huridocs
human rights information and documentation systems

Basic digital security information for human rights defenders

This brief provides general information about basic digital security practices that human rights defenders (HRDs) may consider in the course of their work. It does not provide exhaustive information on how to address every digital security incident. Therefore, HRDs are advised to also consult trusted sources of information for their digital safety.

SECURE YOUR PHONE

- Make sure your phone uses the latest operating system and gets regular security updates.
- Only download apps from authorised sites and resources (Google Play Store, Apple Store).
- Use a strong passcode to lock your phone.
- Uninstall apps that you don't use and don't need.
- Remove sensitive files, unused files and consider clearing text and call history.
- Disable displaying message content in notifications (for example, in Signal: Settings → Notifications → Show → choose “Name only” or “No name or message”).

SECURE YOUR COMPUTER

- Make sure your computer gets regular updates and avoid using any unlicensed software or programmes.
- Use a strong password for user authorisation.
- Turn your firewall on.
- Turn your full disk encryption on.
- Install a trusted antivirus (for example, Malwarebytes).
- Ensure that no sensitive data is stored on your computer and consider storing sensitive data in a secured cloud account.
- Always use strong passwords for all accounts and do not use the same passwords for multiple accounts.
- Use a password manager to store all your strong and unique passwords for all your accounts.
- Protect your accounts with 2-factor authentication (2FA) using an app (for example, Google Authenticator), and do not opt for SMS authentication. Where possible generate back-up codes as a secondary 2FA option and store them in a password manager or another preferred secure place.
- Clean your computer of unnecessary data from time to time.
- Always use a virtual private network (VPN) when working in public places (coffee shops, libraries, airports) and when connecting to public networks.
- Check your browser’s settings and make sure your login credentials (usernames and passwords) are not saved in the browser.
- Consider clearing cookies, browser cache and browser history on a regular basis.

PHYSICAL SECURITY

- Be discreet with digital devices and keep these in sight and close to you at all times.
- Be vigilant and aware of your surroundings (meeting room, coworking space, strangers).
- Watch out for strangers who express overall curiosity about your work.
- Watch out for derelict or abandoned devices (USBs, tablets, even notebooks) especially when working in a public space.

Follow us for more tips and updates for human rights defenders, or reach out to collaborate!

www.huridocs.org

hello@huridocs.org