UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

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

8 Safe use of social media

Social media platforms are used for sharing information of all sorts. In some countries, social media platforms are censored or controlled. To protect your social media accounts, as well as to protect your privacy and security, below are some of the DOs and DON'Ts in managing your social media accounts.

DO

It is recommended to enable 2FA/MFA on your social media accounts. 2FA/MFA adds strong protection for attacks and attempts to steal your username and password.

It is recommended to limit the information you use to create your account. Limiting information can prevent attackers from profiling you based on publicly available information.

It is recommended to download backup codes (for two step authentication) from your social media account settings. Extract the backup codes from your social media accounts and keep them safe.

It is recommended to enable the "Trusted Contacts" on Facebook. Trusted Contacts allows you to find your Facebook friends and gives them the ability to create a recovery code for you.

It is recommended to download your data from Facebook. Download your Facebook data in case of any targeted attacks or shutdown attempts on your social media account.

It is recommended to refrain from posting photos of a public or private forum or training. Whatever you post on social media, you may disclose other sensitive information such as meetings and events, attendees, or anyone else participating specially in private activities such as workshops, training, and forums.

It is recommended to review your account's privacy settings. Review your privacy settings and review what information is shared to the public. Also, check the "device history" as it can identify if someone else used your account.

It is recommended to hide or remove personal information from your social media accounts. Limit personal information on your social media such as email, telephone number, home, or office address.

DON'T

It is not recommended to associate your account with your phone number. Social media accounts that are linked to a phone number can be reset by requesting codes to the phone number used. If your phone is stolen and is not well secured, attackers may request a recovery code using your lost phone allowing attackers to change your social media account password. Other common attacks such as SIM spoofing and SIM swapping can be used to gain access to your phone number and then used to receive reset access codes without your knowledge.

It is not recommended to enable tagging to your account. Tagging allows your friends to include you on a post, while that post is also posted on your profile. This may disclose sensitive information such as event locations, your family members, and participants.

It is not recommended to post any sensitive information such as private event details. Posting sensitive information on your social media may pose some risk as it can easily be captured and used for social engineering attacks.

It is not recommended to post any content that is deemed too sensitive or critical, especially if you are in a different region or country. Whenever traveling, refrain from posting any content that is deemed offensive or any context that is taboo in the country or location.