



Protecting Yourself from Online Harassment & Doxing

Dear UC Santa Barbara Students,

Our campus has a long history of student and community activism that has facilitated positive change, engaging dialogue, and intellectual development. We encourage our students to continue advocating for social and environmental justice, and to call for dismantling oppressive systems and inequality.

We recognize that to do so requires visibility and vulnerability, and can occasionally make our students visible to non-affiliates of the university who may engage in online harassment or doxing. We have developed this guide to provide our students with strategies and resources to minimize this risk. Please take a few moments to review it, and if you need support, please reach out to the recommended resources.

In Community,

Margaret Klawunn, Ph.D.
Vice Chancellor for Student Affairs



What is Doxing?

Doxing is the violent Internet-based practice of researching and broadcasting private or identifiable information about an individual or organization in order to harass and traumatize activists. Additionally, such attacks can also be accompanied by real world violence and spread disinformation about an individual and/or a movement.

The following practices will help prevent doxing, protect you if it occurs, and facilitate your resilience.

Protecting Yourself

Change Your Privacy Settings on Your Social Networks

Set your accounts, including Facebook, Twitter, Instagram, and Snapchat to Private. For guidance on protecting your social media and security, visit security.ucsb.edu/students/social-media-and-security

Turn on 2-Factor Authentication (2FA) for All Accounts

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. 2FA is available for UCSB Connect, Gmail, Facebook, Twitter, Amazon, and more.

You can find tutorials for all 2FA instructions for most of your accounts at <https://www.turnon2fa/tutorials> and at <https://twofactorauth.org>

Find out what Information People Can Find About You

Search for your name using DuckDuckGo (an Internet search engine that emphasizes protecting searchers' privacy). This will give you a sense of how much data exists about you online to people who are not in your network. You can then develop a plan to have this information removed or locked down.

Searching for your information using DuckDuckGo will ensure that you do not increase traffic to websites which engage in doxing, thereby reducing risk of visibility.

If You Are Being Doxed

Immediately Contact the Dean of Students Office

In addition to the recommendations below, please immediately notify our Dean of Students if you are being doxed. Email Assistant Vice Chancellor / Dean of Students Katya Armistead at katya@ucsb.edu

Our Dean of Students can connect you with Associated Students Legal Services to issue Cease & Desist Letters, coordinate with campus security, contact faculty regarding course accommodations, and arrange for any necessary letters for students entering the job market.

Protect your Social Media

Follow each platform's guidance to increase digital security and prevent online harassment. The Additional Resources on the following page of this guide provide some helpful recommendations.

Change Your Existing Passwords

It is recommended that you change passwords to a pass phrase whenever possible. Length of the pass phrase is the primary indicator of strength. How to pick a strong pass phrase:

1. Pick a sentence that is easy for you to remember, but is unique and not easily guessed
2. Capitalize two or more words/letters in the sentence
3. Include two or more numbers or special characters such as: !@#\$%^&*
4. Place punctuation or numbers where they do not belong

For example, "I love ucsb" could be made much stronger by changing it to "I.lo.ve.UCSB!"

For additional guidance, visit security.ucsb.edu/news/password-best-practices

Create a Self-Care Plan

Recruit family, friends, and community members to support you. Let them know what is going on, as doxing can be traumatic, and you must prioritize your mental and physical health. Each person's self-care plan will look different, but it can involve asking a friend to review emails, respond to and block messages, etc.

Create an Incident Log

This will help establish patterns of attack and can be useful to compare with other organizers and legal services to identify larger patterns to identify attackers and their organizations. Record the date, time, location, description of the incident, and result/impact.

Campus Resources

Our Dean of Students Office will connect you and help you navigate campus resources. However, please recognize that being doxed can be a traumatic experience. Prioritize your mental health, self-care, and wellness. Please give yourself permission to move on and ask for help if things become too difficult. In an emergency, please call 911.

Dean of Students Office

<http://studentlife.sa.ucsb.edu/departments/dean-of-students>

(805) 893-4569

katya@ucsb.edu

Counseling and Psychological Services (CAPS)

<http://caps.sa.ucsb.edu/>

(805) 893-4411

UCSB Police Department

Non-Emergency: (805) 893-3446

CSO Escort: (805) 893-2000

Additional Resources

[Wired.com/2017/12/digital-security-guide/](http://wired.com/2017/12/digital-security-guide/)

A helpful and comprehensive guide to digital security

iHeartMob.org/About

HeartMob is a community working to help end online harassment

Cybersmile.org

A multi-award winning anti-cyberbullying nonprofit organization. Committed to tackling all forms of digital abuse, harassment and bullying online