DATA PRIVACY IN SOCIAL MEDIA

NADIR ABBAS

Did you know that, on average, an internet user spends more than two hours on social media or that forty-five percent of the world's population uses social media? That means evidently 3.48 billion people are online right now. Networking sites like Facebook, Twitter, Instagram, and Snapchat have become digitized advertisements for internet users rather than just an app.

With the increased use of social media, there comes a privacy concern. Although today's widespread use of social media cuts across all age groups, according to 2019 reports, children and teenagers are the most active Internet users, and they are the least aware of how to secure their personal information on the Internet and, therefore, most exposed to cyber-crimes involving breaches of information privacy.

Unlike other topics that may come and go, data privacy remains a top concern of users online. According to a research analysis among UK and US adults, 29 percent are concerned about how businesses utilize their data. In contrast, 36% of consumers are worried about their privacy but have their profile on public and are not actively willing to change their behavior.

Since these apps are designed solely for connecting and sharing, achieving complete anonymity on social media is quite challenging. According to recent allegations, some of the world's top corporations, including Amazon, Microsoft, and Facebook, as well as different government agencies, are gathering information without consent and keeping it in databases for future use. On the other hand, a recent documentary called "The Social Dilemma" states that users are the product, and their data is what social media is selling to big corporations. Companies analyses our behaviors on internet platforms and then extract the capital generated by people online to enhance growth and advertising income. Therefore, in this digital age, it is nearly hard to claim privacy.

Cybercriminals are skilled at duping social media users into disclosing and stealing personal information and obtaining access to accounts that users deem private. For example, cybercriminals use phishing to get sensitive personal information in the form of an email, text message, or phone call. These communications dupe users into disclosing passwords, banking information, or credit card information. Additionally, one of the social media threats includes Malware sharing, which is a method of gaining access to a user's computer. Once an account has been compromised by acquiring credentials via a phishing attempt, hackers can use it to disseminate malware to all the user's contacts and further use malware to steal personal information, extort money, or profit from forced advertisement. On the other hand, social media bots are commonly used to steal data, spread spam, and conduct distributed denial-of-service assaults, which aid hackers in gaining access to user's devices and networks.

The apparent lack of privacy on social media makes it necessary to safeguard users' online privacy before sharing anything on any social media network. All social media platforms have privacy policies, and therefore, before creating an account on any social media platform, it is critical to comprehend their privacy policies. Most social media default privacy settings may allow your information to be shared with other third-party internet users if it is not checked by the user beforehand. For example, when you make an Instagram account, it is public by default; therefore, changing the privacy settings may restrict the amount of information shared by the social networking site with other users without your awareness.

Consider the following actions to address the issue of lack of privacy.

- Use unique passwords for each of your social media accounts.
- Avoid utilizing public computers for social media accounts.
- Avoid clicking on social network links, especially click baits.

Secure your social media accounts password by using protection apps for that purpose.

In conclusion, the improper use of social media can lead to security breaches and expose information that can lead to privacy violations—as a result, educating users about the risks of exposing sensitive data and promoting awareness of individual privacy is critical. This will lead to a more secure social environment. Furthermore, the use of social media should be regulated by universal standards, regardless of ethnicity, culture, religious beliefs, or socioeconomic standing.