UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

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

4 Data security for cloud storage

All cloud storage that you use must be protected by a strong passphrase and 2-Factor Authentication/ Multi-Factor authentication (2FA/MFA). The most common cloud storage options (Google Drive[1] or Microsoft One Drive[2]) use their own default encryption while storing your documents/files on their premises, and tend to have full access to your information stored on their servers. Your files may also be requested by Governments and are vulnerable to the event of a breach. Using their specific email services means that all your incoming and outgoing emails are stored on the private companies' servers as well. This information is vulnerable to "take downs" following requests by Governments or by companies own policies.[3] The information stored on your office drives is as secure as the servers themselves (physically and digitally).

DO

It is recommended to secure all your online cloud storage accounts by enabling 2-Factor Authentication/Multi-Factor Authentication (2FA/MFA). Adding 2FA/MFA on your cloud storages helps protect your cloud storage account against password attacks such as brute-force or credential stealing. 2FA/MFA should be enabled on all online accounts[4] (including email) that offer this facility.

It is recommended to use an encryption tool (e.g. Cryptomator,[5] or VeraCrypt). **To encrypt your existing cloud storage if it does not come with built-in end-to-end encryption options.** These software (paid or free, depending on the type of subscription,) allow you to encrypt multiple cloud storage accounts.

It is recommended to choose cloud services providers offering end-to-end encryption facilities. Some recommended cloud storage providers such as Sync,[6] MEGA,[7] Tresorit,[8] SpiderOak,[9] and PCloud[10] offer end-to-end encryption options to ensure that the data stored on these companies' servers is only accessible to the end user. These services can be used on both your computer and mobile devices.

It is recommended when sharing folders and documents to others, verify and confirm the email address you share your cloud documents with. When sharing documents from your cloud storage make sure that you have the right email address.

It is recommended to create separate accounts for work and personal cloud storage, to better manage your documents and classify them according to sensitivity.

It is recommended to use a VPN when accessing your cloud storage, to hide your Internet activity and access to your cloud storage from your local Internet service provider, your Hotel Wi-Fi Administrator, or anyone who is in between you and the Internet.

DON'T

It is not recommended to store sensitive information on unencrypted cloud storage (office or otherwise).

It is not recommended to put any unencrypted sensitive files in your cloud storage because of the risk of unauthorized access in the event of breach or system compromise.

It is not recommended to enable "Offline Versions" of your sensitive file as this can allow you to locally store a copy of that file in your browser, which can be accessed by anyone who has physical access to your computer or device. Do not put all your data on one cloud storage because of its "single point of failure." If your cloud storage is compromised, or you cannot access it, all your files will be inaccessible whether it is personal or for work. Separate them and create backups.

1 https://www.google.com/drive/
2 https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage
3 See for example Google Transparency reports https://transparencyreport.google.com/user-data/overview?hl=en
4 List of websites and information about whether or not they support 2FA: https://2fa.directory/int/
5 https://cryptomator.org/
6 https://www.sync.com/
7 https://mega.io/
8 https://tresorit.com/
9 https://spideroak.com/
10 https://www.pcloud.com/