

Doxxing

Quick Reference Guide for Threats to Personal Information and Safety



WHAT IT IS

The public release of your private information (home address, phone, family details) to harass, intimidate, or threaten you.

WHAT TO DO

Step Zero: Are you in immediate physical danger, or has a threat been made against you or your family?

YES



Call 911 immediately

After the current danger is addressed, continue below.

NO

1 DO NOT

- Delete the post, message, or account; it's evidence
- Reply, comment, or confront the person who posted it
- Assume it will resolve on its own

2 DOCUMENT

- Screenshot the post, date/time stamp, username, and web address
- Save DMs and emails; don't delete originals
- Note when you first saw it

3 NOTIFY

- Your supervisor or election director
- Your office's designated safety/security contact

4 REPORT

- File a report with local law enforcement (non-emergency line unless Step 0 applied)
- Report the content to the platform it appeared on

5 SECURE

- Consider changing passwords on email, social media, and work accounts
- Turn on multi-factor authentication (MFA) if it is not already enabled

6 MONITOR

- Check weekly for reposts or new mentions
- Log any new incidents (date / what happened / action taken)

Key Contacts & Resources

JURISDICTION:

ROLE	NAME	PHONE	NOTES
Your Supervisor			
Office Security Contact			
Local Law Enforcement Non-Emergency			
State Election Security Contact			
FBI Local Field Office			
Other:			
Other:			

JURISDICTION NOTES & LOCAL PROTOCOL

ADDITIONAL RESOURCES:

- Full Doxxing Incident Response Guide
- Digital Footprint Self-Assessment
- Platform reporting tools (Facebook, Instagram, X, Reddit, Discord)
- Data broker opt-out guidance (people-search site removal)

Access these
resources
and more:

