UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

6 Protection of information and devices when travelling

The term "sensitive information" includes (not an exhaustive list):

- Your personal safety is your highest priority. Procedures related to data storage must be put in place.
- Your phone/computer must be encrypted, and passwords protected.
- Store the most sensitive information on encrypted cloud storage. If this is not possible, encrypt an external storage device, and modify its file extension using 7-Zip[1] or VeraCrypt.
- Never leave your digital devices unattended e.g., in hotel rooms, airports, or restaurants.
- Do not entrust your devices to unknown persons.

DO

It is recommended to travel light – keep limited information and avoid storing sensitive data on your devices. The less information, the better. Keep your sensitive data off from your computer and mobile phones during travel. These could be subject to inspection and confiscation.

It is recommended to prepare your devices with social media accounts that are not associated with sensitive information. Social media accounts on your devices may be checked when you cross borders or at checkpoints. Ensure you have a social media account without any association or affiliation with civil society organizations or activism.

It is recommended to ensure your phone does not contain banned apps (even secure messaging apps). You may use Facebook messenger as your temporary messaging application while traveling, but do not include any sensitive information on this app.

It is recommended to backup your authentication app (e.g., Authy generates 2-Factor Authentication) and keep another copy at home, which allows you to back up your authentication codes on a separate device. This allows you to recover your 2FA/MFA codes in case your main phone is confiscated or stolen during your travels.

It is recommended to use an email account that is not associated with contacts that may be deemed sensitive. Always use email addresses not associated with any of your personal or work activities. Use this when signing up for subscriptions, through shopping purchases or by simply logging into the logbooks of an establishment.

It is recommended to factor into your decision-making the benefits of using physical maps instead of Google Maps. Having a physical map of the location/region sometimes can be useful especially if you are in a location where there is no DATA/GPS signal or to avoid surveillance or tracking from apps that have access permission to your phone's location service. If you really need an electronic map, download a copy of OpenStreetMap or Google Maps for offline usage.

It is recommended to consider performing a factory reset on all devices if you suspect tampering after traveling to intense surveillance locations. This is to avoid any possibility of potential infection of any of your devices during your travel.

DON'T

It is not recommended to keep any sensitive files on your devices during travel. Your laptop and smartphone may get inspected or confiscated.

It is not recommended to log into any personal accounts on your phone or on your computer when travelling.

It is not recommended to store your login history on your devices. If you are using your devices for browsing, accessing social media, or checking emails, stored logins can be used to gain access into accounts by undesirable access. Stick to only those apps that are essential.

It is not recommended to install any software, applications, or technologies that may have been banned in the country you are traveling to.

It is not recommended to use your work or personal email for logging in to any public information desks.

It is recommended to always use a non-personal, non-work-related email address or information when meeting with a sensitive partner. Public information desks often ask for confidential information.

[1] https://www.7-zip.org