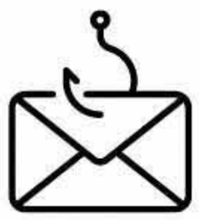
PROTECT YOUR WHATSAPP ACCOUNT FROM SCAMS

Follow these steps to safeguard your account.

Do not use "WhatsApp Web"	If there is a need to, always ensure that you are using the official WhatsApp Desktop App or visiting the official WhatsApp website at the URL address https://web.whatsapp.com.
Never share sensitive information with anyone	This includes your WhatsApp verification codes, personal information, banking details or OTPs. Never click on Singpass login URL weblinks sent through WhatsApp or other messaging methods like SMS.
Be wary of unusual requests	This includes requests from your WhatsApp contacts — they may have been compromised. Requests include monetary loans, assist to make payments through a clickable link or download an APK file that is actually malicious.
Enable Two-Step Verification	This can be done by opening WhatsApp and going to 'Settings' > 'Account' > 'Two-Step Verification' > 'Enable'.
Check your linked devices regularly	Go to 'Settings' > 'Linked Devices' to review all linked devices linked to your account. To remove a linked device, tap the device > 'Log Out'.
Set a device code	Be wary of who may have physical access to your phone. Those that have access to your mobile device may use your WhatsApp account without your permission.
Verify screenshare requests	Exercise caution when receiving screenshare requests. Always verify and confirm the identity of known contacts through a voice/video call before screensharing.

PROTECT YOUR TELEGRAM ACCOUNT FROM SCAMS

Follow these steps to safeguard your account.

Enable Two-Step Verification and Passcode Lock 	Enable this feature under Settings > Privacy and Security > Two-Step Verification > Set Additional Password and Passcode Lock under Settings > Privacy and Security > Passcode & Face ID > Turn Passcode On
Do not share unique verification codes or personal/banking information to anyone 	Do not respond to any suspicious messages requesting for a One-Time-PIN (OTP)/verification code or your personal/banking details. Do not click on any links, especially Singpass login URL weblinks, to provide your personal and/or banking information. Block and report the sender to Telegram.
Do not share your Telegram verification codes 	Do not respond to any suspicious messages requesting for an OTP or code to be send to them. Do not click on any links (e.g. Singpass login URL weblinks) or provide any other personal information.
Prevent unknown persons from contacting you 	Allow only your contacts to call you and add you into chat groups. Change your call permissions and limit who can add you into chat groups under Settings > Privacy and Security > Calls/Groups > Change from 'Everybody to 'My Contacts'
Make your phone number private on Telegram 	Change who is allowed to see your phone number on Telegram by going to Settings > Privacy and Security > Phone Number > 'Nobody' (etc.)
Secure your payment & shipping info 	Clear your payment and shipping information on the app by deleting them under Settings > Privacy and Security > Data Settings > Clear Payment and Shipping Info
Monitor and disable sessions when not in use 	You may disable active sessions when they are not in use under Settings > Devices > Select the session not in use > Terminate Session. Additionally, enable end-to-end encryption by using the secret chat option.
Verify screenshare requests 	Exercise caution when receiving screenshare requests. Always verify and confirm the identity of known contacts through a voice/video call before screensharing.