A beginners guide to data security for activists (2025)

Secure your identity:

- Turn on 2-factor authentication (2FA), aka Multifactor authentication (MFA), for all your accounts whenever possible, this adds an extra step when logging into an account. It requires you to enter a code (generated by an app or by a text message) in addition to a password.
- When you respond to security questions, try using code phrases instead of answering them honestly, so that nobody familiar with your life could guess it and force a password reset without your consent.
- Beware of phishing. Don't open suspicious attachments or click on suspicious links. Never provide passwords to anyone for any reason. Most (over 80%) of inappropriate access to data is due to human error.

Secure your comms:

- Assume most communication platforms including WhatsApp, Telegram, Messenger, phone calls, text messaging, and email are unsafe.
- Use the phone app Signal for end-to-end encrypted texts. Verify your contacts. If you want you can enable disappearing messages. Leave and delete chats about sensitive topics after the conversation is over.
- Clear sensitive messages, chains, or threads frequently.

Additional Resources

- How to create a strong password, a comic: xkcd.com/936
- Electronic Frontier Foundation ssd.eff.org for a deeper dive into all these topics
- Learn more about phishing at phishing.org
- What is a VPN and how do I get one? privacyguides.org/en/basics/vpn-overview
- Activists and the Surveillance State, Learning from Repression, a book edited by Aziz Choudry

Secure your computer:

- Create a strong password. This means it should be original, complex, containing no personal info, and updated as often as possible.
- Store passwords on an encrypted platform such as Bitwarden, LastPass, 1Pass, or KeePass.
- Create separate user and admin accounts. Use a user account for daily activities to avoid digital attacks aimed at the root level of your computer.
- Update operating systems frequently.
- Store sensitive data on external hard drives and USB keys. Assume Google Drive and other platforms are unsafe. Password protect these external devices.
- Use the browser Firefox or Brave.

Backing up your phone:

iPhone: Don't use iCloud backups. Backups made with iCloud are encrypted in such a way that employees at Apple can access them. Keys to unlock the phone's full-disk encryption are also stored in the iCloud backup.

Android: Do not use Android cloud backups prior to version 9. Version 9 and newer includes end-to-end encrypted backups that even Android cannot open without the user's passcode. This feature is automatically active as long as you have a lock screen protected with a PIN, pattern, or passcode.

Secure your phone:

- Use a PIN passcode, never touch ID or face ID. Always lock your screen.
- Keep phone and apps updated.
- Turn off location services. Your location is tracked in the background of your services by default. This data is shared with your applications and your mobile carrier.
- For groups and individuals that have more acute security concerns, a factory reset of mobile device is recommended
- Don't use Google search. Use a search engine like Brave search or DuckDuckGo.
- Use the browser like Firefox or Brave if looking up sensitive content.

- Don't use Google Maps to locate or get to a sensitive location.
- Disable Airdrop unless you are actively using it, then turn it back off.
- Turn off Bluetooth, WiFi, and Ultrawideband (UWB) when needed. These use short-range radios to communicate with other devices. This information can be observed by a "beacon" or scanning device.