Doxing

Learn how to manage your browser history and keep your browsing information secure.

1. What Is Doxing?

Doxing is a digital attack and serious form of online harassment where someone publicizes another person's personal and private information online.

A doxing attack obtains and publicizes information from different private documents (hence the name doxing). This information can include:

- Phone numbers
- Addresses
- Social security numbers
- User names
- Financial information
- Private photographs

Doxing is an act of aggression and is frequently done to seek revenge. This can be due to a personal dispute or because someone gets angry at something another person posted online. Women, LGBTQIA individuals, and people of color online are also often doxed for misogynistic, homophobic, or racist motivations.

Doxing can have serious effects and repercussions for victims. It can:

- Lead to an increase in harassment, cyberbullying, trolling, and cyber stalking
- Be a way to embarrass, intimidate, or silence someone
- Lead to threats of violence
- Lead to real-world consequences including identity theft, causing problems with someone's employer, public shaming, or (rarely) having the police called to someone's home, which is known as swatting.

Remember, if this happens to you, it is not your fault!

2. What Can You Do if You Have Been Doxed?

First, don't try to handle the situation alone:

- Report the incident to sites where your information has been made public and/or where you are experiencing bullying and harassment. For example, Twitter has declared doxing a violation of their terms of service and they have procedures in place for people who have been doxed
- Reach out to a trusted friend or contact for support during this scary situation

Take screenshots:

- Try to document as much as you can about what is happening

Secure your accounts:

- Change passwords
- Set-up multi-factor authentication
- Monitor your accounts for signs of identity theft including odd activity on bank statements, newly created accounts, etc.
- Monitor your accounts for signs of hacks, including odd changes to your social media account, posts you didn't make, etc.
- Be alert of phishing schemes and scams

If you are experiencing threats of physical violence or assault and feel unsafe, contact local law enforcement for help.

Consider going offline for a while. While this can feel like admitting defeat to your harassers, it can also be positive for your mental health, can encourage harassers to lose interest in you, and can give you time to strengthen your digital security. Whether you decide to remain online, go public with what happened, or go offline, your decision is valid.

3. What Are Steps You Can Take to Avoid Being Doxed?

- Limit the amount of personal information you make available online and practice digital minimization
  - It can be difficult to strike a balance between sharing your views online and maintaining your privacy, but there are ways to share your views online while still maintaining your privacy and security!
- Make sure your social media accounts are secure and that you are making use of different account security settings for things like targeted ads and profile information
- Audit your social media post history and remove posts that are oversharing or are revealing too much personal information
- Practice password hygiene by using password managers, multi-factor authentication, and having strong passwords that are long and unique
- Consider using a VPN to conceal your IP address
- Be cautious about what you upload. Word documents and photos often have information included about who created the file or when and where the photo was taken
- Consider pseudonyms or an alternative email for social sites. You might also consider having different user names for sites you use to make it harder to track and trace you across platforms
- Avoid logging into sites with your Facebook or Google account. Create separate accounts to avoid linking all your accounts together. You can also better control what information the site has access to by setting up your own account
- Search for yourself and see what is out there