Responding to and Preventing Doxing: A TSPA Resource

If you've been doxed, please skip to [Respond to Doxing Right Now](#).

This resource was prepared by TSPA community members, including advisors and staff. It was last updated December 15, 2022.

Introduction

Doxing (or doxxing) is when someone—a *doxer*—obtains private or personal identifying information about another person—a *target*—and then widely distributes it without the target's consent with the intent to do harm. Doxing intends to strike fear to silence or chill others' speech or actions. Doxing incites harassment, physical threats, stalking, and dangerous forms of intimidation, both online and offline. On a technical level, doxing is easy. A doxer can collect the digital breadcrumbs left behind from online activities to reveal the target's (or their loved ones') real names, email addresses, physical addresses, and locations.

Due to the nature of trust and safety work, T&S professionals face an increased risk of harassment, stalking, and other forms of online and/or physical harm if their personal or private identifying information[1] is exposed to the public. The community at TSPA developed this guide as a resource for T&S professionals, but we are releasing a public version for anyone who might find it helpful.

Recommendations

We've crowdsourced a list of actions you can take now and resources you can use to build your resilience.

Respond to Doxing Right Now

Step 1: Secure Your Physical Safety

First, ensure you are physically safe. Move to a safer location if needed, and reach out to someone you trust to let them know what's happened. Review your location sharing and tracking settings on all of your devices. Turn off all location sharing that isn't necessary.

Step 2: Collect Evidence

As difficult as it may be, document what's happened. Take screenshots of posts and messages before you delete them; consider asking a friend or trusted colleague to help you. Record what's happened chronologically. Duplicate and store all evidence in a safe place; make physical copies too.

[1] This may include information like real names if someone is typically pseudonymous or anonymous, personal phone numbers, email or physical addresses.

Step 3: Report Doxing and Harassment

If you've been doxed on a social media platform, report it as soon as possible. If you've received threats indicating you're not physically safe, report these threats to local law enforcement if you can. (They may not know how to handle doxing, but having an official record helps.) You may also want to tell your managers, peers, and loved ones so that they can help support and protect you.

Step 4: Retreat and Practice Self-Care

After you've secured your physical safely, collected evidence, and reported doxing, block or mute applicable accounts. Give yourself permission to step away from digital devices, get extra sleep, seek support, and practice self-compassion.

Proactively Protect Yourself (and Your Loved Ones)

Dox Yourself

Search for yourself online using a variety of browsers and search engines so that you know what kind of information can be found. Remember to search using variations of your name, your email addresses, and your social media handles. You may also consider doing a reverse image search.

Remove Your Data

If you find your personal information listed on data broker sites like Spokeo and Whitepages, you can ask them to remove your information. You can make these requests yourself, or you can pay for a scrubbing service (see Resources). You can also ask Google to remove personal information from search results. If you're registered to vote in the United Kingdom, you can request the removal of your information from the open electoral register.

Stop Sharing

Separate the personal and professional. Work information (and related data) should remain on work devices; personal information (and related data) should be restricted to personal devices you control. Your first priority should be to build and maintain a wall between your work life and personal life to minimize your exposure to attacks. This includes:

- Not logging into personal social media accounts, emails, Chrome profiles, apps, iCloud accounts, etc. on your work devices.
- Setting all of your personal social media accounts to "private."

- Using a unique photo—one that cannot be connected to your personal social accounts—for your LinkedIn profile.
- Not listing your location on your professional/public accounts (i.e., LinkedIn profile), especially if you live in a small town.

Secure your accounts. Use multi-factor authentication and unique, strong passwords for all accounts.

Optimize your privacy settings. Each online service has different options for privacy settings. As much as possible, set your accounts to private or "friends-only," remove any identifying information about yourself and your location (e.g., street signs in pictures), and turn off location tracking. If you have websites with domains registered under your name, check that your WHOIS information is concealed.

Use a VPN when visiting untrustworthy sites. Internet Protocol (IP) logging tools can uncover your physical location. When visiting sites likely to be hacked or independent websites that you don't trust, hide your IP address by using a Virtual Private Network (VPN). VPNs can provide a more secure, private, and encrypted internet connection so that bad actors can't view your real IP address. There are various types of VPNs available; use this guide to select one that fits your needs. (Security experts commonly recommend Mullvad, IVPN, and Mozilla VPN.)

Remove hidden data from your files. If you post documents, photos, or videos online, be aware that metadata embedded in files can be used to identify you. Various tools exist to help you control the amount of information you share through metadata; do your research and find one that suits your needs. If you share photos or videos taken with your mobile device, learn about Exchangeable Image File Format (Exif) data and how to scrub it from your files.

Protect your loved ones. Doxers often include the loved ones of high profile targets. Share these resources with your friends and family and have conversations about what's okay to post about one another online. Encourage your loved ones to limit access to the information that doxers may be able to find about them and about you.

Proactively Protect Your Colleagues

Protect Your Team

If you're a manager, you have a responsibility to protect your team members. Discuss preventative measures with your team and provide training and workshops as needed. Instruct

team members to use pseudonyms for user-facing communications and consider obscuring employee names in internal tools and communications. You may also want to have conversations with leadership regarding your organization's ethical and legal responsibilities when employees are doxed due to their roles.

Advocate for Consequences to Doxing

If you work for a social media platform or are involved in an online community, advocate for community guidelines that explicitly prohibit doxing and are clear about the consequences. For example, Patreon has taken a strong stance against doxing regardless of who the target is.

Create a Plan

Draw inspiration from The Front Line Defenders Workbook on Security and develop a security plan for your team or organization. Host a hands-on security training workshop with security experts or schedule sessions to provide time and guidance for employees to follow steps recommended by the security resources below. Openly discuss your risks and vulnerabilities as individuals and as a collective. Determine and agree on the steps you'll take if doxing occurs. Consider designating primary and secondary points of contact who are responsible for ensuring that employees targeted by doxing receive formal support.

Resources

- PEN America Online Harassment Field Manual
- Electronic Frontier Foundation Tools
- The Front Line Defenders Workbook on Security
- Consumer Reports Security Planner
- HeartMob
- Online SOS

Appendix

Doxing is not a crime in most jurisdictions, but many actions associated with doxing (e.g., stalking, harassment) can be prosecuted. This is a list of possible legal avenues for targets of doxing. Laws and their application vary widely from jurisdiction to jurisdiction, and may not apply in all cases. Please review your options with qualified legal counsel.

Locations	**Resources**
Canada	Criminal Code (RSC , 1985, c. C-46) - Criminal Harassment
Singapore	The Protection from Harassment (Amendment) Act 2019
United Kingdom	Protection from Harassment Act 1997, Section 1
United States (Federal)	18 U.S.C. § 2261A - Stalking
California, US	California Penal Code section 422 - Criminal Threats California Penal Code section 646.9 - Miscellaneous Crimes California Code of Civil Procedure section 527.6 - Other Provisional Remedies in Civil Actions
Connecticut, US	CT SB00989 | 2021 | An act concerning online harassment
Nevada, US	AB296 - Establishes a civil cause of action for the dissemination of personal identifying information or sensitive information under certain circumstances. (BDR 3-121)
New York, US	SECTION 240.30 Aggravated harassment in the second degree