7 Digital safety tips for people documenting Human Rights abuses

IMPORTANT:

- **Read the terms and conditions** of ALL platforms and tools before using them.
- Knowing who owns the company and where it is based prevents you and your data from being vulnerable to attacks by governments.
- Check the company's transparency reports and stay updated on any service changes.

1

Protect your personal data

- **Look yourself up online on live sites and internet archive sites**, such as the Wayback Machine (name, phone, address, day of birth even image reverse search). Use the incognito mode!!!
- Look up the data of family members to see what information about them is available.
- **Review the privacy settings on your social media accounts** and remove or restrict your information, including images. Consider blurring out your house on Google Maps and other online maps.
- **Keep track of any activity** related to your personal information using Google Alerts to your name, address, etc.

2

Protect your accounts

- **Use a Password Manager** to manage all your passwords.
- **Use 2-factor authentication** such as Authy and do not use SMS. If you are at high risk, use a security key such as a YubiKey.
- If the 2FA offers you codes, print them, save them in a backup or in your Password Manager, then delete them from your account.
- **Separate** personal and professional data in emails, cloud, phone, etc.
- **Monitor your account activity**, log out from shared devices, and be cautious with public computers.
- Check your accounts in **security incidents** by looking them up on “have I been pwned”.

3

Protect against targeted phishing attacks

- Be cautious of urgent messages.
- Verify sender details.
- Think twice before clicking on links.
- Preview email attachments before downloading them.

Additionally, consider uploading suspicious links and documents to Virus Total scanning.

4

Device security

- Lock devices with a password, code, or PIN
- Update your operating system, apps and browsers when prompted
- Don’t use USB flash drives that are handed out free at events
- Set up your devices to allow you to wipe any data remotely: It will only work if it is connected to the internet
- Encrypt your smartphones. New ones will come with this function on the settings, make sure it is switched on
- Encrypt your computer: Use Bitlocker for Windows, Firevault for Mac, or Veracrypt software for hard drives and external storage.

IMPORTANT

Your device may backup your data to the cloud account linked to the phone.

Information stored in the cloud may not be encrypted. Turn off automatic backups

5

Encrypt your communications

- Use Signal when messaging other people.
- Use the disappearing message functions and regularly review and delete sensitive content from your phone and apps.
- Lock the app with a PIN or passcode where possible to better protect against someone opening the app if they have physical access to your phone.
- Encrypt your email with reputable software and a strong, memorable password for access. The receiver must also download the software.
- Backup your devices regularly and store the backup copies securely;

Details about an email, including the title and the email addresses sending and receiving the message, are not encrypted.

6

Secure your internet

- Protect your browsing history using a virtual private network (VPN - Use Mullvad or Tor)
- Use DuckDuckGo Smarter Encryption to ensure that the site you are visiting is encrypted
- Install an ad-blocker
- Install Privacy Badger to block websites and advertisers from tracking what sites you visit online
- Avoid using public computers, especially at internet cafes or press rooms.

7

If crossing borders

- Assess and remove sensitive information from all devices before traveling. Log out of all accounts on your devices and uninstall apps
- Backup data and use separate, clean devices for travel, especially for highly sensitive work
- Clear your browsing history on all your devices
- Power off your devices to activate disk encryption
- Be cautious of SMS messages and phone calls that may not be end-to-end encrypted and treat confiscated devices as compromised.

For more information, visit cpj.org