Digital Security for Activists - Key Actions

This is a quick guide to practices you may wish to use, depending on your circumstances. For much more detailed information and practical tips see guides such as activistchecklist.org & www.privacyguides.org.

1. Security essentials

- **Prevent personal devices from falling into the wrong hands**
    - Store devices, especially phones and laptops, safely and do not display them in public unnecessarily.
    - Avoid bringing them to riskier situations, such as protest actions.
- **Don't share any sensitive information via insecure communication channels**
    - Consider any public facing channel, any Whatsapp group, or any unvetted chat insecure.
    - Work on the assumption that not everyone with access to group chats or emails will be your ally, and that participants/viewers might not be who they say they are.
- **Avoid storing any potentially sensitive information**
    - Permanently delete anything you no longer need.
    - Store anything you do need as securely as possible.

2. Good Practices

- **Use security-focussed software and tools**
    - For messaging and calls, Signal is likely to be your best option. For advice on how to configure and use Signal as securely as possible see activistchecklist.org/signal.
      Note: For larger meetings Brave Talk is a more secure alternative to Zoom.
    - For email, Protonmail can be a good option, but bear in mind that email is not recommended for secure communications.
    - For web browsing, use a browser such as Firefox or Brave, and configure it to provide the best security. See advice at www.privacyguides.org/en/desktop-browsers.
    - For web searching, use an engine such as Brave search or Duck Duck Go.
    - For shared or collaborative documents, try CryptPad or Proton Docs tools.
    - For navigation, try Magic Earth, Organic Maps or CoMaps. Apple Maps is considered more secure than Google Maps.

- **Further protect yourself against spyware, hacking, tracking and other data breaches**
    - Keep software and devices updated.
    - Activate enhanced device/account protection options (e.g. Android/Google's Advanced Protection Program, Apple devices' Lockdown Mode, Microsoft's Account Guard, Proton's Sentinel). *Note: There may be some trade-offs in terms of device and account usability.*
    - Don't click on suspicious links, e.g. from unknown senders or in unexpected urgent-seeming messages. These can be a route to downloading spyware onto your devices.
    - For password security:
        - Use strong passwords, with different ones for each site/account, rather than sign-ins via Google/Facebook etc.
        - Consider using a password manager e.g. Bitwarden, 1Password or ProtonPass.
        - Passcodes (the longer the better) can be more secure than face or fingerprint access in situations where you could be compelled to unlock your device.
- **Avoid unnecessary data use, storage and sharing**
    - Activate disappearing messages on relevant apps.
    - Disable location services for any software that doesn't need it. *Note: Hardly any apps should require location data, with the exception of navigation tools.*
    - Remove all unnecessary apps and limit use of non-essential online services. Use "opt out" options rather than agreeing by default to standard or recommended terms of use.
    - Remove smart devices and apps designed to listen or record e.g. voice assistants like Amazon 'Alexa' or Google Home.

3. Advanced Security

- **Be vigilant against surveillance**
    - Use a VPN (virtual private network). *Note: most trusted VPN services require a paid subscription.*
    - Cover device cameras when not in use.
    - For any particularly sensitive communications, use an alternative device and set of accounts that are not easily linked to you.
- **Pare back engagement with tech and online media**
    - Remove your personal information from searchable sources. This includes sites and profiles you control such as social media accounts, as well safeguards against data brokering.
    - Move away from platforms with poor track records or uncertain futures with regard to data security and information sharing practices. *This includes all services provided by all major tech companies, including Meta and Google.*