Homeland Security

Department of Homeland Security
Office of Partnership and Engagement (OPE)

Resources for Individuals on the Threat Of Doxing

January 16, 2024

WHAT IS DOXING?

Doxing refers to gathering an individual's personally identifiable information (PII) and releasing it publicly for malicious purposes, such as public humiliation, stalking, identity theft, or targeting for harassment.

EXAMPLES OF SENSITIVE INFORMATION

- **Full Name**
- **Contact Information**
- **Home Address**
- **Family Members**
- **Workplace Details**
- **Financial Information**
- **Social Security Number**

COMMON SOURCES OF SENSITIVE INFORMATION

- **Social Media Posts**
- **Property and Court Records**
- **Wedding Announcements and Obituaries**
- **Newsletters**
- **Public Conferences**
- **Web Forums, Blogs, and Discussion Boards**
- **Unprotected Networks**
- **Voter Registration Lists**

HOW CAN I PROTECT MYSELF FROM DOXING?

- **Be careful** about what you post about yourself online, including photos and videos even if temporary.
- **Remove** PII (address, date of birth, phone number, etc.) from your social media profiles.
- **Review** your followers and reject requests from anyone you do not know.
- **Request** to remove your personal data from public records websites. Well-known websites include BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, and Whitepages.
- **Remove** unnecessary apps and browser extensions to prevent collection of your personal data.
- **Restrict** location tracking on apps and websites. Turn off location services for each app or platform.
- **Turn on** privacy settings on social media, apps, and other websites.
- **Set up** two-step verification, use complex passwords, and do not repeat the same password for multiple accounts.

DHS OPE

HOW CAN I PROTECT MYSELF FROM DOXING?

Request to Remove False, Abusive, or Threatening Content
Consider submitting a takedown request to the platform or website, in accordance with rules and requirements.

Document What Is Happening
Consider taking steps to preserve evidence. Save all emails, voicemails, and text messages you receive, and take screenshots or photos of comments on social media.

Report the Incident
If you have received a threat to your physical safety or feel criminally harassed, report the incident to local law enforcement, as well as the social media platform or website administrator.

ADDITIONAL RESOURCES & GUIDANCE

CISA Cybersecurity Best Practices & Resources: cisa.gov/cybersecurity

CISA Cyber Essentials: cisa.gov/cyber-essentials

CISA Tip: Avoiding Social Engineering and Phishing Attacks: cisa.gov/tips/st04-014

CISA Insights: Enhance Email and Web Security: cisa.gov/publication/enhance-email-and-web-security

CISA Social Media Threat Guidance for School Staff and Authorities Infographic: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

If you are a victim of online crime, file a complaint **with the FBI's Internet Crime Complaint Center (IC3)** at ic3.gov