PHYSICAL SECURITY CYBERSECURITY OPERATIONS

Digital Footprint Self Assessment Worksheet

ELECTION OFFICIAL RISK MANAGEMENT SERIES

ELECTION SECURITY *Exchange*

Purpose

This worksheet guides you in understanding what personal information about you is publicly available online. The goal isn't to disappear from the internet. Instead, you'll identify your highest-risk exposures so you can prioritize what to secure or remove.

If you feel unsafe or threatened, call 911 immediately.

STEP 1: Search Engine Basics

Start by searching for yourself using multiple search engines (Google, Bing, DuckDuckGo).

What to search for:

- □ **Your full name** (exactly as you use it professionally)
- □ **Name + city and stat**e (e.g., "Jane Smith Milwaukee Wisconsin")
- □ **Name variations** (maiden name, nicknames, middle name variations)
- □ **Phone number(s)** (current and old numbers)
- □ **Email address(es)** (work, personal, old accounts)
- □ **Old usernames** (from forums, gaming, hobbies, past jobs)

What to look for:

- **First page results –** What shows up? News articles, social media, professional profiles?
- **Images tab –** Are there photos of you, your home, your car or family members?
- **Map results –** Does your home or workplace appear with identifying information?
- **AI-generated summaries –** Check "AI Overview" or similar features that may pull surprising or outdated information
- **"People Also Searched For" –** Does this reveal connections to family, colleagues or employers?

Notes/Findings:

What surprised you? What information seems most sensitive?

Step 2: Social Media Review

Review your social media accounts as if you were a stranger trying to learn about you.

For each platform (Facebook, Instagram, X/Twitter, LinkedIn, TikTok, etc.):

PROFILE INFORMATION

- Is your profile public or private?
- What information is visible? (Birthday, hometown, workplace, education, relationship status)
- Do profile or cover photos reveal location clues? (Street signs, landmarks, house numbers)

POSTS AND CONTENT

- Are old posts visible to the public?
- Do posts include dates, locations, or event check-ins?
- Are there photos with metadata/location tags still attached?
- Do posts reveal routines, schedules, or travel plans?

CONNECTIONS

- Is your friends/followers list public?
- Are family members or coworkers tagged in your posts or theirs?
- Have others posted about you publicly (tagged photos, comments, mentions)?

PRIVACY SETTINGS

- Review who can see your posts (Public, Friends, Custom)
- Who can look you up by phone number or email?
- Who can send you friend requests or messages?
- Are old posts from years ago still public?

Notes/Findings:

Which platform reveals the most? What needs to be locked down first?

Step 3: People-Search Sites and Data Aggregators

These sites collect and package public records, making it easy for anyone to find your contact info, relatives' names, past addresses, and more.

Sites to check:

- □ Whitepages.com
- □ Spokeo.com
- □ TruePeopleSearch.com
- □ FastPeopleSearch.com
- □ BeenVerified.com
- □ Intelius.com
- □ MyLife.com
- □ PeopleFinders.com

Important: Don't click on suspicious ads or unfamiliar "people finder" sites. Stick to known aggregators.

What to look for:

- Current and past addresses
- Phone numbers
- Email addresses
- Relatives' names and ages
- Property records or photos of your home
- Possible associates or neighbors

Notes/Findings:

Which sites have the most information? Note which ones to opt-out from first.

Step 4: Check for Data Breaches

Find out if your email addresses or passwords have been exposed in data breaches.

Sites to check:

- □ **HaveIBeenPwned.com —** Enter each email address you've used
- □ **DeHashed.com —** Search for breached passwords and usernames
- □ **Firefox Monitor (monitor.firefox.com) —** Another breach-checking tool

What to do if you find a breach:

- Change passwords immediately for any compromised accounts
- Enable two-factor authentication (2FA) wherever possible
- Consider using a password manager to create unique passwords for each account

Notes/Findings:

List any breached accounts and mark whether you've updated passwords.

Step 5: Review Family Members and Close Associates

Your digital safety can be compromised through people connected to you.

- Search for your spouse/partner's name + your city
- Search for children's names (if applicable)
- Check if family members' or close friends' social media accounts mention you, your workplace, or your routine

Considerations:

- Are family members' profiles public?
- Do they post photos of your home, car, or neighborhood?
- Have they mentioned your workplace or schedule online?
- ***If you find sensitive information about coworkers, consider letting them know so they can protect themselves too.***

Notes/Findings:

Step 6: Offline Exposure Review

Don't forget the physical clues that can be photographed and used to identify or locate you.

Your Vehicle

- **License plate –** Is it visible in any online photos?
- **Bumper stickers –** Do they reveal political affiliations, schools, organizations, or hobbies?
- **Parking permits or hang tags –** Do these identify where you work or live?

Your Home

- **Street-visible house numbers –** Can these be seen in Google Street View or social media photos?
- **Mailbox –** Does it have your name visible from the street?
- **Security signs or cameras –** Could these inadvertently identify your location?
- **Neighborhood identifiers –** Are there signs, landmarks, or distinctive features visible?

Notes/Findings:

Step 7: Identify High-Risk Platforms and Exposures

Review everything you've found and answer these questions:

Which accounts or exposures are the highest risk?

Consider which ones reveal the most sensitive information or are easiest for someone to access.

1 ______________________________

2 ______________________________

3 ______________________________

What specific information is most concerning?

Examples: home address, children's school, daily routine, workplace location

Step 8: Create Your Action Plan

Now that you understand your online presence, take these steps to manage and respond to it:

Immediate Actions (Do This Week)

- Remove or make private the highest-risk social media posts
- Update privacy settings on social media accounts
- Change passwords for any breached accounts
- Enable two-factor authentication on critical accounts
- ______________________________
- ______________________________

Short-Term Actions (Do This Month)

- Submit opt-out requests to people-search sites (start with those showing the most info)
- Review and adjust Google privacy settings (myaccount.google.com)
- Ask family members to review their own digital footprints
- Remove location metadata from old photos if possible
- Sign up for a data protection service
- ______________________________
- ______________________________

Ongoing Practices

- Google yourself monthly to monitor what's newly visible
- Set up Google Alerts for your name to catch new mentions
- Think before posting: does this reveal too much about location or routine?
- Regularly review privacy settings as platforms change their policies
- ______________________________
- ______________________________

Resources for Opt-Out and Removal

People-Search Site Opt-Out Guides:

- Many sites have opt-out forms, but they can be hard to find
- Search "[site name] opt out" for specific instructions
- Be prepared to verify your identity during opt-out requests
- Note: Information may reappear after 6-12 months and require re-submission

Additional Privacy Tools:

- **Hush.io or DeleteMe –** Paid services that handle opt-outs for you
- **Google's "Results About You" –** Request removal of personal contact info from Google Search
- **Blur Street View Imagery -** Request your house be blurred in street view on Google Maps
- **Two-factor authentication apps –** Google Authenticator, Authy, Microsoft Authenticator

Final Reminders

- **You don't need to disappear from the internet.** The goal is to reduce your exposure and make it harder for someone to build a detailed picture of your life.
- **Digital safety is ongoing.** Information can reappear, platforms change, and new exposures emerge. Make this review a regular habit.
- **Share what you've learned.** If you find concerning information about coworkers or staff, let them know. Digital safety is a team effort.

Questions or concerns? Bring them to your supervisor or designated security contact.

Other Resources

Digital Exposure and Doxxing: How to Stay Off the Radar training: If interested in scheduling this training for your organization, email info@securingelections.org to make that request.

- **Doxxing Incident Response Guide for Elections**
- **How to Mitigate Doxxing**

This worksheet is part of comprehensive security training for the election community. Keep this document in a safe place for future reference.