**Stay Safe While Using Social Media**

Although social media interactions appear harmless on the surface, there are chances of unintentional exposure to stalkers, hackers, and identity thieves even as you share your private life with friends and family. Obviously, it makes sense to take the right security measures for curbing your online risks. As you think about social media safety, remember that it goes much beyond only avoiding the wrong people online. You also need to be cautious about crossing personal boundaries with your friends, teachers, coaches, and professional associations.

Hence, it becomes critical to understand what to share, how much to share, and with whom to share it while you network personally and professionally. Here are some basic rules that have you fully covered when it comes to social media security.

**Rule 1: Verify your connections**

Even before you think about practicing caution with the information you share, there is a need to be watchful about the people you connect with. Apart from the family, friends and acquaintances, you may also want to connect with people you don’t know for the sake of extending your network. But not every other connection may be genuine; people do put up false accounts these days. If you are not convinced about the authenticity of an account, unknown or one that claims to belong to an acquaintance, it is important to verify them.

Users often set up such accounts to misrepresent themselves as someone else or make false statements on their pretext. The intention is to embarrass the real person or even create legal or personal problems for them. Further, fake accounts may be set up to send connections to malicious sites or commit online frauds. A periodic look at your connections is important so that you can detect the fake ones and get rid of them. This becomes more important if you have a long list of followers, which tends to hide such dangerous accounts.

**Rule 2: Privatize your social life**

While being careful about your connections is important, you cannot overlook the value of privatizing your social life. Thankfully, social media apps have effective privacy settings that let you change your personal profile to private. By doing so, you can make sure that only your friends or followers will be able to see your posts or interact with them. Simply speaking, you can be the gatekeeper for your accounts on the network and prevent any unauthorized access. The privacy permissions differ for different platforms but they have you reasonably covered when it comes to security. Some come with specific options that even let you share the posts selectively with your friends and followers as well. Before you start using a platform, go through these privacy settings and set them up. Also, understand how you can work on the privacy of individual posts in case you don’t want everyone in your connections to see them.

**Rule 3: Be judicious about what you share and consider any posting permanent**

Whether it is a personal or professional social media network you are using, practicing caution while sharing information is the key. These websites give you the option to share your details with the connections, but you need to be judicious about what to reveal. For example, sharing your date of birth, home address or phone number is not a great idea as it can pose a physical or online security risk.

Further, you need to be extremely cautious about your financial information such as credit card numbers, banking information or passwords. If these pieces of information fall in wrong hands, you may end up losing money or even compromising your bank accounts. Even small personal and financial details can make you a victim to crimes such as identity theft and stalking. Also note that anything you share, while ‘deletable’ may show up elsewhere. On the internet, few things are ever truly gone no matter how careful you are. If you don’t want your family seeing it, don’t share it on social media even using an anonymous account.

**Rule 4: Be especially careful with posts and pictures**

Needless to say, you have to be careful about your personal and financial details when it comes to social networking. But you have to be equally vigilant about posts and pictures as well, particularly if you have a big following that includes people you do not know personally. There are plenty of impersonators and people with malicious intentions out there, making it vital to understand the value of privacy.

Avoid posting strong opinions and derogatory remarks against a public figure or community if you want to steer clear of trouble. If you are a selfie-lover, stick to pictures that are decent enough to share publicly. You can check out some good [captions for selfies 2020](https://www.facetuneapp.com/awesome-selfie-captions/) to add a storytelling appeal to the pictures. But be sure to think twice before posting anything on the social media because you wouldn’t want attention for the wrong reasons.

**Rule 5: Avoid over-friending on social networks**

Though you may want to have an impressive number of friends or followers on social media, it may not be a good thing in the long run. You may end up with a large number of fake accounts in the friend list and even have some people who befriend others with wrong intentions like hacking or stalking. There are others who cause problems by introducing spam into your timeline. As a rule, prioritize connecting with people you know or at least, the ones who are friends with your friends. Don’t just add people in your friend list to be in competition with others who have hundreds or thousands following them. Limiting your friends will enable you to share information more confidently and without apprehensions about being wronged. So you should stick to the rule of less is more for staying safe on social media!

**Rule 6: Avoid posting your location**

Another mistake that users often make is posting their location virtually as it can endanger your safety in real life. It may feel good to brag that you are on an overseas vacation or checking out the hottest new pub in town, but you end up telling unknown people that no one’s home. Similarly, scammers and predators are on a look out for easy targets at tourist check-in spots and popular venues. Moreover, the disadvantages of posting your location and live pictures go beyond the explicit risks. There are chances that your friends may put two and two together and see through excuses for not hanging out with them. Maybe, your boss and colleagues would come to know you weren’t sick on Friday when you post pictures at the resort on the weekend.

**Rule 7: Keep an eye on your own account**

While you must be vigilant about your connections and people who like or comment on your posts, there is also a need to monitor your account as well. It is easy to assess the security of your own account by simply searching it with a third-person perspective. By doing so, you will be able to see what others are seeing on your account. Obviously, you will get a clear idea about what you are sharing with the public and whether it is too much.

Another benefit of checking out your own account is that you will be able to detect if there are false accounts set up in your name. This is simple because they will turn up when you search your profile by its name on social media. A periodic look at your account, therefore, serves a dual benefit. You can review the information you are sharing socially and also see if someone is running a fake account in your name.

**Rule 8: Block unfriendly connections**

While social media is a great platform to interact with people you know and build personal and professional connections, you cannot be really sure about their credibility. There are chances that you may come across unfriendly connections more than once. Fortunately, you have the option to protect yourself from harassment, stalking or unwanted contacts on social media.  When you join a social network one, be sure to check the blocking option in case you need to block a member you do not want to interact with. Once you block a connection, you can rest assured that they will not be able to access your account or get in touch with you again. This is surely a good way to stay safe.

**Rule 9: Protect your accounts with a strong password**

Another social networking safety rule that you cannot afford to overlook is the protection of your accounts. Security of social network accounts is as important as that for your computer or any other online account. First things first, you need a strong password that is capable of preventing hackers from getting access to your account and posting spam or malicious content through it. There are some simple password creation rules that can give you all the protection you need. Opt for a password that has no less than eight characters and includes numbers, letters and special characters in it. Steer clear of common practices like using your name, date of birth or any other common data as a password. Also, changing it every few months keeps your account safe to a considerable extent.

**Rule 10: Be extra careful with your business accounts**

Yes, sometimes students have businesses–especially using digital media, streaming games, etc. The safety of a business social media account is even more critical than that of your personal accounts. Business accounts are meant to be public because you want to connect with present and prospective customers and stay in touch with them. But you should be wary of strange messages, odd names, and repetitive friend requests from duplicate accounts while managing business accounts. Additionally, you also need to be mindful about the people you do business with on social media. Sharing information and posts across these networks requires extra caution. There are chances that you will receive a message about a great business opportunity online, but it could be a scam as well. So verify your connections carefully and go ahead with any offers only if you are sure about their credibility.

**Rule 11: Follow the rules of professional networking**

There are some key rules that you need to follow carefully when it comes to using professional networks like LinkedIn. Keep things professional when it comes to the images, posts and personal and professional details you share on your account. Ideally, it should be a glimpse of your professional skills, achievements and goals rather than what you do personally. The same rules apply to the connections and interactions as well.

Often, people end up losing their jobs because of their activities on social networking sites. Your employer will probably have some policies related to sharing official stuff on social media, which you need to follow stringent. The idea is to protect the intellectual property, confidential data and reputation of their business. So you must certainly follow the rules and guidelines of your company as you use social media.

Safety on social media is as good as offline safety, which means that you should be careful on both fronts. Be aware of everything you share online, whether it is your personal or professional details or what you do in everyday life. Although the right to share bits of your life is totally yours, just be conscious about sending wrong things to the wrong crowd, particularly the people you are connected with only online. Pay attention to every single interaction because you wouldn’t want to get involved with a shady stranger, share private information with a hacker or get into trouble with your employer. Although there is no harm in enjoying your social media time, you must go the extra mile to make safety your top priority.

contributed by **Louis Burgman**