Social Media Security Risks and Cyber Threats

Saima Shoro, Mir Saqlain Hyder and Syed Naqi Haider Kazmi
Department of Computer Science,
Shah Abdul Latif University, Khairpur, Sindh, Pakistan
shorosaima@gmail.com, Saqlainhyder55@gmail.com, Naqihaider133@gmail.com

ABSTRACT
Social media is being utilized to demonstrate communication skills. Social media provides a way to connect with our loved ones any time anywhere. There are several social networks like Facebook, twitter, LinkedIn and so on are presented over the internet. These social networking sites make an online profile of a user which is shared freely with the public. It can have negative impact on our life. It can allow easy access to one’s privacy. In this paper, we have discussed privacy and network related issues and threats and proposes anti threats steps and preventive measures for users. Although these sites may work harmless but they always have malicious content. The undertaken study is helpful for researchers, scholars and academicians.

KEYWORDS: Social Media, Privacy, Cyber Threats, Social Networking, Security Risks.

I INTRODUCTION

Social media are digital platforms of connecting people and making globalization more mark able. One can easily share their views, and keep linked and discuss even about their lives on regular basis. They have transformed lifestyles, creating roadways for people to flourish communication. Social media keep people updated to new trends, promoting culture and help in building relationship. Moreover, collaboration is created in terms of marketing and how to boost up productivity. First email was sent in 1971, bulletin board system in 1987 exchanged data over phone lines. In 1994 first social website was founded. In 1995 the globe.com was launched and people were given opportunity of interacting with others. American online instant messenger was launched in 1997. Friendster was introduced in 2002 and with time it got 3 million users. In 2003 myspace, in 2004 Facebook and twitter in 2006. [1] [2] [3]

We see in 2018 it has gone to 2.44 billion. The fact number of users is increasing throughout but they're not fully aware of the risks and threats these sites carry [4]. Social networks disconnect you with the whole physical world around you. Entertainment is more as one would never thing of leaving this online world and become an isolated person. We carelessly and casually share our personal details, in today’s world Facebook has more users than the combined population of many countries. The more we share data, the more we invite malicious people to exploit our privacy. Research has a high value in knowing the security threats these social networking sites offer. Social networking sites have both positive and negative impacts. Most of it goes to wastage of time, stopping up physical activities and affecting healthy routine. Natural world is merely a dream these days, fundamentals of social structure are deteriorating. People sitting together prefer to interact via this technical avenue rather than sharing a good talk verbally.

*Corresponding Author: shorosaima@gmail.com
A-SOCIAL NETWORKING SITES

a) FACEBOOK: A communication site which is the most leading one nowadays, it has listed users who creates their profiles, shares updates, photos, videos, meet people around the globe, convey instant massages, and be in contact with fellows, family, neighbors etc. It not only a site for communication but on commercial level it makes user aware of arranged promotions. It can set up and event where people can easily reach out to one another, having common interest, in term of business, hobbies, literature, art and so on. People create their pages and they work on a specific ground. They also promote their origination, create up an event i.e launching, provide details regarding that as their companies easily get along.

There is so much creative on this social site, for example, birthday’s posts, features in messenger, video calling, groups. But the thing we usually share are that secure, they’re more open to public, which poses risk too.

b) TWITTER: An online news and long range informal webpage for common actions, where people impart in short massages called tweets. Tweeting is sending short massages to any individual who tails you on twitter those messages can be important, fascination to your group of onlookers. Another portrayal of twitter and tweeting may be microblogging. Here we do two things we mention specific user in our tweets while Hastings allow us to be part of group discusser. Individual tweet for find out and old friend, or if they are few of any celebrity, talk about political issues, twitter also turn out be a powerfully platform for sharing insights, not only we have informative content but pure online entertainment too.

c) LINKEDIN: LinkedIn is a kind of formal platforms of communication. It allows enrolled user to create their professional portfolios, and get in touch with pages to, different aptitude, business, proficient system news, schedules, courses, academics info. Here participation is free individual are named as associations and members can invite others to be part of it connection.

d) INSTAGRAM: This colorful social networking site if full of photographs and videos, short clips, animated stuff that individuals share from their cell phones. It also has featured profiles has followers, and following check. Which defines number of people they go stalking and users who tail them too. Individuals try to make their profiles visually pleasing as to get more followers, they keep colorful themes, captioning their photos, videos, in different styles, and much more others things.

e) MySpace: MySpace is a classic social network where people can exchange messages and ideas. it offers, interaction between friends, groups music’s, and has great impact on music culture. Musicians can how off their talent, have more fans.

B-PRIVACY RELATED THREATS

We come across settings on these social websites as maintaining privacy, but here is a big question mark? Is our information really protected? It’s so far behavioral than technical. We create personal home pages, sharing out data as phone numbers, address, date of births, current locations etc. which can be easily be accessed by hacker or say some malicious worker, terrorist organizations or they can be our personal enemies too. They take the advantage of breaking the integrity of data. [5]

a) Profiling risks: This is the easiest way by which hackers create clone of user’s profile. Hacker acquire personal information, they portrait, the bad social image of a person, by being familiar with victim’s friends. Social networking sites offer no security for profile cloning. Another term is cross-site profile cloning. In which hacker get information from one social site and create users profile on another social site.

b) Identity Theft: A portion of the hacker’s attack through the application in which they approach authorization for getting to the data gave in the profile of SNS. We see some applications asks for permission accessing the information we give in our profile on these social networking sites. We allow these applications to access contact, gallery, email etc. by this attacker get the chance to get entry without permission and used the information for their malicious purposes.
c) **Fake Product Sales:** We come across different advertisements on social networking sites where hacker’s sale items attracting users by low discounts rates. When we click on these links our information is stolen and when users go for purchasing they submit their account, numbers, address thus attackers retrieve this information and get benefit.

### C- NETWORK RELATED THREATS

As the number of user’s increase and so the attackers get more chance to go after them. Cybercriminals use various methods as an instrument for creating violence. So, the picture changes from entertaining to fearful darkness. [6]

a) **Phishing:** In 2007 phishing in sns begins. It duplicates the original profile and get control over one’s login form. Phishers and spammers send deceptive messages to victim’s contact to gain unauthorized accessed.

b) **Keylogger:** Keylogger is a software that records keystrokes and monitor the action of the victim. Keylogger is often found to be in public WIFI’s, cafes, offices etc. this software steal passwords and other confidential data

c) **Click jacking:** Click jacking is the type of method in which attacker share photos, videos and links and victim when click on these, some vicious actions are processed.

d) **CBIR(Content based Image Retrieval):**
The hacker can know the area of a victim by coordinating the examples of the pictures related with the profile of the victim. These types of attacks are done to know the present area of the victim. [2]

e) **Neighbourhood Attack:** The area assaults are finished by the hacker’s by knowing the casualty’s neighbourhood. It implies the assailant knows the companions of the casualty. Assailant utilizes the relationship among these companions and in view of this relationship tries to recognize the casualty. [2]

f) **Application’s vulnerability:** Most informal organizations enable application to have wide range of access to user’s information through various interfaces. Some give achieved APIs That enables particular access to data likewise some access is given on consent premise with the that user can decide which access to give to application then it can interfere on free level showing some halfway data on an alternating site. [6]

g) **Follower Scams:** with advancement of informalities that has allowed individuals on these social networking sites to have much online companions and making yourself more prevalent. Some websites offer free services where you have to submit your account name and password and they will insure you that you will have more followers every new day. Since you cannot control what will be done to your account, in most cases it is also against the term and conditions of social networks. These services simply take the account and start using it to send unrelated spam massages to all the connected friends which is surely not the user wanted. [6]

### II METHODOLOGY

We used online research methods (ORMS) to collect data via internet. Existing researches are re-imagined, and reviewed. Online articles are well studied and information is revised [7] [8] [9] [6] [3] and we got to learn, there is still a lot more to come on this social media security risks. Newer technologies will hold new methodologies to understand its consequences. We dealt with several research papers that had common vision but quite different in areas of focus and design. We went through videos, tutorials, statistical platforms, published pieces and we came up with similarities and differences.

### III FINDINGS

We found that that most of the attacks are carried out due to casual behavior of users, being unaware of these risks. The most used site is Facebook, which is prone to attack. On Facebook an individual updates status, share locations, give access to different applications as games, quizzes, join groups, and keep other about their personal activities. Although the application may look harmless but they always have malicious contents.
Figure-2 Percentage of Threats in Social Networks

In figure 2 Facebook hold highest risk percentage 61% and the less is in LinkedIn, so potentially thousands of users of Facebook are unsafe.

Figure 3 Impact of Social media on teenagers

Figure 3 demonstrate young adults between 18-29 ages are more at risk of harm. 28% of them loses their passwords and emails. Because the more they share, the more they lose privacy, they don’t even miss out a second being offline. 23% are being harassed in terms of photos, videos, young girls are being blackmailed for unethical purposes. If we throw light on business related threats. People between ages 30-49, loses their important data, bank codes, credit cards info. 13% of middle aged had reputation issues as actors, famous personalities face fake information issues. Dreadfully 11% of young 4% of middle age have life threats. One can easily access your where about, and so the criminal, murderer, terrorist can cause potential damage. [10] Through these websites fake news are also certify which is illegal act. [11] [12] [13]

IV ANTI THREATS STRETIGIES

- Awareness program, educational trainings, seminars, symposium raise this sensitive topic, and should address making people know more about these dangers of leaking privacy.
- Government should have check and balance to strongly monitor the unauthorized events, activities to protect overall country, limiting access, blocking unethical sites, and allowing entertainment and information within certain boundaries.
- Creating more advanced security features for users as they can manage their accounts.
- Verification must be exceptionally solid with the goal that cybercrimes done by programmers, spammers, could be decreased however much as could reasonably be expected.
- Utilization the most intense antivirus tools, with general updates and should keep the proper default setting so that antivirus software’s could work in effective way. [5]

V RISKS PREVENTION STEPS

- Share limited information.
- Use strong password (numeric, symbols etc.)
- Don’t click on unknown content, unknown websites.
- Don’t go off your circle if not important
- Don’t use public WIFI, other computers.
- Password should be changed on regular basis to limit the hackers.
- Don’t install unnecessary apps.
VI CONCLUSION

Technological advancement eased out lives, but we cannot ignore the danger zones, incidents and accidents have equal importance. Highlighting how to be protected and the challenges regarding security risk. In this piece of work, we defined positive and negative impacts of social media. Diagrammatically showed users, discussed about privacy and network related threats, preventive measures, anti-threat steps and government policies to benefit the public as a whole, we believe to study more, and work on to make social networking sites, more improved in terms of security.

REFERENCES


