UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

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

9 Where to go for help

During digital security incidents or regular technical issues, it is important to know what is happening in your surroundings to be able to understand your security context, as well as the attacker's technique, tactics, and intention. If you or your organization have the capacity to perform an initial investigation and troubleshooting of these incidents, try to record all information accurately.

✓ DO

It is recommended to document the occurrence during or just after a digital attack, in particular the date and time, context, and chronology.

It is recommended to take screen shots, photos, or video of the occurrence e.g., error messages. If there is no time to note, take pictures or videos of the actual digital security incident.

If there is a sign of computer infection, it is recommended to disconnect your PC from the Internet. Malware is also used to download data, information, and any user-related documents that it finds relevant. If there is any sign of malware infection, disconnect your computer from the Internet immediately.

It is recommended to initiate personal/ organizational security protocol. If you suspect that your computer has been infected, or your social media account compromised, change your passwords immediately, enable 2FA/MFA and disconnect any “connected” devices on your account, from the account settings.

It is recommended to always prioritize your personal safety over your digital devices. There are no devices or information that can be more valuable than your own safety.

It is recommended to familiarize yourself with organizations that can support you.

✗ DON’T

Don’t panic! Keep calm and analyse the situation. You will make better decisions once you are calm.

It is not recommended to miss any important error messages. If an IT support person can identify what the error is right away, it can ensure the problem is resolved promptly.

It is not recommended to release any information to the public before thoroughly understanding the impact of doing so.

TIPS!

Access Now have a Digital Helpline that will follow up within two hours of the reporting (email: help@accessnow.org).

Citizen Labs has a team of experts that may be able to help you and your organization in any digital security incidents. Sharing incident details with your partners, friends and organizations about the attack may prevent others from also being targeted. You can contact them here.

Frontline Defenders has an emergency call number for human rights defenders who will help determine how to best support in an urgent situation. In cases of time differences, poor connectivity, and the significant amount of details in urgent cases, you can send them a message via secure and encrypted channel using their contact form here or email them at info@frontlinedefenders.org.

Note: References to external entities and websites are only indicative and should not be considered an OHCHR’s endorsement to such entities and websites and the services provided by them. These references are provided, without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. Under no circumstances shall OHCHR be liable for any loss, damage, liability or expense incurred or suffered that is claimed to have resulted from the use of these websites. The use of these websites is at the user’s sole risk. The external websites are not under the control of OHCHR, and OHCHR is not responsible for their content or any link contained in these sites.