

Social media platforms and the use of social media has evolved over time, to become a core component of modern living and socialization. This can be attributed to the advancement in technology and increased internet accessibility across the world. Over the last twenty years, we have experienced a rise in the number of social media platforms developed in a bid to make the world become more connected and virtually reduce the distance between us and our family members, friends, colleagues, or other like-minded individuals who may not have necessarily met in person. This has made the world smaller virtually and enclosed us in one global village.

Although social media has brought about many benefits such as building communities and relationships, making information widely available and accessible, and increasing visibility; there is a rising concern on how secure our personal information is on these platforms. We tend to share a lot of our PII (Personally Identifiable Information) on these social media platforms, including our names, email address, location, and interests; where they are also publicly available. This information can be valuable to advertisers, and if it falls into the wrong hands, it can also be used for identity theft or other malicious purposes.

Personal privacy is the right of a person to maintain the secrecy of their private affairs, including their private discussions, beliefs, and day to day life activities. A person's right to personal privacy includes the ability to decide how their names, address, and phone number are to be used and disseminated. In the contrary, information privacy refers to safeguarding of information against illegal access to, or disclosure of a person's private or sensitive information, such as their financials, health biodata, or legal information. The right to govern how one's personal information, such as their browsing history, social media activity, and online transactions, is also a part of information privacy.

Whereas information privacy focuses on an individual's sensitive or confidential information, personal privacy is primarily concerned with a person's private life and activities. In the current digital era, where people increasingly rely on technology for communication, information sharing, and business transactions, both aspects are crucial and require some form of control and protection.

With the rise in use of social media platforms, it is becoming increasingly important to take steps to protect the security of information shared and ensure that there is some level of control to access of this information. Here are some ways to do so:

1. Be cautious when sharing information on the platforms:  
We should be vigilant when disclosing personal or sensitive information such as your home location or personal contacts on social media. Such information could be utilized by attackers to track you or impersonate you for use in illegal activities. Moreover, use caution while downloading files and attachments or clicking links from unidentified sites because they can be infected with viruses or malware that can damage your data.
2. Review your privacy and accessibility settings on the applications: Examine the privacy settings for each of your social media accounts and update them as needed to ensure that your information is only visible and accessible to those you trust.

3. Use strong passwords:  
Do not use the same password for several accounts, instead, use strong, unique passwords for each of your social media accounts. A good and secure password should have a minimum of 8-12 characters and be made up of a combination of letters- both upper case and lower case, numbers, and symbols. It is also good practice to change passwords every three months.
4. Activate two-factor authentication:  
Two-factor authentication, which most social media platforms offer, gives your account an additional layer of security. This implies that even if someone gets to get their hands on your password, they won't be able to access your account without also getting hold of your phone or another reliable device.
5. Update your devices and applications:  
To reduce the chance of having vulnerabilities that can be exploited by hackers, keep your computer operating system, web browser, phone and other software up to date with the most recent updates
6. Use a VPN:  
Consider utilizing a virtual private network (VPN) when connecting to public Wi-Fi networks in order to secure your data from hacking and other threats.

Although security cannot be completely assured due to the changing nature of technology, You can help safeguard your data and reduce the possibility of your personal information getting into the wrong hands by following these measures.