Digital Security & Anti-Doxxing Guide

Stay safe online by taking proactive steps to protect your personal information, minimize exposure, and respond effectively if targeted.

Protect Personal Information

- **Assume everything online is public.**
  Even private messages can be leaked or screenshotted.

- **Separate personal and activism identities.**
  Use different accounts, emails, and devices when possible.

- **Know your rights.**
  While doxing isn't illegal in Canada, it can be prosecuted under harassment, threats, privacy, and cybercrime laws.

Remove Existing Data

1. Scan for Exposure

- Mozilla Monitor
- Have I Been Pwned
- DeHashed

2. Opt-Out of Data Brokers

- Request removal from sites like **Spokeo** or **411.ca**.

3. Delete Old Accounts

- Use tools like Cloaked or JustDeleteMe.

- Manually search your name, username, and email for forgotten profiles.
- Review saved logins and connected apps, then delete through account settings.

Limit New Exposure

- **Use pseudonyms** on forums, petitions, and social media.
- **Create separate emails** (consider ProtonMail) for activism or risky sign-ups.
- **Avoid personal details:**
  Don't post locations, workplaces, or family info — and don't share in real time.
- **Mask website domains** with tools like Njalla.
- **Register businesses** with a business address — not your home.
- **Use a VPN** to hide IP and location.
- **Choose privacy-focused browsers** (Firefox, Brave) with tracking protection.

Secure Online Accounts

- **Password Manager:** KeePassXC or Bitwarden.
- **Enable 2FA:** Prefer hardware keys (Yubikey) or authenticator apps (Aegis/Authy) over SMS.
- **Separate Emails:**
    - Personal (trusted contacts)
    - Activism (public-facing)
    - Social media accounts

    - Burners (high-risk sign-ups)

Social Media Safety

- Lock privacy settings — set profiles to private, limit past posts.
- Disable “search by phone/email” on Facebook, Twitter, LinkedIn.
- Ask friends/family to remove or untag photos of you.
- Avoid linking personal and activism accounts.
- Strip EXIF data from photos using ExifTool.
- Regularly clear old posts, comments, and unnecessary data.

Phishing & Social Engineering

- **Verify requests** (via Signal or in person) before sharing info.
- Watch for fake friends or allies who try to extract details.
- Avoid “free” tools that log data — use CryptPad instead of Google Docs for sensitive files.

AI-Assisted Doxing Risks

- Facial recognition can match your photos — wear masks, cover tattoos, and avoid unique identifiers in public photos.
- Always use a VPN and avoid clicking unknown links.
- Avoid storing sensitive data in Google Drive; use CryptPad or another encrypted tool.

If You're Doxed or Targeted

1. **Document everything:** screenshots, URLs, archive links (Archive.today).
2. **File a "Notice and Notice"** request for unauthorized use of photos (Canada).
3. **Report to platforms:** Twitter, Facebook, etc.
4. **Contact a lawyer** or digital rights group.
5. **Request takedowns** from websites/social media.
6. **Lock down accounts:** change passwords, enable 2FA.

Recommended Guides

- CIPPIC (Canadian Internet Policy & Public Interest Clinic)
- EFF's Surveillance Self-Defense (Canada Section)
- Access Now's Self-Doxing Guide