The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

HOW TO PREVENT ONLINE HARASSMENT FROM "DOXXING"

What is Doxxing?
Doxxing refers to gathering an individual's Personally Identifiable Information (PII) and disclosing or posting it publicly, usually for malicious purposes such as public humiliation, stalking, identity theft, or targeting an individual for harassment.

How Can Doxxing Impact You?
Doxxers may target government employees for such purposes as identifying law enforcement or security personnel, demonstrating their hacking capabilities, or attempting to embarrass the government.

HOW IS IT DONE?

Hacking, Social Engineering, or Other Malicious Cyber Activities

Doxxers may use hacking, social engineering, or other malicious cyber activities to access personal information. One common practice is **getting access to a victim's email account**. A doxxer could use social engineering to get your password by posing as a representative from the IT helpdesk or your Internet Service Provider.

- Once a doxxer has access to your email account, he or she will attempt to **obtain more personal information from your account or break into other web-based accounts** (e.g., social media, online storage, and financial records) by using email-based password resets or harvesting your information in order to answer website security questions. The doxxer may also attempt to use the same email address and password combination on other sites to gain access to additional accounts.
- **A doxxer could use your DHS username and password to attempt to access the DHS network.**

Collecting Publicly Available Information

Doxxers may collect information about you from Internet sources, such as property records, social media postings, obituaries, wedding announcements, newsletters, public conferences, and web forums.

- Most, if not all, of this information is publicly available. The doxxer compiles information from multiple public-facing sources to reveal sensitive information about the victim, such as the victim's home address, family members, photos, workplace, and information about the individual's habits, hobbies, or interests.
- In this "mosaic effect," **the seemingly innocuous information we post or share can be put together to develop a detailed dossier about us**.

Purchasing Information from Data Brokers

Doxxers may also use "data brokers" or people-search sites that compile information from public and commercial sources and then sell this information to companies or the public. These **brokers may obtain commercial data from retailers, catalog companies, magazines, and websites (e.g., news, travel).**

STEPS TO MITIGATE DOXXING

Limit What You Share Online

- **Be careful about what you choose to share online.** Some of the publicly available information (e.g., public records) may be out of your control, but remember that anything you post on the Internet might be misused, including photos. Once it's online, you cannot take it back.
- **Avoid posting information that may increase your chances of being targeted for doxxing.** Not all information has the same sensitivity level. For example, don't post information about your job on social media, especially sensitive details about your job duties or your physical location.
  - Avoid posting information that might be used to answer website security questions, such as your pet's name or where you were born.
- **Turn on privacy settings** on social media, mobile applications, and other websites, and be careful about the connections or friends you may have on these sites.
- **Limit your use of third-party applications** on social media and the use of social media accounts to log into other websites. These third-party applications receive PII from your profile when you use them.
- **Consider removing yourself from data brokers.** Unfortunately, this can be a time-consuming process, and your information may re-appear when data brokers receive new or updated data sources, so everyone must weigh the potential benefit against the effort required.

Stay Secure

- **Practice good cyber hygiene.** Set up two-step verification, use complex passwords, and avoid using the same password for multiple accounts to help prevent the hacking or hijacking of your accounts.

Act Fast

- **If you receive a suspicious email on your DHS account, forward it to DHSSPAM@hq.dhs.gov.**
- If doxxers publish your information on social media, report it immediately and ask that it be taken down.
- Document threats you receive, and if you think you're in danger, call the police. If you believe you are the victim of identity theft, file a report with your local police office. Even if they do nothing, it's good to get a report on file. Ask to speak with an officer who specializes in online crimes.

FOR MORE INFORMATION

- The Office of the Chief Security Officer also has a Social Media Safety page with a helpful booklet and many other resources.
- FBI's Public Service Announcement on doxxing.
- US-CERT cyber tip sheets.
- FTC video on Sharing Information: A Day in Your Life and FTC tips on protecting personal information.
- DHS's Stop. Think. Connect.™