



A Study on How to Protect Your Social Media Privacy

Pooja R. Gaikwad

Department of Commerce
Pune District Education Association's
Waghire College of Arts, Commerce and
Science, Saswad, Tal-Purandar,
Pune - 412301
(Savitribai Phule Pune University)

Dr. Narsing S. Giri

Department of Commerce
Waghire College of Arts, Commerce and
Science Saswad, Tal-Purandar,
Pune - 412301

ABSTRACT:

People nowadays are very active on social media platforms, such as We investigate a privacy threat to a social network in which an attacker's goal is to get knowledge about a significant fraction of the network's links. In terms of look ahead, we formalize the standard social network interface and the information about links that it delivers to its users. We study a credible threat wherein a virtual way user accounts to gather information about the network's surrounding communities and piece them together to produce a global picture. We explore the number of users accounts an attacker would need to subvert for a successful attack, both experimentally and logically, as a function of his approach for selecting users whose accounts to subvert and the network's look ahead. We conclude that such an attack is practicable, and that any social network that wants to preserve its users' link privacy should choose the look ahead of its interface with care, restricting it to 1 or 2 whenever possible.

Keywords: *Media, Social network; Privacy; Security issues; Client information*

Introduction:

In India now a day's technology use has been increased. We see the changes rapidly in Information technology within the past 20 years. So, from last decade we saw a gastric changes in social media and its speed are extremely high. Thanks to technology and social media there are numerous crimes increases. Constant violation of regulations associated with social networking has resulted in civil and criminal cases that require urgent attention. With repeated cases of faux news and trolling, the laws governing social media got to be understood. This text will discuss on privacy and social media. In India teenager are use social media on large scale. They're easily share their personal information on social Accounts. Thanks to this habit teenagers are getting to face tons of



issues regarding privacy of their social accounts. When the user is open their account they give a permission to the present site for access personal information. Then they face cybercrime issues. So, due to that they need to aware of social media and their privacy rules and regulations. When these sites ask to access permission, they strictly avoided to offer this type of permission.

For web users, social networking sites including Facebook, Twitter, Instagram, and Snap chat have become digital billboards. People do enjoy sharing their personal opinions on what is happening in their daily lives. But pause for a moment and ponder what you've just said. This info, some of it pretty personal, is being released on the internet. How many of us are going to look at what you post except your trusted group of friends and relatives? Phishing sites, vengeful acquaintances, and even cybercriminals could all be interested. Nowadays, particularly in light of the Cambridge Analytical scandal, the argument between privacy rights and social networking platforms has sparked widespread public and political discussion. Phishing sites, vengeful acquaintances, and even cybercriminals could all be interested. Nowadays, particularly in light of the Cambridge Analytical scandal, the argument between privacy rights and social networking platforms has sparked widespread public and political discussion. With this in mind, we've put together some pointers to help you preserve your privacy while somehow making social networking more enjoyable.

Objective:

1. To understand how to protect social media privacy.
2. How to create Awareness of Social Media act.
3. To understand the Act related cybercrime.

Purpose of study:

Social networking sites like Twitter, Tumbler, Facebook, Telegram, Instagram, Linked In, and Snap chat have morphed into digital billboards for internet users. The vast amount of personal information that people disclose on social media attracts followers those outside their trust - worthy circle of relatives and friends. For reasons you may not be aware of, much of what you do on social media is recorded elsewhere. The authorities, Spambots, ad corporations, vengeful acquaintances, and, worst of all, cybercriminals may be interested in your personal data. In this post, we identify solutions to preserve your privacy on social media based on these privacy issues. We trust that by using the information in this post, you will be able to take the necessary steps to safeguard your social media privacy. In this post, we identify solutions to preserve your privacy on social media based on these privacy issues. We trust that



by using the information in this post, you will be able to take the necessary steps to safeguard your social media privacy.

Research Methodology:

Methods of exploration in order to fulfill the above-mentioned goals, the researcher needed to collect primary data from users who had also been currently involved in the use of social networking sites throughout one way or another. A data survey study design was created as a result of this. The research study selected a group of persons from a broad group of people from whom data was collected using survey research design. These people's comments were interpreted as representing the collective opinion or response of everyone in the research environment. The researcher employed a quantitative data collection strategy to acquire data for the study as part of the survey re-search design.

Act to avoid cybercrime:

People, particularly youths, are very engaged on social media. The Information Technology Act, passed in 2000, governs social media in India. This was put in place to control the issues that arose from the use of information technology. The right to freedom of speech and expression is guaranteed by Article 19 (1) (a) of the Indian Constitution of 1950. This is a basic human right. However, it is important to remember that freedom of expression does not grant someone 'complete' freedom. This does not guarantee that they will be able to write or speak whatever they want. Any news or information transmitted through social media/networking platforms must have its context or intent monitored and examined. The validity must be verified because it has the potential to have a huge impact on the population.

What is Social Media?

Social media in recent times has become synonymous with Social Networking sites such as Facebook or Micro blogging sites such as Twitter. However, very broadly social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content.

Need for Social Media awareness:

It's impossible to escape social media these days. Your company is almost surely using Twitter or Facebook to promote itself but communicate with potential clients, and if that isn't the case, your coworkers are almost probably using social media towards some extent. Getting into the wrong hands' information is undoubtedly the most dangerous aspect of using social media, and there are several ways in which it can be destructive. Potential burglars are on the lookout for individuals on vacation, hackers are hunting for information they may use to break



into your accounts, fraudsters are on the lookout for people to con, and identity thieves are on the lookout for easy targets. Nowadays, social media networks are abundant, and they have connected us in ways we could have never imagined five years ago. We instantly share information and updates with the networks of connections we've created, and we're inundated with updates from those same networks. While exchanging information in this manner is helpful for a variety of reasons, it also carries a number of disadvantages.

Privacy concern:

1. **1. Impersonation and account hacking:** Spammers, hackers, and other internet criminals are increasingly targeting social media sites. A hijacked social media account is an interesting target since they can impersonate you if they can get into your Facebook or Twitter account.
2. **Being forced to divulge passwords:** Regrettably, you may be required to provide over access to your networking site accounts in some circumstances. One of the most prevalent occurs when a person begins a new job. Employers are increasingly requesting access to workers' social media accounts to guarantee that confidential information or trade secrets are not shared.
3. **Personal data is being leaked through Facebook apps:** Several times, it has been revealed that certain Facebook apps are releasing private information about users to advertising and Internet tracking organizations. And without the users' knowledge!
4. **Social media tracking on the internet:** Several social media sites allow advertisers to embed cookies and beacons - small bits of software that follow your movements on a website and collect information about what you're doing. Note that these monitoring methods are frequently used online, but mostly on websites aimed towards children and teenagers, raising serious concerns about children's online privacy.

How to Protect your Social Media Privacy:

1. **Read the terms and conditions of the social networking site:** Almost webpage on the internet, including social networking platforms, has privacy policies. It is critical to read and understand the privacy conditions of any social media site before signing up for an account.
2. **Activity Status should be hide:** Your followers can see if you're active, offline, or the last time you were online on numerous social apps. If you don't want your activity status to be visible to all of your friends, several social apps allow you to disable it.



3. **Don't give out personal information such as your full name and address:** Your entire name and address should be kept to yourself. The same advice applies to publicizing the full names of your children or grandchildren. Sharing people's complete names may appear harmless, but then you never know how well a stalker or cybercriminal can exploit such information. Remind your teenagers to follow your example, as they are more inclined to divulge personal information. When joining an online platform, your children might not even think twice about providing about their name, location, or other personal information.
4. **Disable the Read Receipts feature:** Turn off read receipts in social networking apps to preserve your privacy even further. Read receipts are messages that inform your contacts that you've read everyone's message. You can stop read receipts in your direct messages on Twitter, but doing so will prevent you from knowing when others have viewed your message.
 - On the top left, tap your avatar symbol.
 - Select Privacy and Settings.
 - Go to the Privacy and Security section.
 - Uncheck the box that says "Show read receipts."
5. **Use caution when sharing images on social media sites:** If you're going to post a photo, think carefully. You may be sharing too much info for what you believed was an innocuous snapshot, even if you don't expressly share a child's name.
6. **Use caution when sharing images on social media sites:** If you're going to post a photo, think carefully. You may be sharing too much info for what you believed was an innocuous snapshot, even if you don't expressly share a child's name. Consider the following scenario: At the big game, you want to post a digital snapshot of your grandchild in their new sports gear. What's the problem, you might wonder? A stranger wouldn't have too much trouble figuring down your grandchild's location and identity if the photo included the school's name, either on uniforms or in the backdrop. If you know how, consider blurring or clipping such sensitive elements. If not, it's possible the photo isn't the best to share.
7. **Change the privacy settings on the social media platform:** Controlling privacy policies on social media platforms differs by platform. Always consider who can see, react to, or comment on your article or photos before sharing them. When examining your privacy settings for each platform, consider whether you want your social media



posts and photographs to be available to everyone, simply friends, or groups of friends. For each article, you may also create a custom list. Tagging pals can be a lot of fun, but can also be a privacy infringement.

8. **Keep an eye on your privacy settings:** Websites like Google are steadily making it possible to limit who accesses your personal information to trusted pals, and Twitter, Instagram, and many other platforms have choices to limiting who can view your posts and who may follow you.

Conclusion:

It has just been noted that privacy concerns in social networking sites are quite weak, and users' efforts to make necessary adjustments to their social media privacy are far lower than in other modes of security operations. Furthermore, many social media users lack technical skills, resulting in minimal privacy concerns regarding their individual content. Most of the other flaws and hitches on the technological side of privacy - related safeguards on social networking sites were discovered in the numbers collected. As a result, we identified the possible source of the problems and offered improvements to address environmental and social networking site's privacy concerns. We could safeguard the social network by imposing a set of well-defined norms for social media, such as using a strong password, updating passwords frequently, being mindful of information leakage, knowing the purpose of antivirus or related software, and proprietary software, among other things.

Reference:

1. <https://www.taylorfrancis.com/books/mono/10.4324/9780429202834/social-media-communication-jeremy-harris-lipschultz>
2. <https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/>
3. <https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html>
4. <https://www.hilarispublisher.com/open-access/social-network-and-privacy-2165-7912-1000288.pdf>
5. [sciencedirect.com/science/article/pii/S1877050916000211](https://www.sciencedirect.com/science/article/pii/S1877050916000211)
6. <https://it.wisc.edu/news/4-ways-to-better-protect-your-privacy-in-social-media-apps/>