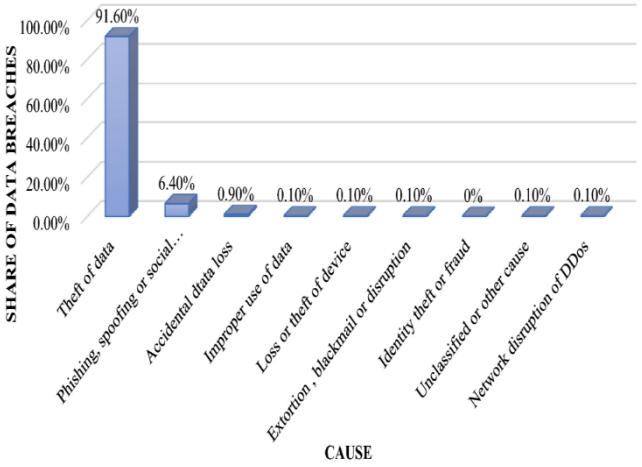

Fig. 2: challenges and threats [1]

As nowadays, geo-tagged photos are very popular, people mark their geo-locations with their photos and share them online, some apps have this geo-tagging feature which automatically tags the current location within the photo until the user converts it manually[35], and this can lead to the disclosure of personal information of the individual, such as where he lives, where he travels to, and this makes him a target for theft, and this can pose a threat to their lives through stalking and potential theft. According to a report issued by Heimdall Security, a Hacking 6 Facebook accounts per day[36].

Because of the great use of social networks in recent years, Internet users have been exposed to many threats related to privacy and information security, and these threats can be classified according to the study into classic and modern threats: -

(1) Classic Threats: These are online threats that not only put OSN users at risk but also other Internet users who do not use them at risk. Although researchers and industries have addressed these threats in the past with the invention of social networks, they are It can spread in a new way and faster than ever before and uses classic threats to extract users' personal information,

which is shared through OSN, to attack not only targeted users but also their peers by modifying the threat to relate to users' private characteristics(4).

(2) Modern Threats: These threats are usually associated with OSN networks, and the focus of modern threats is usually to get the private information of users and their friends, for example, the attacker wants to know information about the user [37], and if the users have their privacy settings on their account On Facebook as public, it can be easily viewed. However, if they have the custom privacy setting, it will only be viewable to their friends. In this case, the attacker can create a fake Facebook profile and send a friend request to the targeted users and when the friend request is accepted, the details are revealed to the attacker. Similarly, an intruder can use a heuristics attack to collect users' personal information from content that is publicly available to their peers [38].

In study (1), threats were divided into three categories: traditional threats, modern threats, and targeted threats. Traditional threats include threats that users have used since the beginning of using social networks, modern threats are attacks that use advanced techniques to compromise user accounts, and targeted attacks are attacks targeting a specific user that can be committed by any user for various personal revenge. As shown in Figure 3.

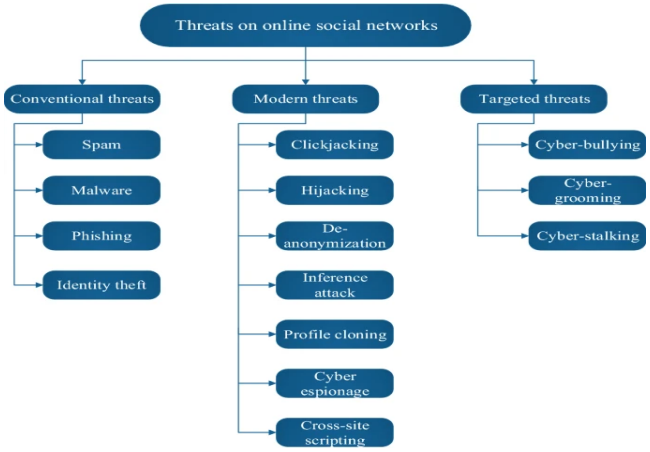

Fig. 3: Types of Threats towards Individuals [1]

Conventional threats:

(1) Spam attack:

Spam is the term used for unsolicited bulk email messages, most spam is commercial advertisements but can also be used to collect sensitive information from users or may contain viruses, malware, or scams. wall or unsolicited instant message[39]. OSN spam is more dangerous compared to traditional spam because users spend more time on OSN, and spam messages usually come from hacked accounts and spam bots. However, most spam spreads from hacked accounts. Spam filtering methods are used to detect a malicious message or a URL in a message and filter it before it is delivered to the target system [40].

(2) Malware attack:

Malware is malicious software that is explicitly developed to infect or access a computer system, usually without user information. An intruder attacker uses various methods to spread malware and infect devices and networks. For example, malware may be installed by clicking on a malicious URL, on the client's framework or may redirect the client to a fake website that seeks private data from the client [4] . Some malicious scripts can be inserted into URLs and clicking URLs can make this script run on a system that may collect sensitive information from that system. In social media platforms, the malware uses the online social networking (OSN) architecture to propagate itself such as several heads, a number of edges, average shortest path, and longest path [41].

(3) Phishing:

A phishing attack is a type of social engineering attack where the attacker can obtain sensitive and confidential information such as the username, password, and credit card details of the user through fake websites and emails that look real. Intruders can impersonate a real user and may use his/her identity to send fake messages to other users via a social networking platform containing a malicious URL[42]. This URL may return the consumer's address to the fake website where it asks for personal information, in the case of SNS, the attacker needs to lure the customer to a fake page where he can perform a phishing attack, and to achieve this, the attacker uses various social engineering methodologies. For example, he could send a message to a user saying, "Your profile pictures are shared on this site, please check!" By clicking this URL, the user is redirected to a fake website that looks like some legitimate social networking site[43].

(4) Identity theft:

In this type of assault, the assailant uses someone else's identity like social security number, mobile number, and address without his permission, with the help of these details, the attacker can easily access the victim's friend list and claim confidential information from them using various social engineering techniques. Since the attacker is impersonating a legitimate user, he can take advantage of this identification in any conceivable way that could seriously affect real customers[44].

Modern threats

(1) Cross-site scripting attack:

Cross-site scripting is a very common attack vector among users. The attack is abbreviated as XSS and known as "Self-XSS", basically, the attack causes malicious JavaScript to be executed on the victim's browser through various techniques. These attacks are categorized as persistent, broken, DOM-based XSS attacks, and the browser can be hacked One click of a button may send a malicious text to the server [45]. This text is returned to the victim and executed on the browser. Attractive links and

buttons on popular social networking sites such as Twitter and Facebook can trick the user to the following URLs (40).

Even worse, some users may feel compelled to copy and paste JavaScript-containing links onto their browser's address bar. These attacks can steal information or act as spyware. Such attacks can also hijack computers to launch attacks on unsuspecting users and the real culprit of the attack is hiding behind the compromised machine [46].

(2) Profile cloning attack:

In this attack, the attacker clones profiles of users that he has prior knowledge. An attacker can use this cloned profile either in the same social networking platform or on a different social networking platform to establish a trusting relationship with the user's real friends. Once the connection is established [47], the attacker deceives the victim's friends into believing the fake profile is correct and successfully captures confidential information which is not shared in their public profiles. This attack can also be used to commit other types of cybercrime such as cyberbullying, online stalking and extortion (4).

(3) Hijacking:

In hijacking, the adversary compromises or takes control of the user's account to carry out online fraud, sites without multi-factor authentication and accounts with weak passwords are more likely to be hijacked as passwords can be obtained through phishing. Once the account is hacked, the hijacker can send messages, share the malicious link, and can change the account information that may harm the reputation of the user[48].

(4) Inferenceattack:

A heuristic attack deduces confidential information of the processor which the user may not want to disclose, from other statistics that the user has placed on some social networking sites. It uses information mining procedures on visually available data such as a user's friend list and network topology. Using this technology, an attacker can discover confidential organization information or user geographic and educational information [49].

(5) Sybil attack:

In this attack, a node claims multiple identities in a network. They can be harmful to social networking platforms because they have many users who are associated through a peer-to-peer network, and peers are computer frames that are connected to each other via the Internet and can share records directly without the need for a central server. A single online entity can create many fake identities and use these identities to distribute junk information or malware [50].

(6) Clickjacking:

An action in which an attacker deceives a user into clicking on a different page than he or she intended to click. The attacker exploits the browser's vulnerability to carry out this attack and loads another page on top of the page the user wants to access, as a transparent layer. The two well-known types of click hacks are hacking and hacking [51]. The front layer shows the essence that can be fed to the customer. The moment a customer clicks on that content, they click the Like button, the more people like the post, the more it will spread. The actual cursor is shifted from the actual mouse position. In this way, the intruder deceives the consumer into clicking on the malicious site through the intelligent configuration of page elements[52].

(7) De-anonymization attack:

On a lot of social networking sites like Twitter and Facebook, users can hide or protect their real identity before releasing any data using a pseudonym or a fake name but if a third party wants to discover the true identity of the user, this can be done simply by linking the information leaked by the social networking sites They use strategies such as cookie tracking, network topologies, and user group affiliation to reveal the true identity of the customer. It is a kind of information mining technique, and an attacker can collect information about a user's group membership by stealing the history from their browser and by merging that history with the collected data. The attacker can thus identify the user who visits the attacker's website[53].

(8) Cyber espionage:

Cyber espionage is an act that uses electronic capabilities to collect sensitive information or intellectual property with the intent of communicating it to conflicting parties. These attacks are motivated by greed for financial benefits and are generally used as an integral part of military activity as evidence of unlawful intimidation. It may cause loss of competitive advantage, material, information, basis, or death toll. A social engineer can perform social engineering attacks using social networking sites. He can get important data like worker assignments, email addresses, etc. using social networking sites [54].

Targeted threats

(1) Cyberbullying:

Cyberbullying is the use of electronic media such as emails, chats, phone conversations, and online social networks to bully or harass a person. Unlike traditional bullying [55], cyberbullying is an ongoing process. The attacker frequently sends intimidating messages, sexual notes, and posts, and sometimes even posts embarrassing pictures or videos to harass someone. He may also post personal or private information about the victim that causes embarrassment or humiliation. Online bullying can also happen accidentally(40).

(2) Cyber grooming:

Online grooming is the establishment of an intimate and emotional relationship with the victim (usually children and adolescents) with the intent to coerce sexual assault [56]. The key point in online grooming is to gain the confidence of a young child and through it can obtain personal and intimate information from the child. The data is often sensual in nature through sexual conversations, photos, and videos that give the attacker an advantage to threaten and blackmail the child. Attackers often approach teens or children through fake child-friendly websites, leaving them vulnerable and unaware that they have come any closer to the goal of electronic grooming (4).

(3) Cyberstalking:

Cyber-stalking is the monitoring of an individual via the Internet, e-mail, or any other type of electronic communication that results in a fear of violence and interferes with that individual's mental peace. It entails a violation of a person's right to privacy [57]. The attacker tracks victims' personal or confidential information and uses it to threaten them with persistent messages throughout the day. This behavior makes the victim exceptionally concerned for his or her safety. Most people these days share their personal information like phone number, place of residence, region, and schedule in their social networking profile. In addition to this, they also share their location-based data. An attacker can collect this data and use it for online stalking [58].

7. *Information security challenges and threats for organizations related to social media*

For organizations and their employees, social media enables new ways to communicate with customers and colleagues, and vast amounts of information are exchanged on social media. This information is a high asset, and therefore information security questions are becoming more and more important. As organizations, institutions and companies are becoming increasingly concerned about social media related to information security (30).

Several studies have examined how social media can be utilized by organizations and indicated that for many of them, social networking technology is used in their marketing efforts, for example, to communicate with customers and attract new customers(13). Examines the tensions that can arise when social networks cross hierarchy, status, or authority boundaries in the workplace (for example, when people feel "compelled" to communicate with their boss, clients, or co-workers) (30). They also discussed questions related to the legality of the use of social media in the workplace and the conflation of private and professional personalities (39).

On the challenges posed by social media to organizations, I identified internal and external challenges similar to these: internal challenges related to resource challenges (such as how employees use their work time), ownership challenges (who is responsible for social media in the company), licensing challenges (i.e. Who is allowed to contribute to social media), situational challenges (i.e. employees' attitudes toward social media use), economic challenges (i.e. costs related to implementing a social media strategy) [59].

External challenges relate to reputation challenges, legal challenges, and identity challenges (i.e., the issue of distinguishing between professional and private identity). This same phenomenon has become a major threat in organizations. According to [60], threats and potential consequences for people sharing information too freely include privacy risks, rejection when applying for a job, dismissal due to inappropriate social media posts, and posts that lead to threats. They further argued that for the organization in which these people work, the free sharing of information can lead to security risks (60).

According to the study (30) of the most important types of challenges and risks in social media from the point of view of information security, they came in the main challenges, which are external attacks on employees or the company, challenges resulting from employee actions or lack of awareness, and challenges related to roles as shown in **table 1.**

Table 1: Social Media Challenge Types and Information Security Risks

Challenge type	**Information security risks**
Outside attacks on employees/company	Malware, Spam, Untrusted applications, Unsafe Internet connection (remote work)
Challenges arising from employees' actions/unawareness	Scams, Phishing, Identity theft, leaking information (intentionally or by accident), Audience blurring, Reputation damage
Challenges related to roles	Social media as a networking tool (customer communication or keeping network of professional peers), Confusion of private and professional identity, social media as 'the next media'

Many researchers have found that challenges arising from employee actions or unconsciousness appear to present greater information security risks than challenges posed by external attacks. Account management appears to be a major information security concern for social media-related businesses. There can be many risks due to the actions of employees in social media (30), which are also often the result of a lack of awareness of certain threats or characteristics of social media. These risks are related to phishing, identity theft, information leakage, reputational damage, and public image distortion on social media. The risks related to scams and phishing were greater in those organizations that clearly had confidential data protection.

Here, social media is seen to easily gather information about others (13).

It has also been found that confusing private and professional roles is more of an information security risk than collaboration and communication in social networks, since whether the private and professional roles can be distinguished, and social media identity is highly dependent on the employee's position in the company. Also, companies and employees use social networks to collaborate and communicate with co-workers and customers. From an information security perspective, this is particularly challenging when communication, collaboration, and participation are initiated and shared by employees without being pushed by the company, as in many cases private and professional employees are more likely to mix roles. One challenge is how to determine which employees are allowed to interact with others on social media [61].

3 Solutions for various threats

Many researchers in both academia and industries have constantly tried to find solutions to the above threats in social media. They have suggested many solutions and some methods to combat these threats:

- Security and privacy settings: Many social networking sites provide security and privacy settings to enable the user to protect their personal information from unwanted access by strangers or applications. For example, a Facebook user can modify their security settings and select the audience (such as friends, friends of friends, and everyone) in the network who can see their details, photos, posts, and other sensitive information. Furthermore, Facebook also allows its users to either acknowledge or deny third-party apps' access to their personal information. Many social networking sites were equipped with internal security measures for the regime(30).

- Report users: Online social networks protect users from being harassed by providing a means to report any form of abuse or policy violations by any user in their network. For example, if a user sees something on Facebook that is objectionable to an individual's feelings, but does not violate Facebook's terms, the user can use the report links to send a message to someone who posted it asking them to remove it (61).

4 Security guidelines for OSNs user

- **Use a strong password**: To keep accounts secure, it doesn't have to be too short because short passwords can be easily guessed. It should be long enough and should contain alphanumeric values with some special characters. Users should not use the same password they use for other accounts because if an attacker somehow manages to figure out that password (13), he can hack all of that user's accounts. So, choosing a strong password can help the user to protect their account and prevent unauthorized access (51).

- **Limit location sharing:** Nowadays, many social networking sites have also introduced a geolocation feature which automatically determines the user's geolocation when the user uploads any multimedia on social media, the user must switch it to manual so as not to flag location automatically. Sharing the location online makes the user vulnerable to real-life crimes such as theft (4).

- **Be selective with friend requests:** It is noticeable that many users accept friend requests without analyzing the complete profile of the applicant and generally people accept friend requests based on mutual friends if there are some mutual friends then they accept it, sometimes attackers make their profile intentionally attractive, or they may impersonate an account. So, if the person who sent the friend request is unknown, they should ignore that friend request. It could be a fake account trying to steal sensitive information (1).

- **Be careful what you share:** Users should be careful about their posts as they may reveal their personal information and sometimes others too. Many organizations maintain strict rules and regulations for sharing information and multimedia content. There are many reports of people giving up their jobs because of illegally sharing information. This situation can be avoided if employees are well versed in the protocols of the organization in which they work regarding the photos, videos, and messages they post online. Unlawful sharing of information can damage the organization's good reputation in the marketplace along with its data and intellectual property as well (50).

- **Be aware of links and third-party applications**: Unauthorized users can access someone's account and obtain sensitive information by sharing a malicious link. And nowadays short URLs are very popular on various social media platforms. These short URLs may be obfuscated with malicious code or script. These scripts attempt to collect personal and confidential user information that may violate that user's privacy. Moreover, hackers may take advantage of vulnerabilities found in a third-party application that is integrated with many popular social networks (50).

One example of this third-party application is games that can be played on online social networks that ask for the user's public information to consume their services. This collected information may be provided to third parties or third-party interventions. To avoid this risk, the user should be careful while installing third-party applications in their profile (51).

- **Install internet security software:** Some known threats can easily be detected by antivirus software. Threats such as online grooming and cyberbullying can be detected to some extent with antivirus software. Many malicious

links can be shared by our friends without their knowledge which will redirect the user to a phishing website. And your antivirus software should be updated regularly because there are many viruses that are being tackled by hackers daily (1). Some social networking sites also have their own security tools that users can use to protect themselves from cyber-attacks.

5 Conclusion

This paper provides a comprehensive review of various security and privacy threats related to information and current solutions that can provide security for users of social networks by citing some statistical reports. In addition to this, we discussed various defensive approaches to OSN security by monitoring relevant security guidelines to achieve trustworthiness in online social networks for individuals and organizations.

Conflict of interest

The authors declare that there is no conflict regarding the publication of this paper.

References

[1] Ankit Kumar Jain,Somya Ranjan Sahoo,&Jyoti Kaubi yal, Online social networks security and privacy:comprehensive review and analysis.Complex&IntelligentSystems (2021),Published: 01 June 2021, .(2021). https://link.springer.com/article/10.1007%2Fs40747-021-00409-7.

[2] Jeong, Y. & Kim, Y.Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. Computers in Human Behavior**(69)**, pp302-310, (2017).

[3] Mandeep Singh ,Chaman Verma, & Pamela Juneja , Social media security threats investigation and mitigation methods: A preliminary review, Journal of Physics, Conference Series**(1706)**,(2020), doi:10.1088/1742-6596/1706/1/012142

[4] Shaukat Ali, Naveed Islam , Azhar Rauf , Ikram Ud Din & Mohsen Guizani and Joel J. P. C. Rodrigues.Privacy and Security Issues in Online Social Networks. Future Internet 10**(12)**,p114,(2018). https://doi.org/10.3390/fi10120114

[5] Annica Santdstro, The Performance of Policy Networks.The Relation Between Networks Structure And Networks Performance.The Policy Studies Journal, 36**(4),**Published By Wiley Periodicals,Oxford,Pp 497-505(2018).

[6] Brainard, L. & Edlins, M,Top 10 US municipal police departments and their social media usage. The American Review of Public Administration, 45 (6), pp 728-745.(2015).

[7] Ellison, N. & Hardey, M,Social media and local government:citizenship, consumption and democracy, Local Government Studies. **40 (1),**pp21-40 (2014).

[8] Eun Sun Lee& Kyujin Jung. Dynamics of social economy self-organized on social media:following social entrepreneur forum and social economy network on Facebook.QualQuant(2018**),(52),**pp635–65,(2018).©SpringerScience+Business Media B.V.,part of Springer Nature 2018.

[9] Jonathan A.Obarn., Social media definition and the governancen challenge: An introduction to the special issue .Faculty of Social Science and Humanities,University of Ontario,Institute of Technology,Canada, Editorial/ Telecommunications Policy **(39)**,PP 745–750,(2018).

[10] Lisa McDermott, Online news comments as a public sphere forum: Deliberations on Canadian children's physical activity habits. International Review for the Sociology of Sport 2018, **53(2)**,pp173–196,(2018).

[11] Number of social network users worldwide from 2017 to 2025, Statista [Online]. https://www.statista.com/statistics/278414/numberof-worldwide-social-network-users/. Accessed 14 oct 2021.

[12] Digital Marketing Consultants—SEO Consulting—Zephoria Inc. (Facebook-Stats-Q2-2021.png (800×2000) (zephoria.com,2021),[Online]https://zephoria.com/wp-content/uploads/2021/09/Facebook-Stats-Q2-2021.png Accessed 13 oct 2021.

[13] Gupta BB,& Sahoo SR, Online social networks security: principles, algorithm, applications, and perspectives. CRC Press,(2021) .

[14] Lan Ye&Yunjae Cheong,Using Facebook efficiently:Assessing the impact of organizational Facebook activities on organizational reputation. Corporate Communications: An International Journal, **22 (4),** pp440-454,(2017).

[15] Kristina Horn Sheeler,Texts and Tweets from Hillary:Meta Meming and Postfeminist Political Culture.Special Issue:Symposium on Screening the Presidency,**44(2)**,Pp201-380,(2015).

[16] Colicev A, Malshe A, Pauwels K& O'Connor P, Improving consumer mindset metrics and shareholder value through social media: the different roles of owned and earned media. J Mark **82(1),**pp37–56,(2018).https://journals.sagepub.com/doi/full/10.1509/jm.16.0055.

[17] Liu F& Xu D, Social roles and consequences in using social media in disasters: a structurational perspective. Inf Syst Front **20(4),**pp693–711,(2018).https://link.springer.com/article/10.1007%2Fs10796-017-9787-6.

[18] DanKetchum ,The Positive and Negative Effects of Social Networking,Techwalla.com[Online] ,(2019). https://www.techwalla.com/articles/the-positive-and-negative-effects-of-social-networking. Accessed 23 oct 2021.

[19] BEN STEGNER,Negative Effects of Social Media on People and Users,(2020). https://www.makeuseof.com/tag/negative-effects-social-media/. Accessed 24 oct 2021.

[20] Zhu Y, Xu B, Shi X & Wang Y ,A survey of social-based routing in delay tolerant networks: positive and negative social effects. IEEE Commun Surv Tutorials **15(1)**,pp387–401.(2013).https://ieeexplore.ieee.org/abstract/document/6177189

[21] Groth, G.G., Longo, L.M. & Martin, J.L. ,Social media and college student risk behaviors: A mini-review. Addictive behaviors**(65),** pp.87-91,(2017).

[22] Wolniewicz CA, Tiamiyu MF, Weeks JW& Elhai JD. ,Problematic smartphone use and relations with negative affect, fear of missing out, and fear of negative and positive evaluation. Psychiatry Res**(262)**,pp618–623,(2018).https://www.sciencedirect.com/science/article/abs/pii/S0165178117309010

[23] Moon J. Lee& Jung Won Chun., Reading others'comments and public opinion poll results on social media:Social judgment and spiral of empowerment. Department of Public Relations, University of Florida, United States,Computers in Human Behavior**(65),**PP479-487,(2018).

[24] Muhammad Zubair Khan,.Revitalization of the Public Sphere: A Comparison between Habermasian and the New Public Sphere. Department of Political Science , GomalUniversity,AUDC.8 **(1)**,pp41-57,(2014). http://journals.univ-danubius. ro/index.php/communicatio/article.

[25] Philip Pond & Jeff Lewis,Riots and Twitter:connective politics,social media and framing discourses in the digital public sphere . JournalInformation, Communication & Society , 22**(2),**Pp213-231,(2019).

[26] Walther,J. B.,& Jang,J.-W. ,Communication processes in participatory web Sites.Journal of Computer-Mediated Communication, **18**,pp2–15,(2012).

[27] William,This is why white evangelicals still support Donald Trump.(It's not economic anxiety.(2019).(June19-2019).https://www.washingtonpost.com/news/monkey-cage/wp/2018/06/19.

[28] Yun Wang,Michel Rod,Shaobo Ji & Qi Deng. Social media capability in B2B marketing:toward a definition and a research model. Journal of Business & Industrial Marketing, 32 **(8)**. pp1125-1135,(2016).

[29] Tsung-Yi Chen,Meng-Che Tsai ,&Yuh-MinChen, A user's personality prediction approach by mining network interaction behaviors on Facebook. Online Information Review, 40**(7),**pp913-937,(2017).

[30] Peter Bellström,Monika Magnusson,John Sören Pettersson & Claes Thorén, Facebook usage in a local government:A content analysis of page owner posts and user posts. Transforming Government, People,Process and Policy,10 (4), pp548-567,(2017).

[31] Hekkala Riitta, Väyrynen Karin,& Wiander Timo, Information Security Challenges of Social Media for Companies. ECIS 2012 Proceedings, P56,(2012).https://www.researchgate.net/publication/264894370_Information_Security_Challenges_of_Social_Media_for_Companies Accessed 15 oct 2021.

[32] Proserpio,D & Zervas,G,Online reputation management:estimating the impact of management responses on consumer reviews. Marketing Science,(2017).

[33] Zlatolas, L.N., Welzer, T., Heričko, M.& Hölbl, M,Privacy antecedents for SNS selfdisclosure: The case of Facebook. Computers in Human Behavior45, pp158-167,(2015).

[34] Manetti,G. & Bellucci,M. (2016). The use of social media for engaging stakeholders in sustainability reporting. Accounting,Auditing &Accountability Journal 29**(6),**pp985-1011.

[35] Data breach causes worldwide :2016|Statistic[Online].https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/. Accessed 22 oct 2021.

[36] Heimdal Security—Proactive Cyber Security Software[Online] https://heimdalsecurity.com/en/. Accessed 9 Nov 2021.

[37] Imrul Kayes &Adriana Iamnitchi. ,Privacy and security in online social networks: A survey. Online Social Networks and Media, **3(4)**, October2017,Pp 1-21(2017). https://doi.org/10.1016/j.osnem.2017.09.001

[38] Aggarwal A, Rajadesingan A & Kumaraguru P ,PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime, pp1–12,(2012).

[39] Rathore S, Loia V&Park JH , SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook.Appl Soft Comput**(67),**pp920–932,(2018).https://www.sciencedirect.com/science/article/abs/pii/S1568494617305719

[40] Michalopoulos D, Mavridis I& Jankovic M,.GARS: Real-time system for identification, assessment and control of cyber grooming attacks.ComputSecur**(42),**pp177-190,(2014).https://doi.org/10.1016/j.cose.2013.12.004

[41] Grosse K, Papernot N, Manoharan P, Backes M& McDaniel P,.Adversarial examples for malware detection. Springer, Cham, pp 62–79,(2017).https://link.springer.com/chapter/10.1007/978-3-319-66399-9_4

[42] Jakobsson M,Two-factor in authentication—the rise in SMS phishingattacks.ComputFraudSecur2018**(6),** (2018),pp68.https://doi.org/10.1016/S1361-3723(18)30052-6

[43] Chen J, Mishler S, Hu B, Li N& Proctor RW .(2018) .The description-experience gap in the effect of warning reliability on user trust and performance in a phishing-detection context. Int J Hum Comput Study (119),pp35-47.https://www.sciencedirect.com/science/article/abs/pii/S1071581918302763

[44] Wani, M.A., Jabin, S.,& Ahmad, N.(2018). A sneak into the Devil's Colony-Fake Profiles in Online Social Networks.https://arxiv.org/ftp/arxiv/papers/1705/1705.09929.pdf, (accessed on 29 October 2021).

[45] Chaudhary P& Gupta BB,.Plague of cross-site scripting on web applications: a review, taxonomy and challenges. Int J Web Based Communit 14**(1),**p64,(2018).

[46] Bukhari SN, Ahmad Dar M & Iqbal U ,Reducing attack surface corresponding to Type 1 cross-site scripting attacks using secure development life cycle practices. In 2018 fourth international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB), pp 1–4,(2018).

[47] Fire M, Goldschmidt R& Elovici Y,Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials .**16(4)**, Fourthquarter2014),pp2019–2036,(2014).DOI: 10.1109/COMST.2014.2321628

[48] Xin Y, Zhao C, Zhu H, & Gao M,A Survey of Malicious Accounts Detection in Large-Scale Online Social Networks. In: 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), pp 155–158,(2018).

[49] Mei B, Xiao Y, Li R, Li H, Cheng X & Sun Y,.Image and attribute based convolutional neural network inference attacks in social networks. In: IEEE Trans. Netw. Sci. Eng, pp 1–1,(2018).

[50] Jan MA, Nanda P, He X,& Liu RP ,A Sybil attack detection scheme for a forest wildfire monitoring application. Future Generation ComputerSystems**(80),**March2018,Pp613626,2018). https://www.sciencedirect.com/science/article/abs/pii/S0167739X16301522

[51] Sinha R, Uppal D, Rathi R,&Kanwar K , Combating clickjacking using content security policy and aspect oriented programming. Springer, Singapore, pp323–331,(2018).https://link.springer.com/chapter/10.1007/978-981-10-3773-3_32

[52] Albladi SM & Weir GRS, A semi-automated security advisory system to resist cyber-attack in social networks. Springer, Cham, pp 146–156,(2018). https://link.springer.com/chapter/10.1007/978-3-319-98443-8_14

[53] Mao J, Tian W, Jiang J, He Z, Zhou Z& Liu J, Understanding structure-based social network de-anonymization techniques via empirical analysis. EURASIP Journal on Wireless Communications and Networking **(1),**p279,(2018).https://link.springer.com/article/10.1186/s13638-018-1291-2

[54] Ghalaty NF& Ben Salem M ,A Hierarchical Framework to Detect Targeted Attacks using Deep Neural Network.In: 2018 IEEE International Conference on Big Data (Big Data), pp 5021–5026,(2018).

[55] Holfeld B& Mishna F,Longitudinal associations in youth involvement as victimized, bullying, or witnessing cyberbullying . Cyberpsychology,Behavior,andSocialNetworking**.21(4)**,pp234239,(2018).https://www.liebertpub.com/doi/abs/10.1089/cyber.2017.0369

[56] Ngejane C, Mabuza-Hocquet G, Eloff JH & Lefophane S , Mitigating online sexual grooming cybercrime on social media using machine learning: a desktop survey. In 2018 international conference on advances in Big Data, computing and data communication systems ,(icABCD) pp 1–6,(2018).

[57] Cyberstalking|GetSafeOnline[Online].https://www.getsafeonline.org/protecting-yourself/cyberstalking/. Accessed 15 Nov 2021.

[58] How to avoid becoming a cyberstalking victim |Association for Progressive Communications [Online]. https://www.apc.org/en/pubs/issue/how-avoid-becoming-cyberstalking-victim. Accessed 15 Nov 2021.

[59] Dijkmans,C.,Kerkhof,P.& Beukeboom,C.J,A stage to engage: social media use and corporate reputation. Tourism Management **(47),**pp58-67,(2015).

[60] Allen, J.P.,Social Media Risks. The Latest Potential Disasters Outlined. http://www.jpedia.org/wp/archives/383. Accessed 15 oct 2021,(2015).

[61] Raymond Henry &Lisa Bosman,Strategic Management and Social Media:An Empirical Analysis of Electronic Social Capital and Online Fundraising. In Social Media in Strategic Management **(11).** pp115-127,(2017).