FAQs for Digital Political Engagement

Updated on May 9, 2025
michael@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 (CFS) 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.**

Digital Political Engagement involves information security risks that can impact your privacy, reputation, finances, and even physical safety. This Frequently Asked Questions (FAQ) guide provides practical answers and best practices to help you navigate these challenges securely.

This FAQ addresses key aspects of digital security for political engagement, including:

- Identifying online political activities and their associated digital risks, such as phishing, malware, reputational harm, and compromised anonymity.
- Guidance on assessing your personal risk level based on your specific activities and public visibility.
- Actionable security measures, tiered from foundational daily habits to moderate and more intensive protocols, for protecting your data, devices (especially concerning confiscation or use during protests), and communications.
- Considerations for using various tools and platforms, including cloud services, social media, AI assistants, and related software.

This guide offers actionable strategies to help you understand threats and apply effective security measures. Consider tailoring these practices to your individual circumstances, the nature of your engagement, and your specific risk profile.

1. **What is considered online political engagement?**

    - Use of social media for public-facing posts
    - Use of social media for private or limited distribution
        - Direct messages
        - Facebook groups
        - Limited visibility microblog posts (e.g., "friends only" settings)
    - Use of personal devices for communication, coordination, or documentation related to political activities, including at public events.

2. **What types of risks are involved with online political engagement?**

    - **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.
    - **Phishing, Malware, and Spyware:** Malicious software installed on your device without your consent, aimed at spying, exfiltrating data, damaging your device, extortion, blackmail, or related harmful purposes.
    - **Third-party Data Correlation:** Third parties can passively monitor website visits, mobile application usage, and mobile phone-related activities, among other data points, to build a profile of your digital activity and potentially your political leanings.
    - **Man-in-the-Middle (MitM) Attacks:** Interception of data or metadata transmissions via mobile networks, Wi-Fi, or other communication channels.
    - **Physical Security:** Unauthorized third-party physical access to your digital devices (e.g., phone, computer).

3. **How do I assess my personal level of risk for digital security?**

    - Each person's level of personal risk is unique to their individual circumstances. Individuals with heightened risk may need to implement more comprehensive mitigating measures.

    - Risk mitigation measures are not without cost: they may require extra time, financial expenditures, and could potentially impact productivity.

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

    - Evaluating these factors and determining a personal course of action is a personal decision.

4. **What are some low- or no-cost best practices for improving my personal digital security?**

    - **Use a Password Manager:** Generate and store strong, unique passwords for every online service. Never share passwords between services. Never store passwords in unsecure locations (e.g., plain text in a Word or Google Doc).
    - **Enable Two-Factor Authentication (2FA/MFA):** Add an extra layer of security to your accounts wherever available.
    - **Use Encrypted Communication:** Utilize end-to-end encrypted messaging apps like Signal for sensitive personal and political communications.
        - **Account Segregation:** Create separate email accounts (e.g., Google, ProtonMail) and potentially social media profiles for your personal life versus your political activities to limit cross-contamination of data.
    - **Consider a VPN:** Use a reputable commercial Virtual Private Network (VPN) service, especially on public Wi-Fi. Scrutinize their privacy policies and assertions regarding anonymity.
        - **Be Link-Aware:** Be cautious of links received in text messages, emails, or direct messages, especially if unsolicited or from unknown senders. These can lead to phishing sites or malicious software.
    - **Keep Software Updated:** Regularly update your operating system, web browsers, and all applications to patch security vulnerabilities.

- **Review Privacy Settings:** Regularly check and adjust privacy settings on social media platforms and other online services to control who sees your information.
- **Limit App Permissions:** Only grant applications the permissions they absolutely need to function.

5. **What are some practices I should avoid?**

- **Using Unsecure Communication Channels for Sensitive Information:** Avoid using unencrypted text messages (SMS) or emails for highly sensitive political communications. While some platforms and circumstances might offer security, it's often difficult to definitively determine the security posture of these systems for the average user.
- **Connecting to Unsecured Wi-Fi:** Do not use unsecured or unknown public Wi-Fi access points without a VPN, especially for sensitive activities.
- **Oversharing Personal Information:** Avoid posting excessive personal details online that could be used to identify or target you (e.g., home address, daily routines, specific location check-ins).
- **Using Weak or Reused Passwords.**
- **Clicking Suspicious Links or Downloading Unknown Attachments.**
- **Ignoring Software Update Prompts.**

6. **Should Google Cloud and/or Microsoft Office 365 be utilized to store sensitive personal or restricted information?**

It depends on your risk assessment and the sensitivity of the information. In many cases, for general use, they are reasonably secure. However, for very sensitive communications or documents, consider alternatives.

While both services provide encryption for documents and data, in most consumer instances (unless the services are being utilized in specific corporate/enterprise configurations with customer-managed keys), Google and Microsoft generally hold the "keys" used for encryption. These companies may be compelled to decrypt and release your information in response to lawful requests from law enforcement or judicial authorities. In such events, you, as the owner or administrator, may not always be notified.

To ensure greater security and privacy where you control the encryption key, consider services like CryptPad.org (provides end-to-end encrypted collaborative editing), Proton Drive (end-to-end encrypted cloud storage), or using software like LibreOffice to encrypt your documents locally *before* uploading them to any cloud service.

It is important to note that no encryption method is entirely foolproof. With sufficient resources and time, or due to implementation flaws, some encryption methods could theoretically be compromised. However, using services where you control the encryption key, or employing strong end-to-end encryption, significantly enhances your privacy and security.

7. **What can happen if an unauthorized third-party obtains custody of my device?**

    If an unauthorized third party gains physical possession of your device:

    - If the device is **locked** with a strong passcode/PIN and ideally full-disk encryption, exfiltrating its contents is difficult and time-consuming, requiring significant resources and expertise. However, it may still be possible for well-resourced adversaries.
    - If the device is **unlocked**, or if the attacker can bypass the lock (e.g., knows the PIN, can compel biometric unlock), data can be immediately exfiltrated.

8. **What steps can I take to decrease the risk of data exfiltration if an unauthorized third-party obtains custody of my device?**

    In situations where an unauthorized third party could obtain custody of your device, consider these mitigating measures (among others):

    1. **Use a Strong, Unique Passcode/PIN:** Avoid easily guessable combinations. Use alphanumeric passphrases if possible.
    2. **Enable Full-Disk Encryption:** Ensure it is active (most modern smartphones have this by default; ensure it is enabled on laptops/computers).
    3. **Data Minimization on Device:** Regularly remove applications and data that you wish to remain completely private and secure if they are not essential to have on that device, especially if going into high-risk environments.
    4. **Apple Device "Lockdown Mode":** If you have an Apple device and anticipate high risk, utilize "Lockdown Mode," which severely restricts certain functionalities to reduce attack surfaces.

5. **Disable Biometric Authentication in High-Risk Situations:** In specific scenarios where you might be compelled to unlock your device consider temporarily disabling biometric-based authentication (Touch ID, Face ID, fingerprint unlock) and relying solely on a strong PIN or alphanumeric passcode.
6. **Enable Remote Wipe/Lock Capabilities:** Configure services like "Find My iPhone" (Apple) or "Find My Device" (Android) to allow you to remotely locate, lock, or erase your device if it's lost or stolen.
7. **Set a Short Auto-Lock Period:** Configure your device to lock automatically after a brief period of inactivity.

9. **Should I buy a "burner phone"?**

Purchasing an additional ("burner") mobile or desktop device can help limit the risk of data exfiltration if a third party obtains custody of one of your devices. It can also limit the impact if malware, spyware, or a phishing attack compromises the security of one computing device, as your primary data and accounts would be separate.

This option incurs expenses for the device and any associated data plan. If you anticipate situations where an unauthorized third party could gain access to your device, or if your activities place you at high risk, then the use of a burner phone (used with appropriate operational security) may be an appropriate measure.

10. **I'm concerned about previous posts I've made on social media. Should I delete my social media history?**

The general rule is that information released to the internet can rarely be completely and permanently deleted. However, through privacy settings, it's often possible to significantly reduce the accessibility or visibility of previously posted content (depending on the platform). Platforms also provide options to delete accounts, though there are caveats.

Deletion requests do not conclusively guarantee that every copy of your data has been removed from all locations. For example, if your previous posts were collected by third parties via screenshots, archiving services (like the Wayback Machine), or other automated methods, you likely cannot identify all those third parties nor enforce data deletion requests with them.

However, deleting posts or accounts does ensure that, from the time of deletion (and after any platform processing period), the content of your original posts is generally not accessible to the public *directly from that platform*.

- **Meta (Facebook and Instagram):** You may utilize the Meta Privacy Center (https://www.facebook.com/privacy/center/) to review and adjust the visibility of posts and personal information, or to request account deletion.
- **X (formerly Twitter):** X provides instructions for account deactivation and deletion: https://help.x.com/en/managing-your-account/how-to-deactivate-x-account#how-to-deactivate
    - Note: Due to the public nature of X, limiting the visibility of individual past public tweets is difficult without making the entire account protected (which only affects future visibility to non-followers and requires approval for new followers) or deleting them.
- **Bluesky:** Bluesky provides instructions for account deactivation: https://bsky.app/profile/safety.bsky.app/post/3ku74ugpby22f
    - Note: Due to the nature of Bluesky (and the underlying AT Protocol), there may not be practical means of limiting visibility of posts on federated relays. Account deactivation does not guarantee that previous messages will be deleted from all parts of the decentralized network.

11. **What should I do with my mobile phone when participating in a public organizing or protest event?**

Mobile devices are invaluable tools for organizing and documentation; however, bringing your device to locations where unauthorized third parties might gain access (physically or digitally) carries risks. These include, but are not limited to, unauthorized confiscation, malware infection, man-in-the-middle attacks (especially on unknown Wi-Fi), and location tracking.

If your personal risk assessment indicates a heightened threat level for such events, consider these risk-mitigating steps for any personal devices you bring:

- **Review Section 8:** Implement relevant measures from "What steps can I take to decrease the risk of data exfiltration…".
- **Use a "Clean" or Burner Device:** As discussed in Section 9, a separate device with minimal personal data is often the safest option for high-risk activities.

- **Disable Wi-Fi and Bluetooth:** Turn these off when not actively needed to reduce tracking vectors and attack surfaces from nearby devices.
- **Enable Airplane Mode:** If you only need offline capabilities (e.g., taking photos, notes) and don't need to communicate, Airplane Mode can reduce some (but not all) transmission risks. Be aware that some advanced surveillance tools might still be able to interact with a device in certain states, even in Airplane Mode.
- **Power Off Completely:** If you don't need the device, powering it off entirely is the most secure state as it stops all transmissions and makes forensic access much harder without first bypassing the lock screen on boot.
- **Use Encrypted Communication Apps:** For any necessary communication, use end-to-end encrypted apps (e.g., Signal).
- **Be Aware of IMSI Catchers (Stingrays):** These devices can mimic cell towers to intercept mobile traffic or track locations. While difficult for an individual to detect, using end-to-end encrypted communication apps and reputable VPNs (for data traffic that isn't already E2EE) can mitigate some of their impact on data content, though not necessarily on metadata like location or call logs.
- **Consider Photography/Videography Ethics:** Be mindful if capturing images/videos of other participants could put them at risk. Seek consent where possible or consider blurring faces and other identifying information before sharing.
- **Physical Security:** Keep your device secure on your person to prevent snatching or loss.