# How to Mitigate Doxxing

ELECTION OFFICIAL RISK MANAGEMENT SERIES

ELECTION SECURITY Exchange

## What is Doxxing and How Does it Happen?

Doxxing is the deliberate public release or amplification of an individual's personal information – such as a home address, phone number, or family details – without consent, typically to harass, intimidate, or threaten.

For election officials, doxxing can increase the risk of harassment, coordinated abuse, swatting or false emergency reports, targeting of family members, and escalation to physical security concerns.

Most doxxing incidents rely on information that is already publicly accessible. Common sources include social media posts and photos, public records (property, voter, court), professional biographies and media interviews, data broker websites, and compromised or reused passwords. In many cases, small pieces of information from multiple sources are aggregated to create a detailed profile and amplify targeting.

## How to Reduce Your Risk

### *Minimize Your Digital Footprint*

- Review and restrict privacy settings on all social media accounts.
- Remove home addresses, personal phone numbers, and family details from public profiles and bios.
- Avoid posting real-time location, travel, or family information.
- Search your name on people-search and data broker websites and request removal where possible. Consider using a reputable data removal service if needed (DeleteMe, Hush, Incogni).
- Be cautious with photos that reveal identifiable landmarks, school names, license plates, or home details.

### *Control Public Records & Contact Information:*

- Avoid listing personal contact information in public-facing materials.
- Limit use of personal email or phone numbers in professional settings.

- Understand what voter, property, or court records are publicly accessible in your jurisdiction.
- Use an office address or P.O. box for public filings when permitted.

### *Strengthen Account Security*

- Separate personal and professional accounts.
- Use strong, unique passwords (consider a password manager).
- Enable multi-factor authentication, especially on email and social media.
- Remove personal phone numbers from account recovery settings when possible.
- Use a VPN when working remotely or on public wifi.
- Keep devices and software updated.

### *Plan Ahead*

- Establish internal reporting protocols for harassment or digital exposure.
- Identify a designated point of contact for digital safety concerns.
- Set up alerts for your name and office to monitor potential exposure.
- Conduct periodic digital footprint reviews for staff in high-visibility staff.
- Coordinate mitigation and response protocols across your office or jurisdiction.

## Other Resources

- **Digital Exposure and Doxxing: How to Stay Off the Radar training**. If you are interested in scheduling this training for your organization, email info@securingelections.org
- Digital Footprint Self-Assessment
- Doxxing Incident Response Guide for Elections