Personal Safety & Security

Protect Yourself Online – Shield from Doxing

Personal Safety & Security
YOUR SAFETY OUR PRIORITY

The safety and security of Federal employees and those who visit Federal facilities is the Federal Protective Service's mission and top priority. As co-chair of the Government Services and Facilities Sector, FPS promotes security and resilience by sharing information and resources sharing with state, local, tribal, and territorial government personnel, as well as for the essential functions they perform.

WHAT IS DOXING?

Short for "docs" or "dropping docs," doxing is the act of compiling and publishing another individual's personally identifiable information (PII) or an organization's sensitive information online to expose identities, enact revenge, promote stalking, enable identity theft, or encourage others to perpetrate violent or malicious activity against targets or their families.

HOW'S IT DONE?

Doxing occurs when a person collects another's personal information from internet sources, including social media profiles, published data breaches, property and business records, voter registration, judiciary case searches, online newspaper archives, wedding and baby registries, obituaries, business reviews, real estate listings, and more. Most of the information is publicly available, although many victims are not aware of the volume of their personal information that is available online. Most have not taken steps to minimize their online footprints.

FOUR STEPS TO PROTECT YOURSELF ONLINE:

1. **Keep privacy in mind.** Turn on privacy settings on social media, mobile apps, and other websites. Review privacy and location settings to limit what information the public can see. Install applications from app stores, review privacy and data sharing, limit permissions of applications—deny permissions by default. Review "friends" networks and limit connections to those you truly know.
2. **Shield your information**. Create a separate email account for new profiles, retailers, and other services–limit dissemination of your personal email address, telephone number, and online profiles. Remove sensitive information from online profiles. Provide only the minimum information required for online services; for example, a photo framing website doesn't require your date of birth. Enable encryption, updates, and multifactor authentication applications.
3. **Think before you post.** Avoid posting information that may increase your chances of being targeted for doxing: don't post information about your job duties or your physical location; avoid posting information that might be used to answer website security questions, such as your maiden name, the name or location of your high school, or pet's name. Photos taken with your smart device contain embedded metadata that includes where the photo was taken—information available online once you post the photo.
4. **Limit use of third-party applications** on social media to log into other accounts. These third-party applications receive PII from your profile when you use them. Depending on your official position or the terms of service, you can opt out or decline to have this information shared.

TAKE ACTION.

If you suspect you've been victimized by doxing, identify theft, or any cybercrime, you should:

- ✓ **Report** it immediately to law enforcement, such as the FBI's Internet Crime Complaint Center.
- ✓ **Inform** your workplace, family, and friends to increase vigilance.
- ✓ **Document** what occurred by saving the name of the sender/receiver, email exchanges, website addresses, and take screen shots of posts.
- ✓ **Determine** if the information is protective/sensitive and possible sources.
- ✓ **Request to remove** false, abusive, or threatening content—consider submitting a takedown request to the platform or website, in accordance with their rules and requirements.

CONTACT THE FPS MEGACENTER TO REPORT ANY SUSPICIOUS ACTIVITY:

1-877-4FPS-411 (1-877-437-7411)
OR CONTACT YOUR LOCAL AUTHORITIES
****DIAL 911 FOR EMERGENCIES*

Resources for victims of crime: dhs.gov/victims-crime

FEDERAL PROTECTIVE SERVICE
FPS

Connect on social media @FPSDHS
Learn more at DHS.gov/FPS
Scan QR code to visit DHS.gov/Publication/YourSafetyOurPriority