UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

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

12 Encryption

Encryption is a tool to protect against cyberattacks that attempt to compromise or access data without prior authorization. Communication and device encryption may protect us against unexpected attacks, online surveillance or if devices are confiscated.

Encrypted data.

- Encrypted data are data that are encoded or made unreadable. The only way to open and read it is by using an encryption key.
- An encryption key is an auto-generated string of characters that looks like gibberish to make it difficult to read.

Password-protected data.

- Password-protected data are data that simply require a password to open or access.
- Passwords are required to open a password-protected file. Passwords are in the form of text and are often readable and are vulnerable to attacks like keylogging – or capturing keystrokes using malicious software.

End-to-end encryption.

- Is the process of encrypting information from the senders' device and decrypting it only on the receivers' device.

Full Disk Encryption (FDE).

- A term that refers to the encryption of the entire hard disk drive of an operating system, including operating system files and personal data and sensitive information

Symmetric encryption.

- Uses identical or one key or password to decrypt or encrypt data.

Asymmetric encryption.

- Uses two related keys (public and private) for data encryption and decryption.
- Think of this as the mailbox outside your home. Your mailbox refers to your "public" key. Your mailbox has a lock and requires a key. This "Key" to open your mailbox is now your "private" key.

Bit Locker encryption

- Bit Locker is an encryption software that is built-in into some editions of the Windows operating system. It is not available on Windows 10/11 home edition and not enabled by default, but can be enabled while the system is in use.

FileVault encryption

- FileVault is an encryption software for Apple (Mac OS) computers on Mac OS X 10.3 and later versions. It is not available by default but can be enabled while the system is in use.

LUKS

- LUKS is an encryption tool for Linux operating system. To enable this and apply full-disk-encryption (FDE), you need to enable this during installation, unlike Windows and Mac OS.