Digital Political Engagement: Risks and Best Practices

Civic Forge Solutions LLC

May 9, 2025

civicforge.solutions

Disclaimers

- This presentation is designed to raise awareness and share best practices on information security for activists and organizations engaged in Constitutionally protected, non-violent political activity.

- **Civic Forge Solutions LLC provides this information for guidance and informational purposes. We are not attorneys, and this presentation is not legal advice. This document reflects information available as of May 9, 2025.**

- **Content is provided "as is" without warranties of any kind. Readers should consult qualified legal professionals for situation-specific advice. CFS disclaims all representations and warranties and assume no liability for consequences arising from the use or misuse of this information. This disclaimer may be updated without notice.**

Objectives

- Accurately assess their personal information security risks associated with various forms of digital political engagement.
- Understand the diverse digital threats and vulnerabilities commonly faced by individuals participating in online political activities.
- Select and implement appropriate risk mitigation measures, ranging from foundational practices to more intensive strategies, tailored to their specific circumstances and risk levels

Key Messages

- Any political activity, digital or otherwise, incurs some level of personal risk. However, collective abstention from political activity can result in broader societal consequences.

- You can take steps to mitigate your personal risk related to digital political activity. Many of these steps have little to no financial cost.

- ”What goes on the internet stays on the internet”: Make informed decisions about what you post to public forums or social media. Permanent and confirmed deletion of posts is effectively impossible.

Personal Risks

- **Reputational:** Your online political activity could be evaluated by employers, friends, organizations, or governmental authorities, potentially impacting employment, services, benefits, or social standing.

- **Financial:** Costs may be incurred for risk mitigation measures, or for repairing/replacing personal devices compromised due to online activities.

- **Physical**: Your digital political activities can translate into tangible physical risks, ranging from unauthorized access to or seizure of your devices to direct threats to your personal safety.

Evaluating Your Personal Risk

- Immigration/Nationalization/Citizenship Status
- Federal Government Employee or Contractor
- Private Sector Employer's Politics
- Future International Travel
- Current/Future Interactions with the Federal Government (grants, requests, complaints)
- Affiliation or Member of a Community, Neighborhood, or Organization retaliating for political action or beliefs
- Family or friends in one of the above categories

Attack Vectors: Your Digital Vulnerabilities

Phishing, malware, spyware: Installing software on your personal devices for spying, exfiltrating data, harm to your device, extortion, blackmail, or other purposes.

Correlating digital activity: Matching digital activity (social media, email, phone calls) and public surveillance (CCTV) with other personal identity attributes.

Man-in-the-Middle (MitM): Intercepting mobile phone data/connections and internet connections.

Physical Security: Confiscation of personal devices.

Top 5 Best Practices

- **Use a password manager**. Do not store your passwords in Google Docs or unsecured documents on your computing devices. Do not reuse passwords across services.
- Utilize **Two-Factor Authentication** for all online services. Biometric and physical security keys are best. One-Time password is OK, and SMS should be avoided.
- **Keep your personal and desktop devices updated** with the latest security updates.
- **Use communication tools with adequate encryption** for political communications and activities.
- **Be aware of phishing emails and text message risks.**

Social Media Considerations

- Assume everything you do on social media, including DMs, can be seen by others unless you actively protect yourself; details like your location and internet use are also often tracked.
- For resourceful groups, it's easy to connect your activities across different social media sites back to your real identity.
- Successfully hiding your social media activity requires constant care, can cost money (like for VPNs), and even small mistakes can expose you.

Choosing Risk Mitigation Measures

- **Your Role & Visibility:** Are you a private citizen, an organizer, or a public figure?
- **Activity Sensitivity:** What is the nature of your political engagement (e.g., general discussion, organizing on sensitive topics, high-stakes activism)?
- **Potential Adversaries & Capabilities:** Who might be interested in your activities (e.g., online trolls, organized opposition, state actors)?
- **Reputational Risk**: If your private data (communications, files, contacts, plans) were breached, what are the potential consequences (e.g., doxing, identity theft, operational compromise)?
- **Impact of Compromis**e: If your private communications were leaked or your online activities misrepresented, how could your reputation (personal or professional) be damaged (e.g., public shaming, loss of trust, employment issues)?
- **Anonymity**: If you are operating anonymously or pseudonymously and your real identity is exposed, what are the potential repercussions (e.g., targeted harassment, physical threats, exposing others in your network)?

Low-Cost / Free Risk Mitigation Measures

- **Utilize separate email accounts for political communications.** Services permitting anonymous registration and offering strong privacy features (like end-to-end encryption) may be appropriate in some cases.
- **Consider using a VPN (Virtual Private Network)** to enhance privacy when engaging in online political activities.
- For web-based political activities, use **separate browser profiles** or private/incognito mode to maintain separation of that activity.
- **Refrain from political communications or activities on networks subject to monitoring**, such as work computers or corporate networks.
- For confidential political communications, **utilize secure communication applications** (e.g., Signal). Avoid using standard email, text messages, or direct messages on other platforms for such sensitive exchanges.

Moderate Cost Risk Mitigation Measures

- When traveling or engaging in political activities, consider **utilizing device-specific high-security modes** (such as Apple's Lockdown Mode) or enabling Airplane Mode to reduce immediate digital exposure.
- For sensitive political collaboration**, limit reliance on standard cloud-based services** (e.g., Google Workspace, Microsoft 365, Dropbox); prioritize more secure, end-to-end encrypted alternatives where practical.
- Implement **comprehensive separation between personal accounts and those utilized for online political engagement**, including distinct credentials and profiles.
- Invest in **hardware security keys** (e.g., YubiKey, Google Titan) for two-factor authentication on critical accounts to significantly bolster login security against phishing and account takeover.
- Consider subscribing to a **reputable paid, privacy-focused email service** for sensitive political communications, which often offer enhanced security features and stronger data protection policies than free ad-supported services.
- Regularly **audit and manage the privacy settings of your online accounts** and device applications, revoking unnecessary permissions and culling outdated or unused services.

High-Cost Risk Mitigation Measures

- **Use physically separate devices (computers, phones) exclusively** for political activities, ensuring complete isolation from all other uses.
- For sensitive online political work, **operate within highly anonymized environments** (e.g., Tails OS routing via Tor) using pseudonymous identities.
- For high-risk travel or events where unauthorized third-party access to devices is possible, **use sanitized 'clean' or disposable 'burner' devices**, assuming all data onboard is vulnerable.
- **Employ anonymized or non-attributable payment methods** for all services and resources related to sensitive political activities.
- **Drastically reduce your digital footprint**: eliminate AI assistance and non-essential software on relevant devices and severely restrict or cease public social media activity.

Additional Resources

- **Electronic Freedom Foundation (EFF):** Tips, Tools, and How-Tos for Safer Online Communications**:** **ssd.eff.org**

- **Commercial VPN Services:**
  - **NordVPN**

- **Higher-Security Productivity Software and Tools**
  - **CryptPad**
  - **LibreOffice**
  - **Proton Mail**
  - **Proton Drive**

About Civic Forge Solutions LLC

Civic Forge Solutions LLC (CFS) is a political technical consulting firm helping Democratic and progressive campaigns, candidates, and causes succeed through innovative strategies that bridge traditional campaigning with digital outreach.

Learn more about CFS @ civicforge.solutions

Bluesky: @hello.civicforge.solutions