GUIDE TO SECURING YOUR ONLINE FOOTPRINT

OVERVIEW

After any incident of online harassment, it is important for you to secure your online accounts. Depending on the severity of the attack, you may wish to amend your privacy settings, make your account completely private, change your passwords, or temporarily deactivate your accounts. This quick reference guide will walk you through the steps to secure your online footprint to limit the impact of online harassment.

REVISIT YOUR PRIVACY SETTINGS

All social media platforms have privacy or security settings that limit the ability of strangers to interact with your profiles or pages.

Key settings to review on each platform:

1. Who can see your profile
2. Who can add you to their profile or page
3. What personal information (email, location, workplace, etc.) is visible
4. Who can send messages to you
5. Who can see or comment on your posts
6. Who can tag you in photos or posts

Privacy policies and security settings change frequently and are different for each platform. For the most up to date information on privacy policies and security settings, please visit the specific social media site to learn more.

Twitter | Facebook | Instagram | TikTok | LinkedIn | Snapchat | Discord | Reddit | WhatsApp | WeChat

CHANGE YOUR PASSWORDS

On occasion, online harassment can lead to hacking attempts, which is why it is important to update your passwords, particularly if you use the same password on multiple sites, to new, secure passwords to preempt any hacking attempts. Please visit our page on password security to learn more about how you can create strong passwords and protect your account.

To strengthen your account security, IT Services strongly encourages users to consider opting in to Two-Factor Authentication (2FA). Two-Factor Authentication (2FA) enhances the security of your account by using your phone, tablet, or some other device to verify that you are really the person

attempting to log in when you attempt to access University applications or social media sites. This prevents anyone but you from using your credentials to log into websites, even if they know your username and password.

You can find more information about 2FA and how to use it in the Two-Factor Authentication (2FA) Overview and the Two-Factor Authentication (2FA) FAQ.

MUTE, REPORT, AND BLOCK

All social media platforms give you the ability to report other users and block others' access to your account, and some platforms (Facebook, Instagram, and Twitter) provide you with the option to mute certain individuals or groups that you do not wish to fully block or unfollow, but would prefer not to see or engage with their content.

While it is important to protect yourself from seeing online harassment, it is equally important to report users engaging in online harassment. These reports can be critical in the event law enforcement needs to be involved and can serve as evidence for filings and warrants. Each platform has their own specific process for reporting users, comments, and fake accounts impersonating an individual. Typically, once the report is received, it will be reviewed and a determination will be made whether to delete the comment, suspend the user's account, or in extreme cases, notify law enforcement.

We highly recommend engaging your personal support network to help you report online harassment, as some people may find it difficult to engage directly with negative or hateful comments, and the more complaints a platform receives about a specific user, the faster they will take action.

PERIODIC AUDITS

After the harassment has died down, it is a good idea to audit yourself via a Google search of your name to see what records or articles pertaining to the attack might still be tied to your name. Here are a few ways to manage your online reputation and help control what people see when they search for you on Google:

1. Search for your name on Google to see what information about you comes up.
2. Create a Google Account to manage your information—such as your bio, contact details, and other information about you—that people see across Google Services.
3. Remove unwanted content and the associated search results. If you find content online—say, your telephone number or an inappropriate photo of you—that you don't want to appear online, first determine whether you or someone else controls the content. If the unwanted content resides on a site or page you don't control, you can follow our tips on removing personal information from Google.

CONCLUSION

Even when things die down, you may still feel uncomfortable opening your social media accounts to the general public or making public commentary on an issue, and it is okay to feel that way or wish to maintain certain levels of privacy. Individuals who engage frequently with the public may want to consider keeping personal profiles private and creating new public/professional social media profiles. Professional profiles and pages are useful, because they typically do not contain much personal information (e.g., - friend lists, family members, personal photos, etc.), and allow you to engage normally with friends and family on private channels.

Dealing with online harassment and the aftermath can be overwhelming, but by following the above guidance and following the steps in our Guide to Managing Online Harassment, it is possible to mitigate the potential impact and take control of the situation.