DOI: http://dx.doi.org/10.26483/ijarcs.v10i2.6384

ISSN No. 0976-5697

Volume 10, No. 2, March-April 2019

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# THE IMPACT OF CYBER THREATS ON SOCIAL NETWORKING SITES

Hilal Almarabeh
King Saud Bin Abdul-Aziz University for Health Sciences
College of Science and Health Professions
Riyadh, Kingdom of Saudi Arabia

Amjad Sulieman
King Saud Bin Abdul-Aziz University for Health Sciences
College of Science and Health Professions
Riyadh, Kingdom of Saudi Arabia

*Abstract:* Social networks are websites that enable people to communicate with others, express their opinions, and share their thoughts, experiences, and interests. It also contributes to job creation and facilitates the marketing of various products and services. A cyber threat is the malicious attempt to access a computer network through a data communications pathway by illegal means; they can be intended or unintended, direct or indirect, and are usually carried out by hackers, virus code writers, industrial spies, organized crime unions, vengeful employees and spiteful intruders. This paper presents the history of online social networking and classifies their types; it also discusses cyber threats on social networking websites and puts forward a policy and action plan to counter threats to social networks in the future.

***Keywords:*** Social Networking Sites, Cyber Threats, Security Issues, Risk Prevention, Threats Vulnerabilities.

## I. INTRODUCTION

The tremendous growth in the use of information technology and the increasing reliance on social networks around the world has become particularly marked in recent decades due to its great value at all levels of professional and personal life, raising productivity and solving issues and to facilitate an easier way of life. Human interaction has become increasingly dependent on instant and continuous communication through the Internet in general and social networking sites in particular, in addition to e-mail, information exchange, e-learning, and various other applications and uses in professional and non-professional domains. With the popularity of mobile devices and applications, combined with social networking technologies, communication using online social networking tools has become a new way of life for people [1].

As a result of the increasing need for managing with information technology, threats have increased which hinder progress and prevent complete control over data and information. Malicious programs have spread in various ways and are evolving continuously in their complexity, making it more difficult to stop their negative and often destructive effects. Data piracy has increased in recent years at the institutional level, as well as on the level of the private user.

Users often take various risks with their personal information when utilizing social networks services; for example, users are prone to using unapproved programs, misusing corporate PCs, accessing unapproved networks, and sharing sensitive data on unsecured networks [2].

In recent years there has been a significant increase in the rate of use of social networks at the global level. For example, Facebook has now surpassed 2.25 billion monthly active users, making the issue of piracy of user data and the privacy of such information very important.

## II. SOCIAL MEDIA NETWORKING

In recent years, the number of social networking sites has increased alongside the diversity of its objectives and uses, and this is made more complex by the increasingly large number of users. Social networking sites vary in characteristics and objectives, and can be divided into a number of groups in light of their objectives, such as follows:

### *A.* Contact Sites

The main purpose of this site is to exchange data and communicate between friends, in addition to increasing the number of user groups of a given similar interest. the LinkedIn site is an example of a social networking site that connects colleagues and classmates in order to build a network that can help advance a user’s career.

### B. Social Networking Sites

The main purpose of this type of site is to locate friends and participate in their virtual lives. Well-known examples include sites such as Facebook, WhatsApp, Twitter. Although these sites were established in order to cater to private individuals, at there are now many institutions that have started to use and exploit such sites for professional and commercial purposes.

### C. Visual Information Sharing Sites

These sites allow users to publish videos and personal photos. They also allow users to upload movies and television programs. The most important of these sites is YouTube.

### D. Virtual Realty Site

These are sites that create a virtual 3D environment by simulating reality. Many of these kinds of sites, like Second Life, offer virtual interactive games that attract young people.

Social media platform such as Facebook, LinkedIn, Instagram, MySpace, Snapchat, Twitter, YouTube, and others that involve individual users as well as multiple organizations have emerged as new communication platforms in today’s dynamic and complicated Internet based business world [3]. The service structure of social networking shown in Figure.1, demonstrates the framework of social networking system.

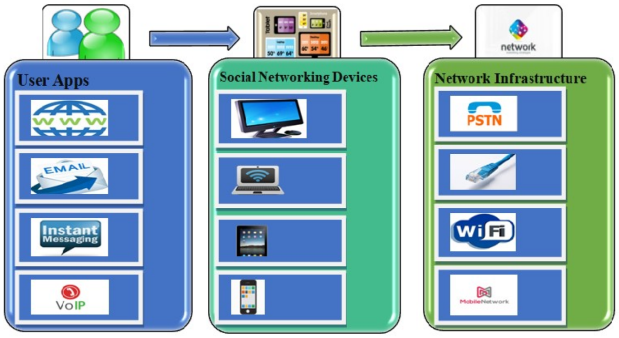


Figure 1. Social Networking Framework

The structure is divided into three main parts. The first part shows user applications that include various services such as web, email, instant messaging voice over IP, and other services. The second part shows social network devices that consist of non-portable devices such as desktop computers and portable devices such as mobile phones. The last part shows network bases or infrastructures which include public switched telephone network, networking cables, wireless network (WLAN), and cellular network.

The growth of the number of social media users in recent years is a widely acknowledged phenomenon. The Statista Company has recorded a steady growth in the number of users in most countries from 2010 to 2018[4]. Figure.2 shows this significant growth in the number of users during the same period.

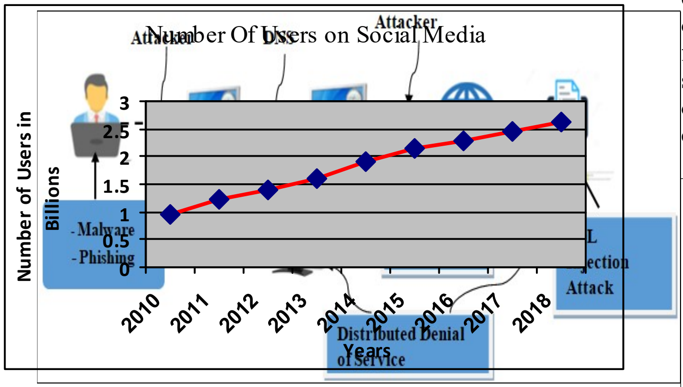


Figure 2. Number of Social Media Users

Social networks are widely available in various languages, and users can be connected with other users across the world. Figure.3 shows the most famous social network sites worldwide ranked by the number of active users as recorded by the Statista company in 2018[4]. Concomitant with the continued development of the Web, the rate of user participation has increased and changed the way users interact with networks; from roaming and surfing between sites in order to access information, to interacting with social networking sites, a natural consequence of the evolution of the web itself.

## III. Cyber Threats to Social Networking

The interaction between users of social networks is the key factor in determining many online trends whether they be commercial, professional, social, or otherwise. Furthermore, many companies, institutions, and individuals have learned to use social networks such as Facebook, Twitter and LinkedIn in order to interact with colleagues and customers.

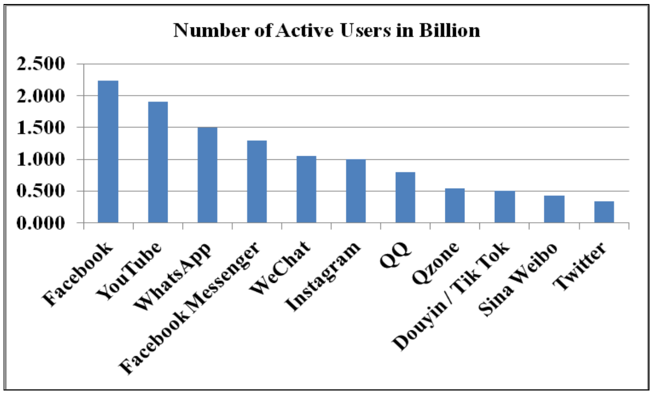


Figure 3. Total Number of Social Media Users

As a result of this rapid growth in the use of social networking sites, threats such as malicious software, computer viruses, and spyware have increased, targeting confidentiality and data security. There are two types of internet and social networking threats; classic threats and modern threats. Classic threats render all users on a given network susceptible to attack; modern threats are related to online social network users only because of the Online Social Networking (OSN) infrastructure that can compromise user privacy and security [5].

### *A.* Classic Threats

Since the advent of the Internet, classic threats have emerged and their issues have increased with the development of the Internet and social networking applications. The most famous threats are malware threats, phishing threats, cross-site scripting attacks, SQL injection attacks, and distributed denial of service (DDoS) attacks. Figure.4 shows the different types of classical threats.

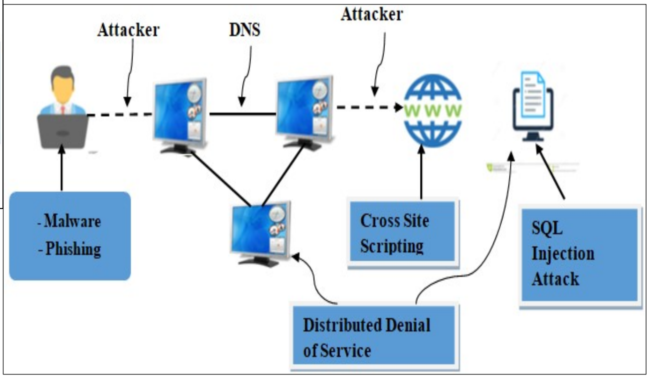


Figure 4. Different Types of Classic Threats

- Malicious software or malware are designed to access a private user’s contents which is often relatively easy to access due to the nature of communication between users. The most common types of malware are adware, bots, bugs, ransomware, rootkits, Trojan horses, spyware, viruses, and worms. The most pernicious forms of malware are those that access a user's credentials and pretend to be legitimate to users. One example of an online social networking malware is Koobface which spread through social networks such as Facebook, Twitter, and Myspace. It was used to collect login credentials and make the target-infected computer a part of a botnet [6]. Committing fraud and propagating malware are criminal actions wherein users are engaged to access a URL and run a malicious code on the computer of an OSN user [7].

- Phishing threats are another type of cyber-attack in which the intruder sends a malicious link or an attachment file by email in order to get personal information such as login information, credit card information, and online banking information. In a phishing attack, attackers often use social engineering and other public information resources, including social networks like LinkedIn, Facebook and Twitter, gathering background information about the victim's personal and work history, interests and activities [8]. For example, during an attack that was attributed to Chinese intelligence services, senior U.K. and U.S. military officials were tricked into becoming Facebook 'friends' with someone impersonating the U.S. Navy Admiral James Stavridis [9]. Similarly, social media were used in many places by hackers posing as other persons [10].

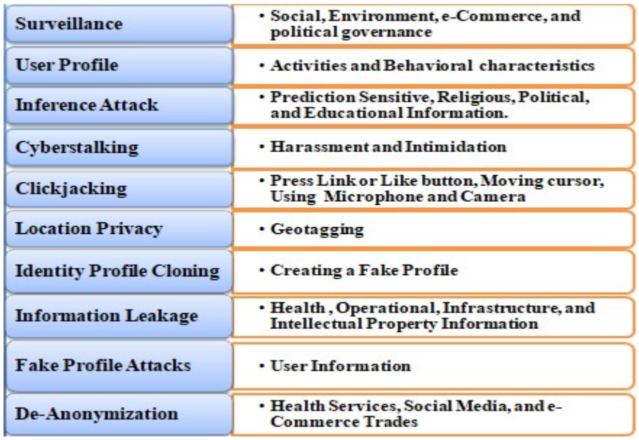
- Cross-Site scripting (XSS) is considered one of the most common forms of attack on web-based applications. Attackers use malicious code and inserted it into web applications to be executed in a user's browser. XSS can affect a victim by stealing cookies, modifying a web page, capturing clipboard contents, key logging, port scanning, and dynamic downloads [11]. Furthermore, an attacker can use XSS with a social-network infrastructure and develop an XSS worm that can be virally spread on online social networks [12]. XSS attacks can be categorized into three parts: the first is 'stored/persistent' in which a malicious script code is saved in the server and it is executed when the user visits the webpage; the second is 'reflected/non persistent' in which a potential victim provides input to the webpage after which attacks are executed, then malicious scripts are saved with links and spread throughout the internet via email or social networking sites; The last one, 'local/document object model', is a client side script where attackers are able to access sensitive information from a victim's computer.

- Distributed denial of services (DDoS) attacks involve an attempt to compromise a system's resources by way of disrupting network bandwidth, rendering such resources unavailable to users. Attacks are initiated from multiple resources such as computers, routers, IoT devices, and other endpoints that are infected by malicious software controlled by the attacker. The most common DDoS types are TCP synchronize flood attack, ping of death attack, teardrop attack, buffer overflow, and Smurf. Since DDoS is typically spread in social media, users have no idea that they've infected their system and spread the malicious software to other computers. Users will always be vulnerable to the spread of malicious software [13]. In 2000, Yahoo, eBay, and Amazon were attacked by DDoS which temporarily disabled their websites. Attackers also targeted the search engine Yahoo and attacked their servers on some remaining sites. In 2002, the New York Times servers were hacked, costing the newspaper $300,000 to rectify. In October 2010, an attack was carried out on MasterCard, PayPal, Visa and Post Finance. Another attack was launched in support of WikiLeaks and lasted more than 16 hours. In November an attack of the magnitude of 10 Gbps was launched on WikiLeaks to prevent the release of secret cables [14]. Some of the largest attacks were reported in 2016, 2015 and 2014, where 600, 500 and 400 Gbps respectively, by ARBOR Networks [15].

- SQL injection attacks allow attackers to have unrestricted access to database applications that contain sensitive information. SQL injection attacks have various targets such as extracting data, executing remote commands, modifying data, performing denial of service, performing database finger printing, evading detection, bypassing authentication, determining database schema, and identifying inject able parameter. In addition, attackers use various methods depending on the target such as blind SQL injection, piggybacked, tautologies, timing attack, inference, stored procedure, and union queries. Web applications with a database that stores important information are one of the prime targets of the SQLIA, since the databases are easily accessible by attackers injecting SQL queries that are retrieved by web applications. As user information is frequently kept in these databases, important information is lost and security violated [16]. SQL injection is recorded as one of the main and top 10 vulnerabilities of web applications between 2007 -2010, as certified by the Open Web Application Security Project [17]. Some of the latest SQL injection attacks were perpetrated against the NestGEN gallery plugin and the California based company Airsoft GI. In 2017, NextGEN was attacked using SQLI to access their database that stores very sensitive user details; researchers said that the attackers used two methods to steal user data [18]. In 2017 also, Airsoft GI forum were attacked and hackers stole information regarding 65,000 accounts that included personal details of registered users. Hackers had also stolen information relating to 40,000 Gmail accounts, 2,500 Outlook accounts, 3,000 Yahoo accounts, 2,500 Hotmail accounts [19].

## *B.* Modern Threats

In a typical manner, these threats are associated with online social networking. They aim to acquire users' personal information in addition to that of their friends. On social networking sites such as Facebook, intruders target a user's privacy setting because it's very important to them. In this way, if personal information is made public, an attacker can easily view this information; otherwise, an attacker can send a friend request to targeted users who have a customized setting. After that, and upon the acceptance of a friendship request from the targeted user, their personal information is revealed. The most modern threats are Surveillance, User Profiling, Inference Attacks, Cyberstalking, Clickjacking, Location Privacy Leakage, Identity Clone Attacks, Information Privacy Leakage, Fake Profiles, and De-Anonymization Attacks. Figure.5 classifies modern threads and information that is likely to be targeted.



| | |
|---|---|
| Surveillance | • Social, Environment, e-Commerce, and political governance |
| User Profile | • Activities and Behavioral characteristics |
| Inference Attack | • Prediction Sensitive, Religious, Political, and Educational Information. |
| Cyberstalking | • Harassment and Intimidation |
| Clickjacking | • Press Link or Like button, Moving cursor, Using Microphone and Camera |
| Location Privacy | • Geotagging |
| Identity Profile Cloning | • Creating a Fake Profile |
| Information Leakage | • Health , Operational, Infrastructure, and Intellectual Property Information |
| Fake Profile Attacks | • User Information |
| De-Anonymization | • Health Services, Social Media, and e-Commerce Trades |

Figure 5. Modern Threads and Information likely to be Targeted

- The surveillance of social networking sites, which is also known as listing and measurement, is a new type of monitoring used to track and obtain user's information, either for individuals, groups, organizations, or companies. Social media networking surveillance is a technology-based surveillance in which human activities are monitored on social media [20]. For example, Facebook allowed the firm Cambridge Analytica to gain access to millions of profiles without the informed consent of users in order to use the information gleaned for political campaigning. The company is claimed to have analyzed social media posts belonging to millions of users in order to create their psychological profiles which were then used for targeted messaging to have an effect on voting patterns. More deliberate monitoring of individuals often takes place in an adversarial and inquisitorial context, increasingly using technical means to gather and analyze data, and is used for social, environmental, economic, or political governance [21].

- User profiling involved the recording and analysis of a user's activities in relation to both psychological and behavioral characteristics by using various methods, such as neural networks, genetic algorithms, and association rules. User profiles contain various contents such as interests, skills, knowledge, goals, and user behaviors. User profiling by inferring users' age, gender and personality traits play an important role in providing personalized services, viral marketing, recommender systems and tailored advertisements [22]. Online service providers perform user profiling for commercial purposes; however, it can open up the way for privacy leakage [23].

- Inference attack is used to predict users' personal information. In this type of attack, the attackers illegally access user's information by using different data mining techniques to predict useful information. Online social media users may not want to reveal their personal and sensitive information such as religious, political affiliations, home address, education, preferences, age, and gender. Specifically, the attacker could be any party (e.g., cybercriminal, online social network provider, advertiser, data broker, and surveillance agency) who has interests in users' private attributes. To perform such privacy attacks, the attacker only needs to collect publicly available data from online social networks [24]. The information on online social media that are detected must has privacy. However, the attacker can use data mining techniques to predict the private information. A mutual-friend-based attack can be used to find the common neighbor of any two users [25]. A principal component analysis (PCA) technique is used to predict the attributes of a user based on their other public attributes that were available online [26]. Facebook was used to test PCA techniques to deduce different user's attributes, such as location and educational background.

- Cyberstalking is occasionally indicated to as online stalking or e-talking. It is a crime where the attackers harass or threaten other users through social networking sites, instant messaging, email, or any others. Harassment behavior involves harassment and intimidation and may include following up or monitoring the victim personally. Common types of cyberstalking are; the composed cyber-stalker, the collective cyber-stalkers, the intimate cyber-stalker, and the vindictive cyber-stalkers. The attackers in cyberstalking rely on anonymity to follow up their victim without being revealed to them or others. A survey was conducted in 2015, the survey was to examine U.S. women's experiences with and attitudes toward cyber harassment by way of an anonymous electronic survey A total of (293) women were asked, where the participants of the survey were selected from different OSN sites in their research. The majority of participants (58.5%) were students at a college or university. About (20%) of women repeatedly received an unsolicited sexually obscene message and/or sexual solicitation on the internet. More than (10%) repeatedly received pornographic messages from someone they did not know, whereas more than a third of them experienced cyber-harassment reported feeling anxious and one-fifth indicated they noticed changes in their sleeping and eating [27]. Another survey was conducted in July 2017, the Pew Research Center's American conducted a survey of 4.248 U.S. adult's internet users' experiences with online harassment. The result was the percentage of American have been personally subjected to harassing behavior online was (41%), and (66%) have witnessed harassing behaviors directed at others. In some cases, these practices are restricted to attitudes that can be ignored as an annoyance of online life. However, nearly one-in-five Americans (18%) have been subjected to particularly severe forms of harassment online, such as physical threats, harassment over a sustained period, sexual harassment or stalking. [28].

- Clickjacking also known as a user interface redress attack, it is an attack that tricks the user to click on a hidden element such as button or link, that they unintended to click. This can cause users to visit a malicious webpage or download malware. For instance, the attackers can trick the online social media users to click a "like" button on a Facebook to links unknowingly. Several variations of clickjacking attack such as likejacking, cursorjacking, drag-and-drop, strokjacking, and others. The attackers can even use the hardware of user computers, for example, a microphone and camera, to record their activities [29]. In 2016, according to the Vulnerability Statistics Report by Edgescan, (61%) of the web application vulnerabilities lead to browser attacks and in 2017, (27%) of all vulnerabilities were associated with web applications and (73%) were network vulnerabilities [30].

- Location privacy leakage is another type of privacy threat. In order to the popularity in using smart phone devices and because it easily to use, it encourage online social media users to share their location on online social networking. Therefore, the risk of user privacy infringement is increased to detect online social media users' location by others or attackers. In addition, online social media users share their location without knowing that by uploading images and videos, and this leads to know their geographical locations. In [31] embedded in the image was a geotag, a bit of data providing the longitude and latitude of where the photo was taken. Hence, he revealed exactly where he lived. A study in [32] found that (12.1%) of examined Twitters tweets (n=253) mentioned the location of a person. In addition, in [33] a classifying technique is used to identify user's location in real time, it found out that the location occurs much more frequently than person and time in sensitive tweets rather than non-sensitive tweets.

- Identity profile cloning is a technique in which attackers create a fake profile by using images, videos, and other private information stolen from a targeted user's real profile. The attackers may duplicate a user's profile that looks very much like the target's profile. Especially if most of the user profile set as public. Profile cloning can be done in two ways, in the cross-site and in the same site cloning. In the cross-site cloning, the user private information is stolen from the different online social networking site. But, in same site cloning, user private information is taken from the same online social networking site. Furthermore, profile cloning can be done automatically and manually. Automatically requires a written script code and to have the authorization to execute the script code in online social networking such as LinkedIn and Facebook [34]. In the manual method, the attacker copies all user's private information and create a new profile.

- Information privacy leakage means when sensitive and private information are detected to unauthorized users. In online social networking, users always share and exchange their information with friends and other users in social media. Information infiltration through online social networking categorized into four ways: infrastructure information such as technical decision, customer data such as health information, operational data such as acquisition, and intellectual property such as documents. A study in [35] demonstrated that (95.8%) of (n=166) from online social media participants shared some health-related information. Leakage of such sensitive and private information may lead to have a negative implication for online social networking users. For example, insurance companies my use online social networking data to distinguish risky clients from others [36]. The leakage of personal information can harm the reputation of your business. Therefore, the future clients will be concerned about having business with you or disclose private information to your company. There are a major reasons of information leakage such as phishing scams, using non-secure tools, stealing information, and send information to wrong users.

- Fake profiles attacks is a profile created by an attacker with fake credentials such as name, interests, social security number, and photographs and other information on a social network and sends messages to targeted users. The target of fake profile is to collect user's information. fake profiles affect the overall reputation of the network in addition to the loss of bandwidth [37]. For instance, an approach was generated in [38] to demonstrate the fake profile and able to send a total of 8,570 connection requests on Facebook. The technique recorded all data related to anticipated stealth and the corresponding users' behavior, along with all accessible users' profile information. Another example, in late 2017 and early 2018, Facebook revealed and suspended some (1.3) billion fake accounts. But an approximately (66) million to (88) million profiles, are also fake but haven't yet been detected. Likewise, estimates are that (9%) to (15%) of Twitter's (336) million accounts are fake [39].

- De-Anonymization attack is a data mining technique in which unidentified data is cross-referenced with other public sources to re-identify the anonymous data source in order to identify a person or group. Anonymization covers all the personally identifiable information of users dealing in different areas such as e-commerce trades, health services, social media, and others. Because of the data shared through online social networking are set to public by default, they are an easy goal for de-anonymization attacks [40] to re-identify a person from such data. For example, in [41] a Bumblebee which is a novel social de-anonymization attack is designed and evaluated and the results demonstrated re-identification rates with high precision, robustness against noise, and also has better error control. In [42] a novel structure-based de-anonymization attack is proposed which does not require the attacker to have prior information. The proposed attack technique is based on multi-hop neighborhood information and optimizing the process of de-anonymization by exploiting enhanced machine learning techniques. The results demonstrated significant advantages which are up to a 10× improvement in de-anonymization accuracy and outperforms the state-of-the-art de-anonymization attacks.

## IV. SECURING ONLINE SOCIAL NETWORKING SITES

In recent times, the spread of piracy on social networking sites are significantly raised with the increasing in the number of social networking sites and user. Table.1 shows (10) worst passwords from 2015 to 2018 [43,44,45,46]. According to SplashData[47] these passwords are mostly used in North America and Western Europe and after evaluating more than five million passwords leaked on the internet, the firm found that computer users continue using the same predictable and easy guessable passwords.

When studying the passwords shown in the below table, it is possible to deduce the similarity between the online social networking users in selecting passwords which lead to facilitate the task of piracy. Intruders usually use such these data with the emphasis on high success rate and penetration. Similarity of these passwords lead to the following facts:

- Users choose a simple password that it easy to save and retrieve.
- Users choose a simple password that it easy to save and retrieve.
- Users select only one password for all networking sites without re-change it and this facilitate the process of penetration.
- Users frequently use the password components associated with each other so that it can be easily retrieved.
- Dealing with social networking sites does not require the use of a complex passwords. Therefore, the users choose the simplest passwords. Furthermore, networking sites do not require continuous change of passwords.
- Users usually choose the password from private information that can be easily remembered. Therefore, it can be hacked by anyone familiar with the data.

Hackers download malicious programs or any other threats on social networking site, email, and others, which monitor and penetrate the users' information. In addition, the pirates communicate with the users and they propose to provide some special services such as to login to website and asking users to enter their password. So, users must avoid entering the password when dealing with any untrusted service applications or websites.

The most important threats to penetrate social networking sites are the method of preparing and using different passwords. Thus, a number of recommendations that positively affect these risks can be mentioned and summarized as follows:

- Do not use a simple passwords because it is easy to penetrate.
- Do not repeat the use of the password for different sites because penetrate one site can cause the penetration of all sites.
- Use a complex password that are not easily to penetrate.

- Use a password management programs such as ZOHO, Keeper, and Dashlane to store and manage passwords.

Table 1. Top 10 Most Common Passwords

| 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|
| 123456 | 123456 | 123456 | 123456 |
| password | password | password | password |
| 12345678 | 12345 | 12345678 | 123456789 |
| qwerty | 12345678 | qwerty | 12345678 |
| 12345 | football | 12345 | 12345 |
| 123456789 | qwerty | 123456789 | 111111 |
| football | 1234567890 | letmein | 1234567 |
| 1234 | 1234567 | 1234567 | sunshine |
| 1234567 | princess | football | qwerty |
| baseball | baseball | 1234 | iloveyou |

## V. RISK PREVENTION AND THREATS VULNERABILITIES

Risk is defined as a potential for damage, leakage, or destroy users' information or devices as a result of a threat exploiting a vulnerability. The vulnerability is a weakness in securing user information that can be exploited by one or more threats. Figure.6 shows the information security risks, threats, and vulnerabilities. For instance, in social networking system when users have a weak passwords or have not a secure system. In this case a user password is vulnerable by attacker or the secure system can be easily penetrated. Furthermore, the risk will be an illegal to access, modify, and damage by intruders.

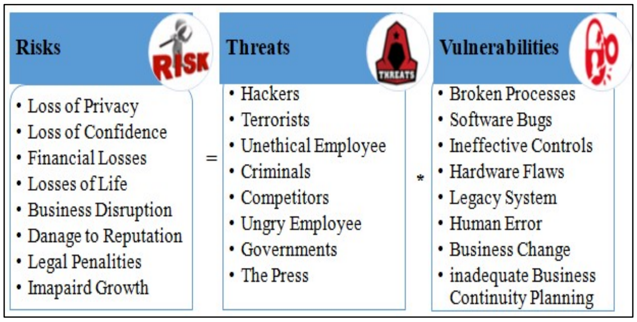


Figure 6. Risks, Threats, and Vulnerabilities

As the threats are spread on social networking sites around the world with different activities, and because of the great decline in the level of user information privacy. The following steps are necessary for anti-threats that faced users on social networking sites.

- Determine the level of privacy required from the site in light of the level of use and a degree of user's interaction on social media.
- Taking the advantages of all updates on the site, which are continuously developed to raise the level of data security.
- Carefully select and review users before you accept them or deal with them.
- The features used for the site should be stopped periodically and run again one after the other.
- Before updating the social networking sites and other software, read carefully all the new features.

The growth in using social networking site in the "Web 0.2"structure results in increasing of the risks of data security which hinders the progressing and technological growth in the desired direction. Figure 7. summarize the top threats worldwide in 2018 which declared by SOPHOS from Xperience Group[48].

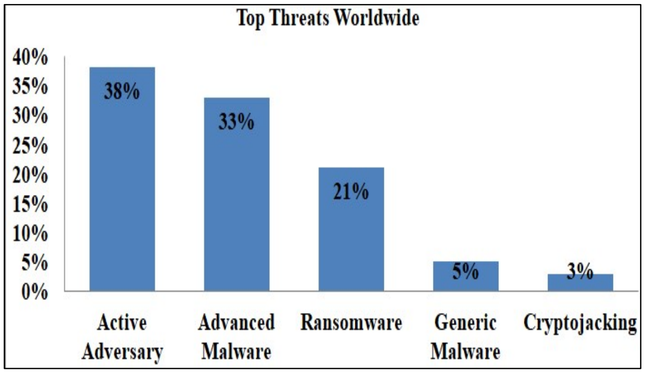


Figure 7. Top Threats Worldwide

Several studies have pointed out that there is a great importance to the impact of threats, especially at the level of institutions that deal with social networking sites and rely heavily on these sites to deal customer, suppliers, and employees in many vital activities relating to operating, economics as well as production. Figure.8 shows the most pressing cyber security issues according to IT security professionals worldwide in 2018[49].

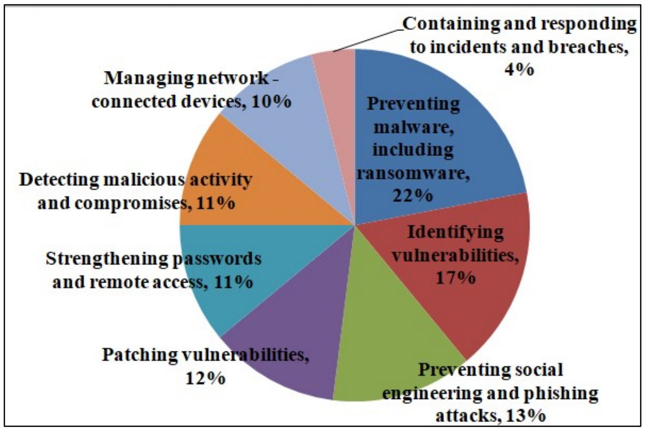


Figure 8. Most Pressing Cyber Security Issues

In line with the study from SOPHOS[48] to manage risk to data and IT assets, figure.9 demonstrates the amount of efforts needed to achieve the lowest risk mitigation to protect data.

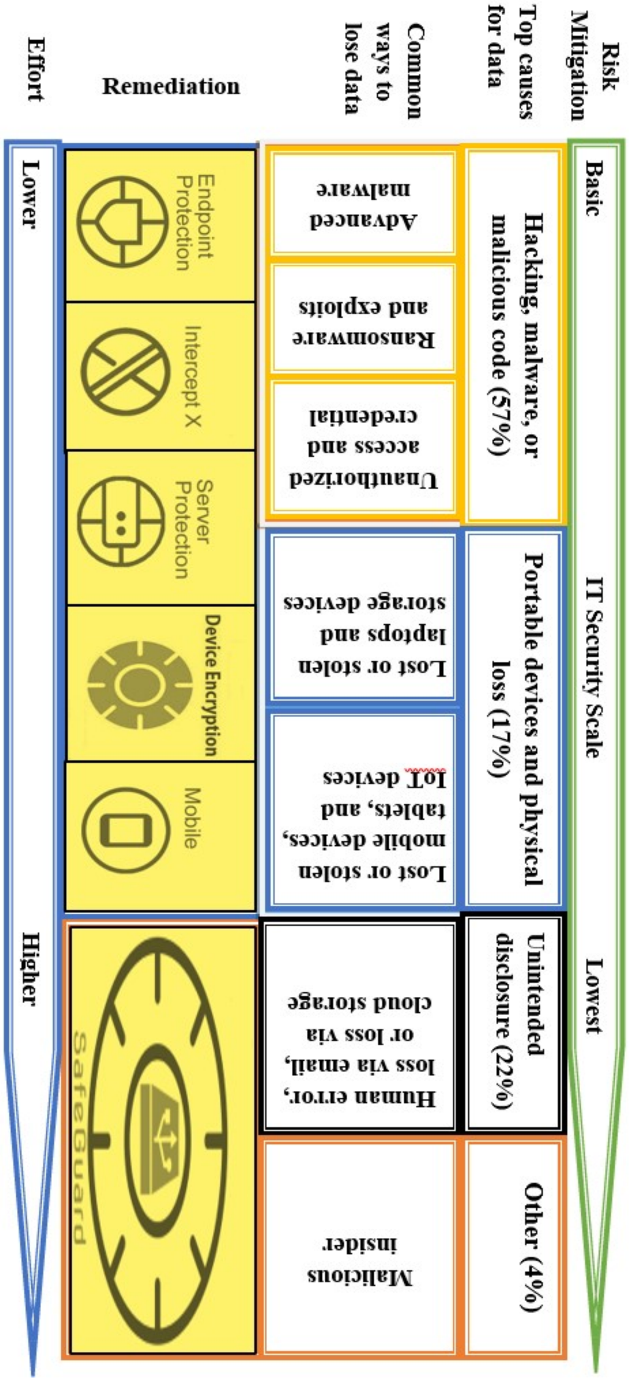

Risk Mitigation
Top causes for data
Common ways to lose data
Remediation
Effort
Basic
IT Security Scale
Lowest
Lower
Higher
Hacking, malware, or malicious code (57%)
Portable devices and physical loss (17%)
Unintended disclosure (22%)
Other (4%)
Advanced malware
Ransomware and exploits
Unauthorized access and credential
Lost or stolen laptops and storage devices
Lost or stolen mobile devices, tablets, and IoT devices
Human error, loss via email, or loss via cloud storage
Malicious insider
Endpoint Protection
Intercept X
Server Protection
Device Encryption
Mobile
SafeGuard

Figure 9. Data Protection

The above essential suggestions have a positive significant impact on online social media users in order to deal with the interactive innovations of the online networking applications and allow to maintain the security and confidentiality of data at the institutional level as well as at the individual level.

As part of the efforts to address these risks, a number of essential suggestions can be enabled on social networking system and that support the use of "Web0.2" technology, which works to secure data and overcome various threats.

- Companies must control the applications used on the Internet to limit malicious programs that do not use the standard protocols.
- Continuous review of the sites used, identification of periods of use and the development of different mechanisms to correct the negatives. The information collected and reviewed in actual use has a great value in identifying the risks and resolve any issues.
- Determine the used browsers and determine their techniques to secure the data by using advanced properties.
- Anti-threats software must be used to combat malicious programs, spyware, and other threats with a state of continuous updating to enable this software to cope with the rapid development of the threats.
- Use a sophisticated passwords that are difficult to penetrate and constantly updating these passwords in all online applications, so as to ensure the preservation of data and avoid piracy.
- Check piracy policies and know about unknown messages and links sends by unknown users.
- Use different mechanisms to protect the data and restore it in case it is tainted or lost as a result of hacking.

## VI. CONCLUSION

At the beginning of the Twenty-first century, the growth and development of internet and social media applications is significantly increased. Therefore, the interaction between users on social media by using different online applications is increased. With this growth, a number of threats have developed to penetrate user data protection and confidentially. This infiltration considered as the most issues when using online social networking. Data penetration could happen from unauthorized users, service providers and others that use online social networking data for their businesses. This paper explained various protection and privacy issues related with online social networking users and data from online threats such as hackers, service providers. Furthermore, it demonstrated the efforts need to address and manage risks in social media. The main target of this research is to shed the light of the threats issues on social media and to educate online social networking users to the way to protect themselves and their data from these threats when they using social media.

## VII. REFERENCES

[1] S. Hathi, “How Social Networking Increases Collaboration at IBM”, Strategic Communication Management, vol. 14, no. 1, (2009), pp. 32-35.

[2] www.securelist.com, «”Instant” threats», Denis Maslennikov, Boris Yampolskiy, 27.05.2008.

[3] Hak J. Kim " Online Social Media Networking and Assessing Its Security Risks:, International Journal of Security and Its Applications, Vol. 6, No. 3, July, 2012.

[4] www.statista.com/statistics.

[5] Davison, H.K.; Maraist, C.C.; Hamilton, R.; Bing, M.N. To Screen or Not to Screen? Using the Internet for

Selection Decisions. Empl. Responsib. Rights J. 2012, 24, 1–21.

[6] Baltazar, J.; Costoya, J.; Flores, R. “The Real Face of Koobface”: The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research, 2009.

[7] Alghamdi, B.; Watson, J.; Xu, Y. “Toward detecting malicious links in online social networks through user behavior”. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence Workshops, Omaha, NE, USA, 13-16 October 2016; pp.5-8.

[8] Muhammet Baykara and Zahit Ziya Gürel, “Detection of phishing attacks”, 2018 IEEE, 978-1-5386-3449-3/18.

[9] Protalinski, E. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials. Available online: https://www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials.

[10] A.Vishwanath,”Getting phished on social media”, “Decisios Support Systems”, ELSEVIER., Vol. 103, November 2017, Pages 70-81.

[11] Raman, P.: ,”JaSPIn: JavaScript based anomaly detection of cross-site scripting attacks.”, Ph.D. thesis, Carleton University, Ottawa (2008).

[12] Faghani, M.R.; Nguyen, U.T., “A study of XSS worm propagation and detection mechanisms in online social networks.”, IEEE Trans. Inf. Forensics Secur. 2013, 8, 1815–1826.

[13] S. T., Joshi, J., & Tipper, D. Zargar, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. ," IEEE communications surveys & tutorials, 2013.

[14] Anstee, D., Escobar, J., Chui, C.F., Sockrider,G.2015,Jan 27). 10th Annual Worldwide Infrastructure Security Report. Arbor Networks Inc.

[15] Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent DDoS attacks. International Journal on Computer Science and Engineering,3(2), 877-883.

[16] Zainab S. Alwan, Manal F. Younis, "Detection and Prevention of SQL Injection Attack: A Survey", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.8, August- 2017, pp. 5-17.

[17] Rua Mohamed Thiyah, Iyab Musab A. M. Ali, Farooq Basil Abdulqader," THE IMPACT OF SQL INJECTION ATTACKS ON THE SECURITY OF DATABASES", Proceedings of the 6th International Conference on Computing and Informatics, ICOCI 2017 25-27 April, 2017 Kuala Lumpur. Universiti Utara Malaysia .

[18] Vatu, G., (2017), Critical SQL Injection Vulnerability Found in NextGEN Gallery WorldPress Plugin http://news.softpedia.com/news/critical-sql-injection-vulnerability-found-in-nextgengallery-wordpress-plugin-513375.shtml.

[19] Amir, W., (2017), Gun retailer Airsoft GI’s Forum hacked; 65,000 user accounts leaked https://www.hackread.com/gun-retailer-airsoft-gi-forums-hacked/

[20] Fuchs, C.; Trottier, D., “Towards a theoretical model of social media surveillance in contemporary society”, Commun. Eur. J. Commun. Res. 2015, 40, 113–135.

[21] IAN BROWN,” Social Media Surveillance”, The International Encyclopedia of Digital Communication and Society, First Edition”, 2015 John Wiley & Sons, Inc. Published 2015 by John Wiley & Sons, Inc., DOI: 10.1002/9781118290743.wbiedcs122.

[22] S. Nowson and J. Oberlander, "The identity of bloggers: Openness and gender in personal weblogs In Proc. of AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs", pages 163–167, 2006.

[23] Ali, S.; Rauf, A.; Islam, N.; Farman, H.; Khan, S. User Profiling:, "A Privacy Issue in Online Public Network.", Sindh Univ. Res. J. (Sci. Seri.) 2017, 49, 125–128.

[24] N. Z. Gong and B. Liu,” Attribute Inference Attacks in Online Social Networks”, ACM Transactions on Privacy and Security, Vol. 21, No. 1, Article 3. Publication date: January 2018.

[25] Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. “Preventing private information inference attacks on social networks.”, IEEE Trans. Knowl. Data Eng. 2013, 25, 1849–1862.

[26] Viswanath, B.; Bashir, M.A.; Crovella, M.; Guha, S.; Gummadi, K.P.; Krishnamurthy, B.; Mislove, A., “Towards Detecting Anomalous User Behavior in Online Social Networks.”, In Proceedings of the USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 223–238.

[27] Sloane Burke Winkelman, Jody Oomen Early, Ashley D. Walker, Lawrence Chu , Alice Yick-Flanagan,” Exploring Cyber Harrassment among Women Who Use Social Media”, Universal Journal of Public Health 3(5): 194-201, 2015. DOI: 10.13189/ujph.2015.030504

[28] http://www.pewinternet.org/2017/07/11/online harassment-2017/

[29] Lundeen, R.; Ou, J.; Rhodes, T.," New Ways Im Going to Hack Your Web APP". Black Hat Abu Dhabi, 2011. Available Online: https://www.blackhat.com/html/bh-ad 11/bh-ad-11-archives.html#Lundeen.

[30] BCC Risk Advisory Ltd., 2016 Vulnerability Statistics Report Edgescan, 2016. Available Online: http://www.edgescan.com.

[31] K. MURPHY, "Web Photos That Reveal Secrets, Like Where You Live", The New York Times, AUG,11, 2010. https://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html.

[32] L. Humphreys, P. Gill, and B. Krishnamurthy,"How much is too much? Privacy issues on Twitters.", In Conference of International Communication, Pages 1-29. ACM Press, 2010.

[33] H. Mao, X. Shuai, A.Kapadia, "Loose Tweets: An Analysis of Privacy Leaks on Twitter", In proceeding of the 10th annual ACM workshop on privacy in the electronic scoiety, pages 1-12. ACM, October, 2011.

[34] Bolton, R.J. and Hand, D.J. 2002. Statistical Fraud Detection: A Review. Statistical Science. 17, 3 (2002), 235–249.

[35] Torabi, S.; Beznosov, K. Privacy Aspects of Health Related Information Sharing in Online Social Networks. In Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, Washington, DC, USA, 12 August 2013; p. 3.

[36] Scism, L.; Maremont, M. Insurers Test Data Profiles to Identify Risky Clients. The Wall Street Journal, 19 November 2010.

[37] Wani, M.A.; Jabin, S.; Ahmad, N. A sneak into the Devil’s Colony-Fake Profiles in Online Social Networks. Available online:https://arxiv.org/abs/1803.08810. 2018.

[38] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu," The Socialbot Network: When Bots Socialize for Fame and Money",In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), December 2011.

[39] https://phys.org/news/2018-09-people-fall-fake-profiles-online.html.

[40] Ding, X.; Zhang, L.; Wan, Z.; Gu, M.,” A brief survey on de-anonymization attacks in online social networks”. In

Proceedings of the IEEE International Conference on Computational Aspects of Social Networks (CASoN 2010), Taiyuan, China, 26–28 September 2010; pp. 611–615.

[41] Gulyás, G.G.; Simon, B.; Imre, S. An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, 24 October 2016; pp. 1–11.

[42] Wei-Han Lee, Changchang Liu, Shouling Ji, “Blind De-anonymization Attacks using Social Networks”, Proceedings of the 2017 on Workshop on privacy in the Electronic Society. Dallas, Texas, USA, October 2017.

[43] Chang, Lulu, "Wookie mistake: 'starwars' is now one of the world's 25 worst passwords". January 19, 2016. Digital Trends.

[44] Bruner, Raisa,"The 25 Worst Passwords You Should Never Use". January 23, 2017. TIME.

[45] Korosec, Kirsten,"The 25 Most Common Passwords of 2017 Include 'Star Wars'". FORTUNE. December 19, 2017

[46] Ehrenkranz, Melanie, "The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius". Gizmodo. December 13, 2018.

[47] https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/.

[48] https://www.xperience-group.com/wp-content/uploads/2018/10/Cybersecurity-Presentation-October-2018.pdf.

[49] https://www.statista.com/statistics/709789/most-pressing-global-cyber-security-issues/.