Social Media Guide:
Tips for Mitigating Harassment & Limiting Escalation

As social media plays an increasingly prominent role in our everyday lives, Banksy's take on Warhol's famous adage becomes extremely relatable – *"in the future, everyone will want to be anonymous for fifteen minutes*." While social media brings many benefits like staying connected with friends, it also leaves many people vulnerable to threats such as cyber harassment, stalking and doxxing. This is especially true for individuals who are members of oppressed communities or who are targeted based on socially or politically charged issues like abortion rights. Secure management of social media accounts has become vital, and individuals who are at risk of online harassment must employ precautions when publicly posting their personal information on the internet.

The recommendations below fall into two general categories: **online privacy** and **account security**. The **privacy** focused settings aim to limit the amount of information about you that strangers can glean from your online presence, while the account **security** tips help protect against unauthorized access to your accounts. Depending on your individual threat model you may be concerned about either of these areas or both. For example, are you more worried about someone piecing together where you live from your tweets (privacy), or are you more concerned about someone getting your Twitter credentials and tweeting something terrible from your own account (security)?

Before diving into the specifics, a word of general advice – the internet is both very permanent and very ephemeral. Any information uploaded to a social media site can also be removed and deleted by that site without your consent. At the same time, posts can be screenshotted and shared even after you delete the original. Any post or picture once uploaded can spread very quickly, almost always irreversibly. Public profiles, accessible by anyone, are more vulnerable than private or restricted profiles. The content of what you choose to post should be carefully selected, and your friend list should be curated with caution.

The following tips have been compiled for popular social media platforms, keeping in mind basic precautionary measures that can enhance protections surrounding your online presence. After reading these general tips, you can check out our specific instructions for managing your LinkedIn, Twitter, Instagram, and Facebook accounts.

General recommendations (applicable to all social media sites):

- Set a quarterly calendar alert to review the privacy settings for your social media accounts. These platforms are always changing, and it's a healthy habit to regularly explore the privacy & security settings available on each platform you use.
- Wherever possible, strive to keep social media accounts private and don't accept friend/follow requests from people you don't know. If you desire to keep a public profile in order to reach a larger audience, maintain different accounts (for example, a private account for near and dear ones, and a separate professional or public account) so that your personal information and data do not inter-mix with their public counterparts.
- If you receive persistent messages from a stalker or suspicious individual, make sure that you inform your friends; dedicated individuals might try to reach out to your friends to gain information about you. In many of these cases, you will need to make a call based on the perceived threat – for example, if an individual sends you some objectionable messages but is otherwise not exhibiting stalking behavior, it might be easier to simply block them.
- Avoid sharing location data or pictures identifying your location. If you choose to share your location, you can take certain precautions such as avoiding posting pictures that show identifying landmarks or only posting pictures of a vacation once you have returned home.
- Limit the amount of personal information on your social media profiles whenever possible:
    - Disable geotagging on your devices and social media sites whenever possible.
    - Avoid tagging your friends and family members in photos accessible via your account.
    - Configure your privacy settings such that other users cannot automatically tag you in photos that could reveal your location or social network.
    - Avoid giving sensitive personal information whenever possible, e.g., do not give your phone number and email address unless it is necessary to do so. You may also want to use a separate email address/phone number for your social media accounts.
    - Take advantage of the privacy controls provided in social media sites that allow you to control the visibility of social media content on a per-post basis.
    - Avoid mentioning your residential address on any social media forum.
    - Avoid giving third party applications access to your social media accounts whenever possible (e.g., Facebook apps sometimes ask you to provide personal information or access your account).
- Make sure that you delete social media accounts that you no longer need, as these accounts might have information about you that a stalker or digital attacker might find useful.

Ready to jump in and change the settings for some of your favorite sites? Keep reading for our detailed instructions for managing your LinkedIn, Twitter, Instagram, and Facebook accounts.

Privacy and Security on Facebook

Note: These instructions may change as Facebook changes its user interface or pushes updates. If you get stuck, we suggest googling "how to [insert setting here] on Facebook" to find updated instructions!

Important Security settings

- Monitor all the active login sessions:
    - Hover over the arrow button at the top right side → click on *Settings* → *Security and Login* → browse to *Where You're Logged In* section → you'll see all the active sessions listed and can log out from any of them.
- Enable Two-Factor Authentication so that Facebook asks you to enter a verification code whenever you login from unusual places:
    - Hover over the arrow button at the top right side → click on *Settings* → *Security and Login* → browse to *Two-Factor Authentication* section → Use two-factor authentication → click on *Edit* → click on *Get Started,* add your phone number and complete the remaining steps.
- You may want to add an extra layer of protection by configuring your account such that you get alerted whenever an unusual login is attempted on your account:
    - Hover over the arrow button at the top right side → click on *Settings* → *Security and Login* →browse to *Setting Up Extra Security* section.
- You can also appoint 3 to 5 of your friends as Trusted Contacts to help you whenever you want to regain access to your account:
    - Hover over the arrow button at the top right side → click on *Settings* → *Security and Login* → Scroll down to *Choose 3 to 5 friends to contact if you get locked out* → click *Edit* → Click *Choose friends* and follow the on-screen instructions.

Important Privacy settings

- Hover over the arrow button at the top right side → click on *Settings* → *Privacy* → you will be presented with *Privacy Settings and Tools* → make sure to limit the visibility of your friends list and posts.
- Under the same *Privacy Settings and Tools*, you can customize privacy settings of your posts, posts you are tagged in, and the people who can send you friend requests on facebook. You can choose to limit these to friends only. These settings can go a long way in managing the privacy of your data and personal information shared on facebook.
- Keep your profile from appearing in search engine results: click on *Settings* → *Privacy* → you will be presented with *Privacy Settings and Tools* → go to *How People Find and Contact You* section→ go to *Do you want search engines outside of Facebook to link to your profile?* → turn off the *'Allow search engines outside of Facebook to link to your profile'* option.

Blocking Users

Facebook allows you to block unwanted contacts or individuals, cutting them off from your profile or any of your posts and profile. Once you block someone, you automatically unfriend them as well. Such a person does not get notified of you having blocked them, although they may find out that you have blocked them because they will be unable to find you on Facebook search results. To block someone in your blocking settings:

1. Click at the top right of Facebook and choose *Settings*.
2. Go to the left side of Facebook and select *'Blocking'*.
3. Click *Blocking* in the left side menu.
4. Enter the name of the person you want to block and click *Block*. You can also block someone using their email address.
5. Select the specific person you want to block from the list that appears and click *Block* > *Block [name]*.

To subsequently unblock a user, you can remove them from your Block list.

Facebook also allows you to block messages from someone, without blocking them from seeing your profile. To block messages from someone on Facebook:

1. From your News Feed, click the Messenger in the left menu.
2. Open the conversation with the person you'd like to block.
3. Click *Privacy & Support* in the right menu.
4. Click Block Messages, then Block Messages.

Remember: Blocking messages from someone does not automatically block them on Facebook. You will still be able to see their Facebook profile and, depending on their privacy settings, their status updates, comments, likes, or other activity.

Managing or Removing access to Third Party Apps

Your facebook account may be linked to a number of third party apps, granting them access to a host of your account and usage related information. You can manage or remove access to such apps by changing your settings on Facebook.

1. Click from the top right of the Facebook page to select 'Settings'.
2. Select *Apps and Websites/Apps* on the menu appearing on the left side.
3. Select the apps or games you'd like to remove.
4. Click *Remove*.

Facebook does caution that even after an app or game has been removed, it may have already accessed and stored some of your information back when you were on the app. In such a case, Facebook links to you to contact the developer to request for deletion of any of the information on you that the app may still possess.

In any case, you can manage and control privacy settings for each app or game while you are signing up for it:

To control your app or game permissions when signing up:

1. Before clicking *Play Now* or *Send to Mobile*, click *Review the info you provide* below the info the app will receive
2. Individually select the categories of information you wish to share and be mindful of what such information sharing may imply.
3. Continue signing up.

Keep in mind that Facebook lets you edit your privacy settings for an app or game at any time. Limiting what you post is one of the best ways to protect your privacy on Facebook. Be sure to review our general tips for social media to build solid privacy habits for all your accounts!

Privacy and Security on Twitter

Note: These instructions may change as Twitter changes its user interface or pushes updates. If you get stuck, we suggest googling "how to [insert setting here] on Twitter" to find updated instructions!

Protecting Your Tweets

- By default, your tweets are publicly accessible, even by users who aren't logged in. You can make your tweets private by navigating to *Settings and privacy → Privacy and safety* and selecting *Protect your Tweets*.

Remember to click *Save changes* all the way at the bottom of the page!

Remember, even when your tweets are protected, the bio, location and website fields of your profile will remain publicly viewable. Be careful what you display in these fields!

When your tweets are protected, you will have the ability to approve or deny other users' requests to follow your account. If you're especially concerned about avoiding online harassment and stalking, you should deny access to users who you don't know. You can also remove existing followers' access. You should be aware, however, that protecting your tweets precludes them spreading beyond your approved followers, since they cannot be retweeted.

Enabling Two-Factor Authentication

The easiest way to protect against unauthorized access to your account is by enabling two-factor authentication.

- Navigate to *Settings and privacy → Privacy and safety* and click *Set up login verification*. Once you complete the dialog, Twitter will use access to your phone number or an authentication app on your phone as a second security layer – when logging in, you'll need to supply a login code sent via text message or generated by the app.

Location Settings

For a user concerned about stalking and harassment, sharing your location can be the most dangerous functionality provided by social media. Twitter's location sharing works differently

depending on whether you're using the mobile app or the web client, so we'll want to disable both.

- In the mobile app, navigate to *Settings and privacy* → *Privacy and safety* and ensure that the *Precise location* setting is disabled.
- On the web client, navigate to the analogous menu under *Settings and privacy* → *Privacy and safety* and ensure that *Tweet with a location* is disabled.
    - You can also use the *Delete location information* button to remove any location information from your previous tweets.

Be sure to review our general tips for social media to build solid privacy habits for your Twitter account!

Privacy and Security on Instagram

Note: These instructions may change as Instagram changes its user interface or pushes updates. If you get stuck, we suggest googling "how to [insert setting here] on Instagram" to find updated instructions!

Managing Privacy Settings

By default, your instagram profile is public, i.e. accessible by any Instagram user. You can make your profile private by changing Account Settings under Instagram. This ensures that only followers' whose request you approve can access your Instagram account. To change your setting to private:

1. Go to your profile, then tap the three short lines at the top right.
2. Open *Settings*.
3. Open *Privacy and Security*
4. Open *Account Privacy* then tap to toggle *Private Account* on.

Once your account is private, even if you use hashtags while posting pictures, your posts won't appear on public hashtag pages except to your followers. A private account also prevents one of your followers from direct messaging/sharing one of your posts to another non-follower, as the post will remain hidden to the recipient.

Additionally, avoid the use of third party web viewers, as using them can lead to your posts appearing on google searches. Instagram is not affiliated with such third party services, but provides a list of commonly used web viewers who users can contact if they wish to revoke their access to their posts (source: Instagram Help Center):

- Webstagram / dm.stagram / search.stagram: Webstagram
- Gramfeed: @gramfeeed on Twitter
- Instagreat: @elliotkember on Twitter
- InstaGallery: http://infinitapps.com/contact.html
- InstaView: http://www.roguesheep.com/support.html

- Flipboard: https://flipboard.com/topic/instagram
- Statigram: contact@statigr.am
- Cityowls: contact@cityowls.com

Blocking and Removing users & Blocking Comments

If you encounter a follower who is behaving like a harasser or stalker, you can block them on Instagram, disabling their access to your profile and direct messages.

- To do this, simply go to that user's profile, tap the three horizontal dots (iPhone) or three vertical dots (Android) to the right of the follower you'd like to remove, then select *Remove*.
- Alternatively, you can select the option to *'Block'* them as well.

Similarly, you can block hateful comments.

- Instagram also allows you to report abusive or hateful behaviour that breaches their internal guidelines. You can report such activity, as well as hacked or impersonation accounts, by following this link: https://help.instagram.com/contact/584460464982589?helpref=faq_content.

Location Settings

Instagram states that by default, its location settings for the app are turned off, subject to the user turning them on while posting a photo and adding a location along with it. You can ensure your location settings are turned off, or actively do so by following the steps listed below:

1. Exit the Instagram app and go to your mobile device's *'Settings'*.
2. Tap *Privacy → Location Services*.
3. Scroll down to select *Instagram*.
4. Select *Never or While Using the App* to set location access.

Enabling Two-Factor Authentication

- To use two-factor authentication to prevent unauthorized access to your account, go to *Settings → Privacy and Security Controls →* scroll down until you see the option *'Two Factor Authentication*' and turn it on.
- Instagram allows you a number of options for this setting. You can choose to receive authentication codes via text message, or by way of integrating with third party authenticators such as Google Mobile or DUO Authenticator.
- You can also choose the option to access *'Recovery Codes'***,** which provide a list of random codes that can be used to log in when you may not have access to your phone or text messages. It is recommended you maintain them securely somewhere other than your phone. Some options include maintaining them in a separate password manager, physically printing them out, or storing them in a safe space locally.

If your account does not have a phone number linked to it, Instagram will ask you to enter your phone number.

- Once you enter your number, tap *'Next'*, and you should receive a verification code via text message. You can similarly follow the process to set up a third party authenticator.

Congrats! You've now taken some important steps to protect your Instagram account.

Privacy and Security on LinkedIn

Note: These instructions may change as LinkedIn changes its user interface or pushes updates. If you get stuck, we suggest googling "how to [insert setting here] on LinkedIn" to find updated instructions!

Accessing Security and Privacy Settings:

- ***Step 1:*** Go to **Me** at the top right side and then click on **Settings & Privacy.**
- ***Step 2:*** Browse to **Privacy** tab to manage your privacy on LinkedIn.
- ***Step 3:*** Browse to **Account** tab and then **Login and security** to configure your security settings.

Important Security Settings:

- Make sure that two-step verification is turned on:
    - *Account tab→ Login and security → Two-step verification*
    - **More details:** you will be asked to enter a phone number, and once you enter it click on *Turn on*. To test if that worked, log out and log back in, you will notice that LinkedIn will send verification codes to your phone number at login.
- Make sure that you monitor active login sessions to your account regularly to spot unauthorized logins to your account early:
    - *Account tab→ Login and security → Where you're signed in*
    - **More details:** If you are signed in from more than one device, you will be presented with a sign out option beside each active session. You can also sign out of all active sessions at once. This is a more secure option, but there is a security-usability trade-off here in that you'd need to sign in again.
- For more security, you may want to change your password to a stronger one:
    - *Account tab→ Login and security → Change password*

Important Privacy Settings:

- Manage the visibility of your profile to non-logged in users (e.g., those who find your profile via search engines):
    - *Privacy tab* → under *'How others see your profile and network information'* → *Edit your public profile* → Use the *Edit Visibility* section to determine whether to *Show* or *Hide* each piece of personal information you have on your LinkedIn profile.

- Manage the visibility of your email address to other users:
    - *Privacy tab* → under *'How others see your profile and network information'* → Use the *Who can see your email address* section to specify who can see your email address.

    - **Advice:** the more restrictive your settings are the better privacy level you get. Keep in mind that your email address could be used to identify your accounts on other online platforms, and that you may be contacted by people who know your email address.

- Manage the visibility of your social connections (friends list):
    - *Privacy tab* → under *'How others see your profile and network information'* → Use *Who can see your connections* section to specify whether you want others to see your friends list or not.
    - **Advice:** Digital attackers could infer a lot of information about you by seeing who your connections are, and therefore it is better to hide them. To do that, choose *Only you* for this option, as this is better from a security standpoint.

- Hide your last name from non-LinkedIn users:
    - *Privacy tab* → under *'How others see your profile and network information'* → Choose the option that hides your last name under *Who can see your last name* section.

- Restrict access to your personal information from your employer's LinkedIn page or other pages which you have connected to:
    - *Privacy tab* → turn off the buttons that appear under *Representing your organization and interests* and *Profile visibility off LinkedIn* sections.

- Prevent others from knowing whether you are online or not:
    - *Privacy tab* → under *'How others see your LinkedIn activity'* → choose *No one* option under *Manage active status* section.

- Prevent the disclosure of other types of personal information whenever possible, some examples are listed below:
    - Don't let LinkedIn notify your friends of your work anniversaries or any other changes in your LinkedIn profile: *Privacy tab* → under *'How others see your LinkedIn activity'* → turn off the button under *Share job changes, education changes, and work anniversaries from profile* section.

- Don't let LinkedIn notify your connections when you are mentioned in the news or other websites: *Privacy tab* → under *'How others see your LinkedIn activity'* → turn off the button under *Notifying connections when you're in the news* section.

- If possible, don't allow others to tag you in their posts: *Privacy tab* → under *'How others see your LinkedIn activity'* → turn off the button under *Mentions or tags by others* section.

- You may want to prevent others from discovering your LinkedIn profile from your email address or phone number: *Privacy tab* → under *'How LinkedIn uses your data'* → choose *Nobody* under *Manage who can discover your profile from your email address* and *Manage who can discover your profile from your phone number* sections.

- Consider blocking accounts that look suspicious to you and report abusive content:
    - Browse to the LinkedIn profile you'd like to block → Click on *More* on the main page → Click *Report / Block* → you will be given the option to block the account or report it as violating Terms of Use, impersonating other person or as being a fake account.

Congratulations on locking down your LinkedIn account!