



STEP 1: ASSESS THE THREAT LEVEL

Is the doxxing exposing personal contact information (e.g., phone number, home address, workplace, family details)?

- ▶ **Yes** → Go to Step 2
- ▶ **No**, only basic or public information → Monitor the situation and increase privacy settings

Is there a direct threat to your safety (e.g., threats of harm or stalking)?

- ▶ **Yes** → Call either UPD or local law enforcement immediately, dial or text 9-1-1 in San Diego and Imperial counties (→ Step 2)
- ▶ **No** → Go to Step 3



STEP 2: FOR YOUR IMMEDIATE SAFETY

If you feel unsafe at home or on campus:

- ▶ Contact the University Police Department and/or local law enforcement
- ▶ Inform trusted colleagues, friends and family
- ▶ Consider relocating temporarily if needed for personal safety
- ▶ Request a campus escort if needed
- ▶ Preserve evidence (e.g., screenshots, messages, emails), which you may need to share with law enforcement as evidence
- ▶ Report the incident as you are able and as appropriate
- ▶ Never send any form of payment to remove doxxed content (Paying ransom only encourages further extortion)



STEP 3: REPORT THE INCIDENT

Who to Notify?

- ▶ The *University Police Department* can aid if there is a threat of harm.
- ▶ The Information Technology Division can help secure your university email account and address web content pertaining to you.

- ▶ The Center for Human Resources (for faculty and staff) and the Division for Student Affairs and Campus Diversity (for students) can offer additional support related to workplace and course accommodations. Additional *university support resources*, including counseling, are available to students, faculty and staff.

Strategic Communications and Public Affairs (StratComm) can assist with media inquiries should reporters reach out to you. In the event that you begin receiving media inquiries, we recommend forwarding the inquiry to a member of the *media relations team*.

- ▶ The *Title IX* team can assist and answer questions if harassment is tied to discrimination.
- ▶ Social media platforms and websites external to SDSU generally provide portals to file reports and request content removal



STEP 4: TAKE ONLINE PROTECTIVE MEASURES

Consider the following actions:

- ▶ Remove your public information and contact information from your social media accounts and websites
- ▶ Request takedowns from social media platforms and web hosts
- ▶ Change passwords for email, banking and social media
- ▶ Enable multi-factor authentication (MFA)
- ▶ Make social media accounts private
- ▶ Restrict who can tag or mention you online via your social media channels



STEP 5: SEEK SUPPORT

- ▶ For mental health and well-being, contact university *support services teams*, to include counseling services offered to students and employees
- ▶ For faculty and staff, speak with your director supervisor, dean, associate dean and/or designated human resources lead
- ▶ Connect with trusted family, friends, colleagues, supervisors and others
- ▶ Limit your social media usage for a period of time that is comfortable to you

sdsu.edu/onlineharassmentguide