

Guide To Addressing and Combatting  
**ONLINE  
HARASSMENT**



3



# Actions to Take if You Are the Target of Online Harassment

1

Call the police. If you or your family (or another identifiable group) appear to be in imminent danger, call 911 immediately! If you receive threats that you feel are serious but not imminent, call the [SU Police Department](#) (410-543-6222).

---

2

Document it. Take screenshots of potentially harassing messages or posts and save the unique links to posts or messages in a separate document. Be sure to grab information about the user or handle names, their real name, the links to their profiles and any other information about the source of the harassment. This information will be useful to your department chair, supervisor, IT, case workers or police units who may be assisting you and could be used as evidence.

---

3

For faculty. Connect with your administrative leader (department chair, program director, the dean's office).

For staff and student employees. Reach out and alert your supervisor right away, especially if the harassment may be in relation to your work.

If the harassment is gender-based harassment and/or sexual in nature, consult the [Title IX Coordinator](#) to understand your rights and resources.

If the harassment is based on another protected class (e.g., race, age), consult with the [Office of Institutional Equity](#) to understand your rights and resources.

Ask for help before responding to media. If you get contacted by the media, you are not obligated to return the call. Reach out immediately to the [SU Public Relations Office](#) (410-543-6030), who will help you sort through the next steps.

Ask for your personal information to be temporarily removed from the campus directory and webpages and social media. You can ask for your contact information to be removed from

the campus directory, department webpages or even have posts removed from campus social media accounts if necessary. Employees should work with campus [Human Resources](#) and the [Web Development Office](#) for help with website/directory listings. Additionally, if you have other web pages (such as Square Space, WordPress, etc.) turn off commenting features and remove any features that allow commenting, emailing or contact. These features can always be turned back on after the online attack passes.

---

4

Revisit your privacy settings. Social media platforms all have privacy settings that can help mitigate the impact of strangers who can contact you or post comments. These settings give you the power to choose who can see your profile, who can message you, who can tag you and how much information is shared from social media publicly. Each platform is different and privacy settings change frequently.

Change your passwords. As an extra precaution, change your passwords to new and secure passwords to preempt any hacks. Enable two-factor authentication where possible.

Take a social media break. Trolling attacks are typically intense but brief. Engaging with these comments tends to add fire to the flame and it's best to not engage. It can help to take a social media break by temporarily removing social media account apps from your phone, which can alleviate distressing notifications or the urge to check social media.

Mute and Block. All social media platforms have the ability to mute or block users from accessing your social media content. On Facebook, X and Instagram you can choose to "mute" an individual or a post. Muting is a great option if you don't want to completely remove that person from accessing your social channels but want to silence notifications and conversations from them. Muting does not block

an explanation about why you've blocked or unfriended them. (Note: University-run accounts need to go through a different and official process and involves different considerations before

---

---

# Checklist for Academic Leaders and Supervisors Supporting Employees Experiencing Online Harassment









- n Establish open communication with the affected faculty member's dean and request updates, as needed, on the situation.
  - n Reach out to the targeted faculty member, reiterating the University's commitment to academic freedom (as appropriate) and encouraging the faculty member to consult with their department chair for support and assistance.
  - n In consultation with the Office of the President and [Public Relations Office](#), issue a statement (as appropriate) asserting the importance of academic freedom, freedom of speech and committing to the safety of the faculty. The statement should emphasize the institution's mission and values rather than comment on the faculty member's scholarship.
- 

6

Prepare staff to handle phone calls, emails, social media comments and inquiries about the harassment issue. The [Public Relations Office](#) can provide an approved statement upon request. If no approved statement is immediately available, provide the below message to staff receiving calls to use until a statement or talking points are made available:

"Thank you for reaching out about this issue. Our team is aware of the situation. All inquiries and questions about this are being handled by **the SU Public Relations Office.**"

If the attack is impacting an instructor, prepare if, when and how questions about how the situation will be addressed with their students. Keep in mind that if the attacks are threatening and public, some students may feel uncomfortable coming to a classroom. Have a plan to move

# Tips to Help Safeguard Your Social Media Engagement

1

Avoid creating social media handles that have your full first, middle and last names. If using social media to advance your professional career, consider just revealing your first and last name and not revealing your middle or other surnames.

---

2

Social media platforms all have privacy settings. These settings give you the power to choose who can see your profile, who can message you, who can tag you and how much information is shared from social media publicly. Each platform is different and privacy settings can change frequently. Consider privacy settings as a regular maintenance task that needs to be checked on at least once a year. Visit the specific social media sites for the most up to date information.

---

3

10

All social media platforms have the ability to block users from accessing your social media content or being able to direct message you. If someone

