International Journal of Humanities and Education Research
www.humanitiesjournal.net
Online ISSN: 2664-9802; Print ISSN: 2664-9799
Received: 04-03-2019; Accepted: 05-04-2019; Published: 12-04-2019
Volume 1; Issue 1; 2019; Page No. 36-38

Social media and security: how to ensure safe social networking

Ishfaq Majid[1], Shazia Kouser[2]
[1-2] School of Education, Central University of Gujarat, Gandhinagar, Gujarat, India

Abstract
The 21st century is the world of technology where most people do not even imagine their life without technology. Social networking sites refer to various applications, websites or new online media that allows large numbers of individuals to share their information and develop a proper social and specialized contact. These sites emphasize the creation of a connection between people to enable them to share their interests. However, sharing of information and creating connections with unknown persons has sometimes a key concern of security which get arised with our action on Social Media. The paper analyses the growing security concerns in Social Media and lay down some measures which will help users to enjoy and ensure smooth and safe social networking.

Keywords: social media, security, virtual private network, two factor verification, security breach

1. Introduction

Social media is a web based technology which enables the sharing of information with the help of building virtual networks and communities. By design, social media is internet-based and generates quick communication of content electronically. The content includes personal information, videos, and photos. The users engage with social media often via personal computers or smartphone or they can be easily accessed by software or web application.

Social networking sites (SNS) are online services that emphasize the creation of a connection between people to enable them to share their interests. These network sites allow people to share their information in a particular group. Therefore, the main purpose of the social networking sites is to allow people to share their real-life interests, activities and experiences. Social networks refer mainly to the means used for interaction, which have become phenomena of growth in the social and academic field. Social media allows people and organizations to create, participate and share new or existing content through multi-way communication. Commonly, the phrase "social network sites" is used as a general term for all social networks, including Facebook, Twitter and Myspace. Over the past decade, every social networking application has worked collaboratively to provide a completely new multimedia experience that can now be accessed via mobile devices.

Social media in the first instance was originated majorly for interaction between a group of users. But later due to its popularity, it was also adopted by various organisations for the purpose of making business and making their organisation much popular in the world. These kind of websites helped the business organisations to come close with its customers. Vitak (2008) [7] reported in a study that there are several reasons why people use a social networking site. One of the reasons is that they meet strangers and become friends. Through social networking sites, users can keep their interpersonal relationship with their friends and users can send private messages, can use chat rooms and other methods of communication. Nowadays, online social networks involve people from the entire world, of any age and with any kind of education. They also helped to increase computer usage among categories that previously showed little interest for it (Stroud, 2008) [6].

This compilation of the most popular social networks worldwide by active users (October, 2018) prepared by Statista gives a clear picture of the number of active users (in millions) with Facebook ruling supreme. With over 2 billion active users Facebook holds the majority market share. Google's YouTube is second with Facebook-owned, Whats App and Messenger not far behind. Facebook's Instagram platform has fewer than half of the visits of Facebook. Following from this, we have predominantly APAC favoured platforms, with QQ, We Chat and Qzone all with over 600 million active users. As thousands of new social media users log on every week, the numbers relating to the flow of information on Facebook become ever more staggering. In one minute of Facebook, 243,055 photos are uploaded by users, 100,000 friends are requested, 13,888 apps are installed, 3,298,611 items are shared, 50,000 links are posted and 15,277,777 like and share buttons are viewed on other websites (Ahmad, 2014) [1].

Most social network users share a large amount of their private information in their social network space. This information ranges from demographic information, contact information, comments, images, videos, etc. Bicen and Cavus (2010) [2] reported in their study that the use and exchange of knowledge on the internet is an integral or internal part of the life of university students. The findings of the study also show that Live Spaces and Facebook are the sites commonly used by students. Many users publish their information publicly without careful consideration. Hence, social networks have become a large pool of sensitive data. Moreover, social network users tend to have a high level of trust toward other social network users. They tend to accept friend requests easily, and trust items that friends send to them (Gunatilaka, 2011) [3].

India emerged as third most vulnerable country in terms of risk of cyber threats, such as malware, spam and ransomware in 2017. The report was published by security solutions provider Symantec (Internet Security Threat Report, 2018).

2. How Social Media security issue arises

Social media is possibly the most vital sector of the internet but being open and social creates legitimate concerns about privacy and safety. Headlines warning of online security breaches are just one reminder of the vulnerability of all websites, including social media outlets. Despite these justifiable security concerns about the Web, some of the reasons a person's social media account is compromised are self-induced.

1. Forgetting to log out: While using social media websites in a cybercafé or in friend’s mobile/laptop, many users forget to logout their accounts. So when the other person starts using that mobile/laptop, he gets access to the account information. This means the person is in command of your account and use it for any purpose. The person who gets access to your computer can access your account, change the password or even post items and communicate with your friends as if they are from your side.
2. Logging in on fake website: We usually search for a social media website using Google search engine. Each and every social media website has its official website or mobile app. Without using that official website address, we usually take help of a search engine. These search engines most of the times take us to the official website but some time we are redirected to any fake website. We assume this as the official website but when we insert our user credentials, we are redirected to some other website.
3. Lack of Privacy: Each and every social media website is inbuilt with some privacy features which help users to secure their accounts. Many of the times, we don’t use these kind of features which can lead us to a possible trouble. These features are like keeping the login email id, date of birth to only me. Many a times, we fail to understand the privacy features of a social media website and we are unaware of utilizing it. The public access to contact information becomes a key concern for arising any security breach in users account.
4. Clicking on Enticing Ads: Viruses and malware often find their way onto your computer through those annoying, but sometimes enticing ads. These kind of ads are some common. A person uses these enticing ads to steal the information of any social media website. When we see such kind of an ad, we are in keen interest to know the more information behind the ad.
5. Using Third Party Apps: Third party apps are now part and parcel of social media websites. Users are seen busy on social media websites while using these kind of apps. Now a days, the social media website like Facebook is showing the appearance of its user to his friends that you friend is online and is playing this kind of game. The person who wants to use these kind of apps needs to grant access to the third party app and then can use these kind of apps. While some apps demand apps to personal information while as some demand for contact information.
6. Common Passwords: Using a common password in online accounts is yet another major concern. Many users use only one common password for different kind of accounts. Sometimes if one account is hacked for one or the other reason, the person gets in trouble as the hacker is now in command of all the social media accounts. Lack of understanding to set a strong password is unavailable among the social media users.
7. Clicking malicious links: Hackers usually send a link to victims and the victim is asked to click the link to claim a special offer. The victim clicks the link and is redirected to another website immediately where he finds nothing like an offer. The user then is in trouble as the information of his social media website is leaked and is automatically sent to the hacker. The hacker gain access to his account and can perform any kind of activity on the victims account.
8. Using Virtual Private Networks: We usually use Virtual Private Networks to access those sites which are blocked by our network administrator. However to by-pass the ban, we make use of Virtual Private Networks apps which keep tracking our data in the background. These Private networks sometimes become helpful for us but may cause of many security issues.

3. How to be ensure safe Social Networking

1. Clearing browser history: We usually make use of different kind of browsers where our username and passwords are kept save by the browser. Those people who use our system may have access to different websites where our login details are already saved. To avoid this security concern, we should always clear the browser history.
2. Two factor verification: Using two factor verification is considered by many social media websites. This verification method helps to prevent unknown access to our account. Here the person who own the social media account receives a text code on his registered mobile number to grant access to a new login on his account.
3. Updating Privacy Setting: Use of privacy setting is very much important now a days. Hiding the contact information like email, Date of birth, mobile number help us to avoid hacking of our social media accounts. Hackers use different kind of ways to access the social media accounts by using the persons contact information.
4. Avoid clicking ads on social media: Social media is full of ads. The users always click different kinds of ads as these ads are very much attractive. After clicking these ads, user is redirected to another website, where is contact information become visible to attackers.
5. Avoid using third party apps: Using third party apps is common today where a user downloads an app and when he start to use it, he is asked to sign in with social media accounts. We sign in with social media accounts and our information on our social media account gets shared with the app. The app uses that information to access our account even the app become capable of sharing contents on behalf of the person. So to avoid such security issues, we should never use our social media information to sign in to any app.
6. Minimizing the use of Virtual Private Networks: Virtual Private Networks usually works as key loggers. What we input in our system, is stored by the virtual private network app. It many a times can prove very much harmful for us.

7. Using different and strong passwords: To be on the safer side of social media, we always should use a different password for our online accounts instead of common password. Social media websites always recommend using of a strong passwords where the password consists of not only numbers but alphabets, special characters etc.
8. Don't trust a message: Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.

4. Conclusions

The world is getting closer and everyone wants to be connected. Static blogs and websites are losing popularity. World is moving more towards "information streams". The information comes to users rather than users have to make effort to get the information. After all the advantages, the problem that arises is of information overload and security. Social networks, unlike the common media, do not have a pattern as to how much information has to be conveyed and where to draw the line. Too much of information may confuse users. Security might be another area of concern where people can get illegal access to a user's information. The future of social networking looks very promising but still it has to deal with the problems associated with it.

References

1. Ahmad I. What Happens in Just one Minute on Facebook? Social media today, 2014. Retrieved from https://goo.gl/1rqAR8.
2. Bicen H, Cavus N. The Most Preferred Social Network Sites by Students. Procedia Social and Behavioural Sciences. 2010; 2(2):5864-5869.doi:org/10.1016/j.sbspro.2010.03.958.
3. Gunatilaka D. A Survey of Privacy and Security Issues in Social Networks. Washington University, 2011. Retrieved from https://goo.gl/JfbUp2.
4. Global social networks ranked. The Statistics Portal. Retrieved from https://goo.gl/cuuGTZ.
5. Internet Security Threat Report Symantec, 2018, 23. Retrieved from https://goo.gl/wPHtHX.
6. Stroud D. Social networking: An age-neutral commodity—Social networking becomes a mature web application. Journal of Direct, Data and Digital Marketing Practice. 2008; 9(3):278-292.
7. Vitak JM. Facebook Friends: How Online identities Impact Offline Relations. Washington, D.C, 2008. Retrieved From https://goo.gl/R4WdWd.