Doxxing: Tips to Protect Your Privacy

**Doxxing**: The malicious release of someone’s private or personally identifiable information, generally or to specific individuals, in an attempt to threaten, embarrass, coerce, or hurt the victim.

01 **Find out what’s public.**

Search for yourself (images, text, and comment searches) on major search engines and social media platforms.

- Note any place where publicly available information could lead someone to private information.

02 **Review site security.**

Set a strong password (with two-factor authentication where possible) for all sites and social media accounts.

- Revoke unauthorized login sessions or applications linked to your account.

03 **Separate your personal and public profiles.**

Don’t create *usernames* based on personally identifiable information, like your name, ethnicity, age, religion, gender, or sexual orientation.

- If you provide *contact information* to parents or students, register a separate phone number via services like Signal or *Google Voice*. Don’t use personal accounts for professional use or vice versa.

04 **Think before you type.**

Comments collected over time can provide enough personal information to identify you.

- Where possible, limit who can see your online comments and set social media sites to auto-delete your comment history.

05 **Teach students digital citizenship.**

A recent *EdWeek Research Center survey* found more teachers reported being threatened or doxxed by students or parents than other community members or strangers.

- Talk to your students about protecting their own and respecting others’ privacy online.

- Ensure students understand the consequences of revealing private information without consent.

**Document.** Keep any emails, texts, social media posts, *screenshots*, or other communications you receive on threats to release your private information. Note any patterns you see.

**Assess the threat.** Use a safety checklist like this one from PEN America to think through whether the doxxing threat is real and could lead to a safety problem.

**Inform those who need to know.** If you know your harasser is a student, parent, colleague, or otherwise related to the school community, alert your principal or supervisor, human resources, technology director, and union staff if available. If the doxxing is accompanied by threats or other harassment, you may also need to contact a lawyer or police.

**Find support.** Privacy invasions can cause stress, anxiety, and depression. Reach out to colleagues, friends, family, and mental health professionals for support.

**Monitor data breaches** via sites like *Haveibeenpwned.com*; follow up to change your password, lock down your account, etc. if you are listed in a breach.

---

**What to do if you’ve been threatened with doxxing?**

**Sources:** PEN America’s *Online Harassment Field Manual*, Citizen Lab, Privacy Rights Clearing House, World Privacy Forum, Future of Privacy Forum, Electronic Frontier Foundation, and *Education Week* reporting.

---

**SOURCES:** PEN America’s *Online Harassment Field Manual*, Citizen Lab, Privacy Rights Clearing House, World Privacy Forum, Future of Privacy Forum, Electronic Frontier Foundation, and *Education Week* reporting.