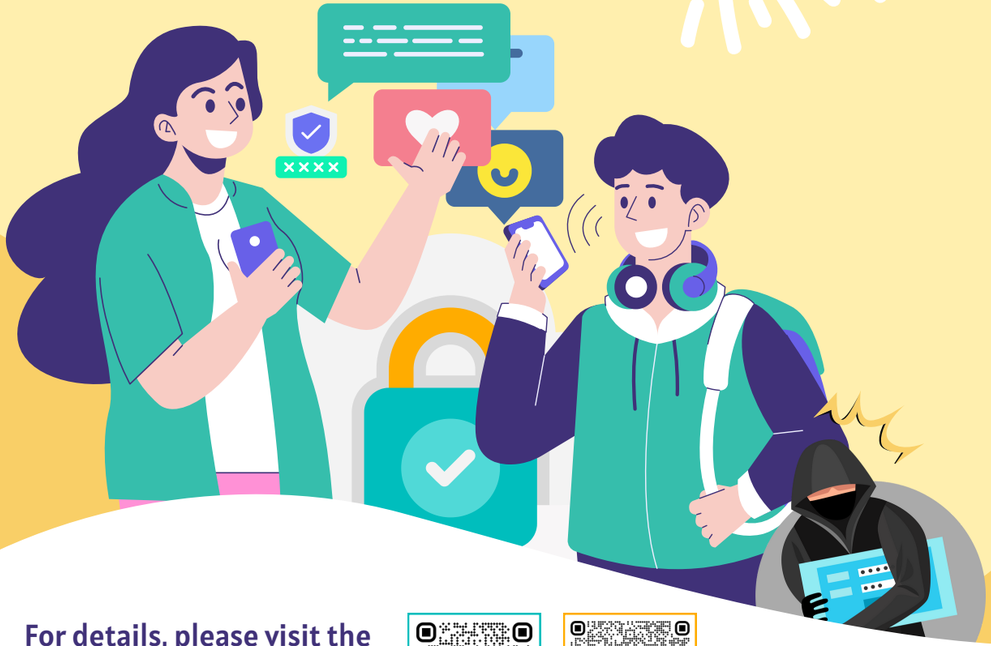
THE DO'S AND DON'TS OF USING INSTANT MESSAGING



For details, please visit the CyberDefender or HKCERT website at :

GovCERT.HK
Government Computer Emergency Response Team Hong Kong

HKCERT Hong Kong Computer Emergency Response Team Coordination Centre

CYBER DEFENDER 守網者

Update instant messaging software regularly. Enable two-factor authentication and set a personal identification number (PIN) for your account.

Leave, block and report a suspicious group if you are being added to it.

Manage privacy settings properly. If available, turn on the "Silence Unknown Callers" function and modify the settings of "Who can add you to groups".

Check the devices linked to your account regularly and log out of any unused devices.

Stop communicating with individuals requesting money, personal or sensitive information. Verify the sender's identity through an alternative channel.

Do not disclose your login verification code or PIN to anyone.

Avoid downloading apps from unofficial sources.

Do not reply to or answer unsolicited messages, voice calls, or video calls.

When searching for the web version, exercise caution with search engine results. The advertisement links placed on top may lead to fake websites.

Do not click on suspicious links within messages or download files from unknown sources.