# Privacy and Security Issues in Social Online Networks

**Radhika Bhagat[1] Rajvi Modi[2] Palaumi Patel[3] Mr. Harshil Joshi[4]**
[1,2,3]UG Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SAL Institute of Technology & Engineering Research, Ahmedabad

*Abstract*— Trend of social networking is burgeoning at tremendous rate. This constant use of internet poses potential dangers to all those people using it. Internet security includes taking measures against malicious attacks over internet and internet privacy includes exposure of private information to third party. Naïve users, especially teenagers reveal their private information comprehending of their location, current status, reputationally damaging photos, etc to the whole world. By keeping security and privacy settings open to public, they create insecure channel through which private information is exchanged which leads to a high risk of intrusion. Often users fall victim of a hyperlink or advertisement, which have catchy or provocative headline that entices a user to click to continue reading an article, which leads to infection of malware to their devices. Our study of survey paper includes all these unfavourable circumstances that befall to the community of social online network users and how they can manage to save themselves from this kind of cyber-crime. Some suggestions or remedies will also be given to the users in this survey paper to prevent themselves from malicious software.

***Key words:*** Social Network, Internet, Security, Privacy, Information, Cyber-Crime

## I. INTRODUCTION

According to the quote seen on Facebook's site – "Connect with friends and the world around you on Facebook", the naïve community of the internet users often forget to whom they should connect and how much information they should share. A Social Networking Site (SNS) is an online platform that is used by people to build social networks or relations with other people who share similar interest, activities, background or connections. This survey paper explains us how the users fall victim to the issues of security and privacy of social media and gives information about whether there are any ways to prevent themselves from exposing.

There will be some surveys, graphs and other information given about all the types of data of a person which are at a high risk of intrusion by cyber-criminals and hackers leading to cyber-attacks or identity thefts. Finally, the survey paper will be concluded by some useful suggestions or ideas which can be beneficial and serviceable to the populace on internet.

## II. USERS OF SOCIAL ONLINE NETWORKS

The above graph shows number of people using all kinds of social networking sites to interact with each other. People now get all kinds of information consisting of news, gossips, latest updates from technology to movie stars on social media. Now a days any big or small news travel through the whole world via internet in a blink of an eye. People share all kinds of personal information and images on this very same media. This is an age where people live their social lives online. For example, Facebook[1] revealed in white paper that its users have uploaded more than 250 billion photos, and are uploading 350 million new photos each day. SNS[25] are currently being used regularly by millions of people. People[25] use Social Networking Sites for countless activities. Among the most common uses are, connecting with existing networks, making and developing friendships/contacts, create an online presence for their users, viewing content/finding information, creating and customizing profiles and so on.

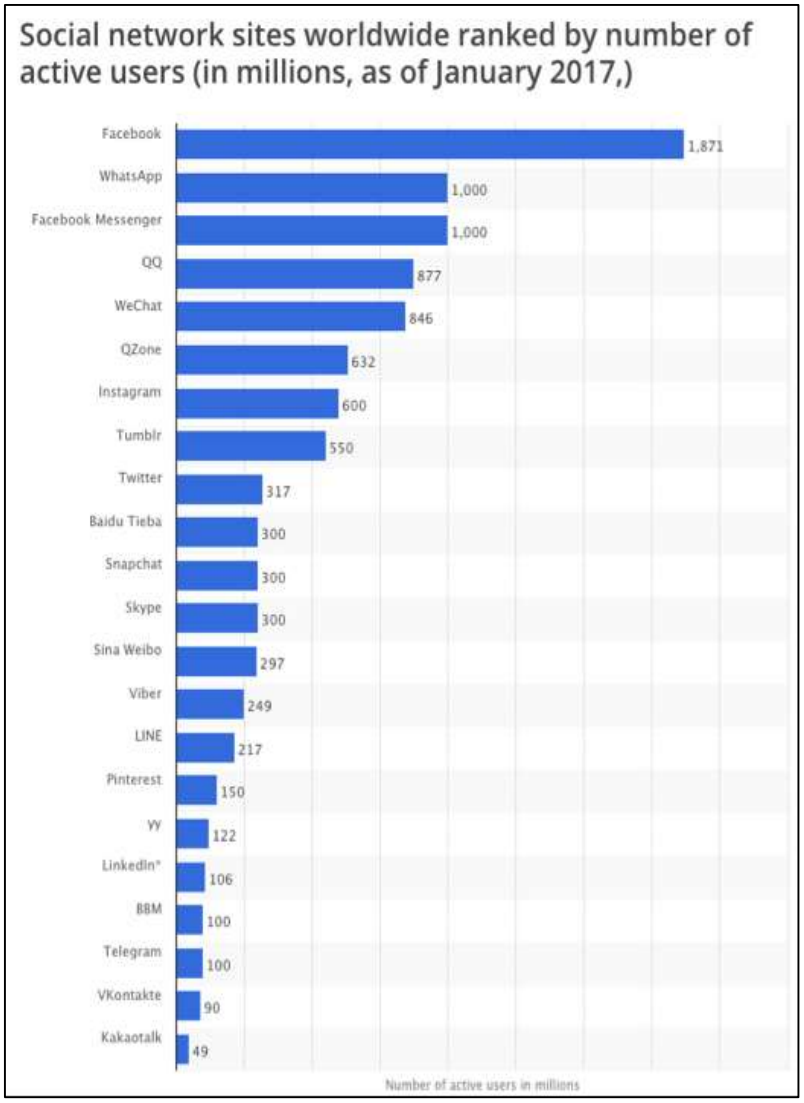


Fig. 1: Number[2] of active users

## III. SECURITY ISSUES IN ONLINE SOCIAL NETWORKS

While using social media, people often tend to forget the security issues that comes with the increasing usage of using such sites. While revealing personal information to accepting an unknown friend request, everything is associated with breaches of security. Various security issues that has happened or are happening which are related to social media are described below:

### *A. Identity Theft[3][4]*

Identity Theft is an act of stealing someone's identity or sensitive information, and then pretending to be that person, or using that identity in a malicious way. Identity[5] theft includes the misuse of another individual's personal information to commit fraud. Social networks are promising targets that attract attackers since they contain a huge number of available user's information. One[6] technique of identity theft is profile cloning. In this technique, attackers take advantage of trust among friends, and that people are not careful when they accept friend requests.

*1) Suggestion*

Users should always check the profile thoroughly before accepting to any unknown friend request and if they find the profile confusing or doubtful, they should report the profile for their own safety.

### *B. Phishing[3][7][9]*

In phishing, attackers create a mock login page which when filled by the user, gives the information like password to the attacker. Using this information the attacker gains access to the user's profile and other personal information.

*1) Suggestion*

Users should only login with their id and password from trustworthy devices. Users should not login to any unknown websites.

### *C. Bruteforce Attack[8][10]*

The hacker repeatedly attempts to guess a user's password.

This technique is very effective against user's password that are short or easy-to-guess like "123456" or "password". Brute[9] force attack attempts on a huge number of key combinations on trial-and-error basis.

*1) Suggestion*

Users should keep their password lengthy and should use as many characters as they can. They should add special characters and numbers and their passwords should not be predictable. For eg: Pet's name.

### *D. Sybil Attack[11][12]*

Here, an individual entity masquerades as multiple simultaneous identities. A concrete example is that by controlling many identities, the adversary can promote the popularity and reputation of an account in e-commerce setting by voting the target account as "good".

*1) Suggestion*

It is not only user's responsibility to check if they are using a trustworthy website or not. There should be a committee which regulate all the websites and if they give a trustworthy mark on the website then only the user should register or login themselves otherwise the user should think twice before entering their personal information.

### *E. Trojan Attack[13][14]*

A part of Malware attack called Trojan attack is such where the attack lures user into infection by promising racy content through a link available on social media. Once the user click on the link, victims are able to view a preview of content present on link. But the users are intruded half way and are asked to download an application or a software which is likely to contain some malicious content which infects victim and allow hackers to control keyboard or mouse activities. It also give rights to the hackers to post links to the users' accounts and tagging other friends hence infecting other users too.

*1) Suggestion*

Third party applications should not be installed in user's devices. Users can download applications from trusted vendors like Google.

## IV. PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS

Whenever a user create a profile on social networking sites, often the user ignore the privacy settings given in the settings of the social media. Social networks hold a plethora of personal information on the users that form the network. All the images uploaded, any personal information like birthdate, current address, telephone number, interests, hobbies, status, location etc. should be seen to only those people the user trust. It is also seen that some people have posted their credit card numbers on social media. Not all those people on the social media are authentic and thus every detail should not be revealed to everybody by keeping it open. The information should be changed to "seen by added friends only". Some privacy threats are explained below:

### *A. Cyber Stalking[8][22]*

Popular social networking sites makes it easy for users to build a web of friends and acquaintances, and share photos, whereabouts, contact information, and interests. With the amount of information that users post about themselves online, it is easy for users to become a victim of stalking without even being aware of it. 63% of Facebook profiles are visible to the public, meaning if you Google someone's name and you add "+Facebook" in the search bar you pretty much will see most of the persons profile. Cyber-stalking[21] victims are less likely to know the identity of their harassers.

*1) Suggestion*

Every user should keep their profile hidden from unknown users. The information should only be seen by trusted users.

### *B. Cyber Bullying[8][23]*

Cyber bullying includes mean messages or rumours, embarrassing pictures or videos posted on posted on social networking sites. All these images or text are posted anonymously and distributed quickly to a very wide audience. Deleting those messages or pictures becomes very difficult after they have be posted everywhere. Cyber-bullying[24] is different from traditional bullying due to the anonymity that the Internet can provide. According[24] to Willard (2006), there are nine main forms of cyberbullying: flaming, harassment, denigration, impersonation, outing, trickery, exclusion, cyberstalking and cyber-treats.

*1) Suggestion*

It becomes extremely important to hide your pictures from third party users. A user should be alert whenever he or she gets mean or embarrassing messages and the user should quickly report the unknown profile.

### *C. Profile Cloning[6][20]*

Profile cloning especially facebook profile cloning is a type of identity theft where unknown users literally make a second profile that looks exactly like the current one. Then they send friend request to all of the user's friends from that cloned profile fooling everyone. The fraud user then are able to communicate with all of the user's friends using user's identity. So[19] the friends might face difficulty in differentiating between genuine and fake identity.

*1) Suggestion*

To prevent oneself from being cloned, the user should not accept unknown friend request as well as change their cover photos/ profile photos on a regular basis. If the user has been cloned, the best solution is to delete the user's profile completely from the social networking sites and the user should communicate with their friends about it.

## V. CONCLUSION

Agglomerating, all the points elaborated above, it can be concluded that even though social media has contributed a lot in ample ways, like every coin, social networking sites also have a negative side. A[16] security environment is to be achieved by improving the stronger security and increasing privacy. All the issues mentioned above does not obfuscate the fact that social media has some advantages too. It helps the users grow themselves into a social world by meeting and befriending those people who share the same interests, work or community as the user does. But it is advisory that the users should be alert while using social online networks.

## REFERENCES

[1] "Facebook users are uploading 350 million new photos each day", Cooper Smith, 18 sept 2013
[2] "Global social media research summary 2017",Dave Chaffey,27 feb 2017
[3] "A survey of privacy and security issues in social networks", Dolvara Gunatilaka
[4] "Privacy and National Security Issues in Social Networks: The Challenges", Shafi'i M. Abdulhamid , Sulaiman Ahmad , Victor O. Waziri and Fatima N. Jibril
[5] Allison, S., Schuck, A., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/ offender characteristics. Journal of Criminal Justice, 33, 19–29
[6] Devmane, M. A., and N. K. Rana. "Detection and prevention of profile cloning in online social networks." Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014.
[7] "Friend-in-the-middle Attacks: Exploiting Social Networking Sites for Spam", Markus Huber, Martin Mulazzani, Gerhard Kitzler, Sigrun Goluch, Edgar Weippl
[8] Malagi, Kiran, Akshata Angadi, and Karuna Gull. "A Survey on Security Issues and Concerns to Social Networks." International Journal of Science and Research (IJSR), India Online ISSN (2013): 2319-7064.
[9] Jesudoss, A., and N. Subramaniam. "A Survey on Authentication Attacks and Countermeasures in a Distributed Environment." Indian Journal of Computer Science and Engineering (IJCSE) 5.2 (2014): 71-77.
[10] Carlisle Adams, Guy-Vincent Jourdan, Jean-Pierre Levac and François Prevost, "Lightweight protection against brute force login attacks on web applications ", in Proc. PST '10, 2010, p. 181-188
[11] Kushwaha, Deepak, Piyush Kumar Shukla, and Raju Baraskar. "A Survey on Sybil Attack in Vehicular Ad-hoc Network." International Journal of Computer Applications 98.15 (2014).
[12] Khan, Faizan. "A Survey Paper on Detection of Sybil Attack in MANET." identities 6.1 (2016).
[13] Bhunia, Swarup, et al. "Hardware Trojan attacks: threat analysis and countermeasures." Proceedings of the IEEE 102.8 (2014): 1229-1247.
[14] "Common Malware Types: Cybersecurity 101", Nate Lord, 12 oct 2012
[15] Novak, Ed, and Qun Li. "A survey of security and privacy in online social networks." College of William and Mary Computer Science Technical Report (2012).
[16] Rajam, S. Thiraviya Regina, and S. Briito Ramesh Kumar. "Security and Privacy issues in Social Network Services: An Overview." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 2014, IJIREEICE 2 (2014).
[17] Balduzzi, Marco, et al. "Abusing social networks for automated user profiling." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2010.
[18] "online social networks malware launch pads", 1 nov 2011
[19] Dave, Deepti, Nishchol Mishra, and Sanjeev Sharma. "Detection Techniques of Clone Attack on Online Social Networks: Survey and Analysis."
[20] Kontaxis, G., Polakis, I., Ioannidis, S. and Markatos, E.P., 2011, March. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on (pp. 295-300). IEEE.
[21] Bocij, Paul. "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet." First Monday 8.10 (2003).
[22] "Prevention of Cyberstalking: A Review of the Literature", Winter 2012 Criminology and Criminal Justice Senior Capstone Class: Michael Abshier, Kerry Allen, Kelly Anderson
[23] "A survey on Datamining in Cyber Bullying", K. Nalini, Dr. L. Jaba Sheela, july 2014
[24] Aune, Nicole M. Cyberbullying Graduate Degree/Major: MS School Psychology Research Adviser: Dr. Amy Schlieve MonthlY ear: December 2009. Diss. University of Wisconsin-Stout, 2009.
[25] "The Usage of Social Networking sites Among the College Students in India", Manjunatha S., 8th May 2013
[26] Gangopadhyay, Saswati, and Ms Debarati Dhar. "Social networking sites and privacy issues concerning youths." Article-2 Global Media Journal-Indian Edition, Summer Issue 5.1 (2014).

[27] "Social Networking Sites and Their Security Issues", Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha, 4, April 2013
[28] Beach, Aaron, Mike Gartrell, and Richard Han. "Solutions to security and privacy issues in mobile social networking." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 4. IEEE, 2009.
[29] "CYBER THREATS IN SOCIAL NETWORKING WEBSITES", Wajeb Gharibi , Maha Shaabi, 1, January 2012
[30] Beach, Aaron, Mike Gartrell, and Richard Han. "Solutions to security and privacy issues in mobile social networking." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 4. IEEE, 2009.
[31] Gao, Hongyu, Jun Hu, Tuo Huang, Jingnan Wang, and Yan Chen. "Security issues in online social networks." IEEE Internet Computing 15, no. 4 (2011): 56-63.
[32] Zhang, Chi, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. "Privacy and security for online social networks: challenges and opportunities." IEEE Network 24, no. 4 (2010).
[33] Rosenblum, David. "What anyone can know: The privacy risks of social networking sites." IEEE Security & Privacy 5.3 (2007).
[34] Ho, Ai, Abdou Maiga, and Esma Aïmeur. "Privacy protection issues in social networking sites." In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on, pp. 271-278. IEEE, 2009.
[35] Bertot, John Carlo, Paul T. Jaeger, and Derek Hansen. "The impact of polices on government social media usage: Issues, challenges, and recommendations." Government information quarterly 29, no. 1 (2012): 30-40.
[36] Albesher, A. and Alhussain, T., 2013, July. Privacy and security issues in social networks: an evaluation of Facebook. In Proceedings of the 2013 International Conference on Information Systems and Design of Communication (pp. 7-10). ACM.
[37] Leitch, Shona, and Matthew Warren. "Security issues challenging Facebook." In Australian Information Security Management Conference, p. 16. 2009.
[38] Al Hasib, A., 2009. Threats of online social networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), pp.288-93.
[39] Bonneau, Joseph, Jonathan Anderson, and George Danezis. "Prying data out of a social network." In Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in, pp. 249-254. IEEE, 2009.
[40] Verma, Akriti, Deepak Kshirsagar, and Sana Khan. "Privacy and security: Online social networking." International Journal of Advanced Computer Research 3, no. 8 (2013): 310-315.
[41] Abdulhamid, Shafii M., Sulaiman Ahmad, Victor O. Waziri, and Fatima N. Jibril. "Privacy and national security issues in social networks: The challenges." arXiv preprint arXiv:1402.3301 (2014).