Security Best Practices for Staff, Clients, and Community Stakeholders

The best practices in this guide are designed to help clients and community stakeholders protect themselves from threats, harassment, and targeted hateful messages through their personal social media accounts and are designed to help staff protect themselves throughout their personal lives.

Social Media Security Best Practices

Best Practice #1: Review your privacy settings

Review the privacy settings on your social media accounts so you know how visible you are to your followers and the general public. Depending on the platform, you can adjust your settings so only people who already follow you can see your content and everyone else requires your permission to follow you.

Adjust your settings as you feel appropriate. We know, especially for publicly-facing and high-profile individuals, being completely private may not be the best or right decision for you. We also know you may have a lot of followers across platforms, many of whom you may not personally know and making your account(s) may not fully protect you from hateful messages or harassment.

Best Practice #2: Block users

Blocking users prevents them from viewing your profile and content, and reaching out to you via comments and direct messages (DMs). It also may make content made by that user no longer visible to you. It's important to note that, depending on the platform, users may be notified when they have been blocked.

One thing to remember about blocking a user is that this doesn't prevent that user from talking about you or your work on the platform – it just means they can't engage directly with you and you won't see what they are saying, which may be anxiety producing.

Best Practice #3: Mute users

One alternative to blocking users is to mute them. What you can mute varies by platform, but the basic idea is to prevent you from seeing certain users, content, DMs, comments, etc. In your social media feed by default. Muted users are generally not notified they have been muted. As with blocking, muting users comes with the same concerns.

Best Practice #4: Restrict users

Another alternative is to restrict users. Again, this varies by platform. In some cases, restricting puts user comments into a folder for you to review before allowing it to post to your account. In other cases, it may enable you to select the audience who can see and reply or interact with your content.

Best Practice #5: Restrict messages

Another alternative to further restrict users is to modify which users have access to openly messaging you. Depending on the social media platform, you can ensure that you only receive messages from users you follow. This will help to limit contact containing any potential hateful messages or harassment.

Best Practice #6: Report users

Reporting users notifies the social media platform about a harmful user. By reporting the user, the social media platform can investigate their actions further and work to restrict their access to the platform. By reporting abuse that violates the terms of service, there is the potential to have the harmful post taken down or to see the user's harmful account suspended.

When you may be unsure of whether or not to report a user's actions, and if you are comfortable, always defer to reporting. By reporting all instances of harm and harassment, malicious actions can be more appropriately flagged on social media platforms.

As a note, the reporting timelines vary across social media platforms. Additionally, it is important to understand that the effectiveness of reporting mechanisms varies across platforms.

Best Practice #7: Remove personal data online

Some websites store personal data such as your name, email address, physical address, phone number, and other data about you, and may buy or sell that data online in a way that could put your privacy, and occasionally your physical safety, at risk. When your personal data is exposed, it could make you vulnerable to surveillance, stalking, doxing, social engineering scams, identity theft and more. Due to these factors, it is advisable to remove personal data from the internet. DeleteMe is a paid service that removes your personal information from multiple online directories. The service searches and removes your personal data from data broker sites every 3 months.

Physical Security Best Practices

Best Practice #1: Identify exits and relevant fire routes

As you walk into new rooms and spaces, it is helpful to always be aware of exits if a situation should occur. When walking into a new space, note the entrance that you entered through and do your best to scan the area to determine any other exits. If you are in large outdoor spaces, it is helpful to locate a map to obtain your bearings of the physical space. If you are in indoor spaces, it is important to identify any relevant fire routes in the event of an emergency.

It is also important to be aware of your surroundings and the people around you. If you need to exit a space or get to a safe location, what is the safest path for you and your group to do that? Discuss your plan with your group. You may also want to identify a "safety point" where you will all gather if you need to evacuate an area during an event.

When evacuating or leaving a space as part of de-escalation, do so as calmly as possible. Move quickly but avoid running when possible.

Best Practice #2: Travel in groups

As you travel from place to place, it is important to travel in groups when possible. By travelling with other individuals, you reduce any threat of personal harm and have peers if an emergency should arise. When you are unable to travel with a group of friends or known-individuals, it is essential to stick to travelling on streets and sidewalks that are well-traveled. This will ensure that you avoid any possibility of walking alone. Traveling in groups is especially important at night, when fewer people may be around you.

Best Practice #3: Travel on well-lit streets

Similarly to using well-traveled streets, remember to use well-lit streets whenever possible. Light is especially important at night and in the event you are traveling alone. Further, light helps you to be alert of your own personal surroundings and works to ensure your safety.

Best Practice #4: Walk without headphones

When walking, the absence of headphones is important as it helps you to be alert in your own surroundings. Headphones can work to cause unnecessary distractions and limit you from your ability to hear any important announcements or signals that may occur in your environment. When possible, walking without headphones is strongly recommended.

Best Practice #5: Park carefully

If you travel by car, always do your best to remain conscious of your surroundings. As you park, try to use well-lit areas whenever possible. If these are not available, try to park your vehicle by others to limit any potential threat. As you prepare to exit the car, remain alert. Finally, always lock your doors promptly as you exit your vehicle.

Best Practice #6: Utilize public transportation carefully

When utilizing public transportation, it is important to stay awake and alert. Not only does this ensure that you do not miss your stop, but it is critical if you are traveling with personal information to keep it secure. When traveling anywhere, you should always know your planned route. This limits any potential confusion and protects your ability to travel from place to place safely.

Best Practice #7: Inform family and friends when travelling

As you move from place to place, it is helpful to inform your friends or family whenever possible. By notifying them of your plans, they can help to track your location or be mindful of any anticipated arrival time. Notifying friends and family members of your travels and commutes simply ensures that you have one more individual looking out for your safety.

Best Practice #8: Turn off geo-locating on social media

As a matter of personal security, it is important to minimize any application that may have access to your location. For instance, many social media applications request your location. If you have to allow any application to access your location, it is helpful to only allow access while the application is in use. By sharing your location in a public manner constantly, strangers may be able to track your location which may leave you more susceptible to harm.

Best Practice #9: Share your personal technology devices carefully

It is important to limit any sharing of your personal technology devices whenever possible. If you have to share your device, work to restrict what personal information is publicly available on the device. Additionally, if you hand your phone to a stranger for a photo, be sure to have your phone in the locked mode. This limits a stranger’s ability to access any personal information on your phone.