JOINT NEWS RELEASE BY SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON SOCIAL MEDIA IMPERSONATION SCAMS INVOLVING TELEGRAM

The Police would like to alert members of the public to a social media impersonation scam variant involving the messaging app, Telegram. Since January 2023, at least 50 victims have fallen prey to this variant, with total losses amounting to at least $18,000.

2 For this scam variant, scammers take over control of victims' Telegram accounts by tricking victims into providing their handphone numbers and Telegram generated login codes. The scam works in the following ways using a compromised account of the victim's known contacts:

i. Victims are added into a secret Telegram chat by scammers pretending to be the victims' known contact and are asked to provide a screenshot of their Telegram chat history. Unknown to victims, the screenshot will reveal a Telegram generated login code because the scammers will simultaneously trigger a Telegram login code for the victim's Telegram account; or

ii. Victims are asked by the scammer pretending to be a known contact to help him locate someone on Telegram and are instructed to search for specific usernames (e.g. login_not, not_this) in their chat history and provide a screenshot of the search results. The screenshot would invariably contain a Telegram login code; or

iii. Victims are asked to help verify or unblock the Telegram account of a known contact that had been restricted by Telegram. To help verify or unblock the Telegram account, victims would send a request to a Telegram handle

which masquerades as a ‘customer service bot’. The bot would then ask for the victims’ details (e.g. mobile number). Victims will then be asked for their Telegram login codes or are sent URL links masquerading as a verification button to allow their ‘friend’ to log in to the victim’s Telegram account; or

iv. Victims are asked by a known contact to help secure a free Telegram membership. Scammers will trick victims into participating by clicking a link to allow the scammers to log in to the victim’s Telegram account, resulting in the victim losing access to his/her Telegram account.

3 Once scammers take over the victims’ Telegram accounts, the scammers would proceed to target the victims’ contacts to repeat the same ruse to take over their Telegram accounts or ask for monies (e.g. loans) to perpetuate the scam. Victims would only realise they had been scammed after they discover that their Telegram account is no longer under their control or when the loan is not returned. In some cases, the scammers would have access to information, such as photographs or videos, in the victims’ Telegram chats. The scammers would then use the information to extort monies from victims and their contacts.

4 The Police and the Cyber Security Agency Of Singapore would also like to advise members of the public to adopt the following precautionary measures:

a) **ADD** – Add the ScamShield App and set security features (e.g., enable two-factor (2FA) or multi-factor authentication for banks, social media, Singpass accounts; set transaction limits on internet banking transactions, including PayNow)

b) **CHECK** – Check for the scam signs with official sources (e.g. ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot, call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg).

c) **TELL** – Tell authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately. Block and report the sender to Telegram. If your Telegram account has been compromised, report this to Telegram Support and inform your family and friends so that

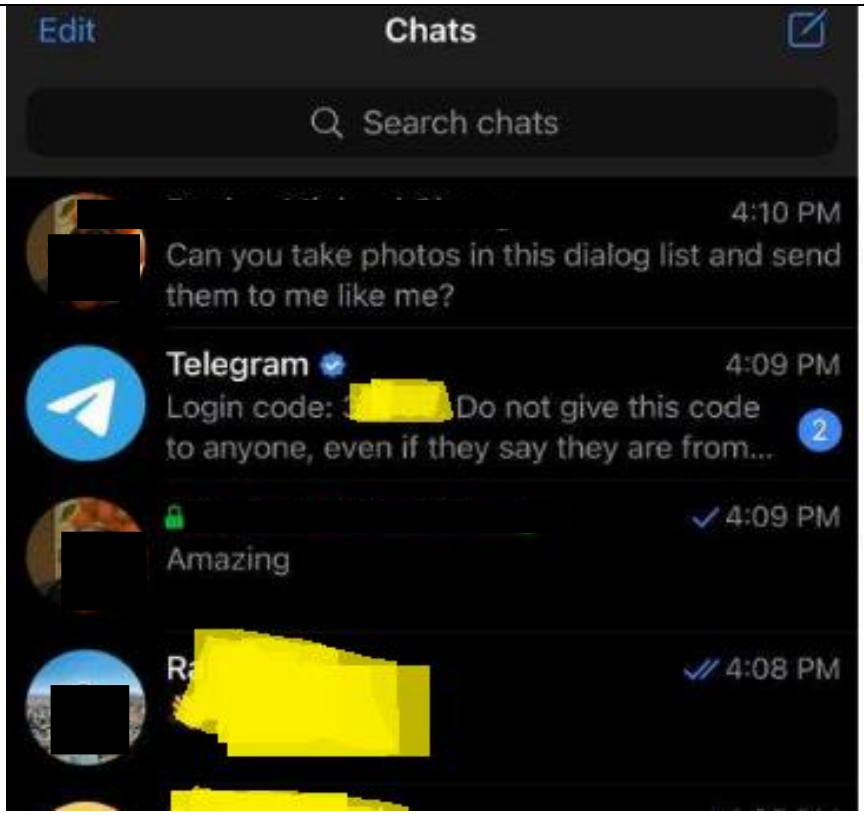
they do not fall prey to scammers who may use your Telegram account to impersonate you. Additionally, you are advised to report the Telegram takeover incident to SingCERT via the online incident reporting form at https://www.go.gov.sg/singcert-incident-reporting-form.

5 If you have any information relating to such crimes or if you are in doubt, please call the Police Hotline at 1800-255-0000, or submit it online at www.police.gov.sg/iwitness. All information will be kept strictly confidential. If you require urgent Police assistance, please dial '999'.

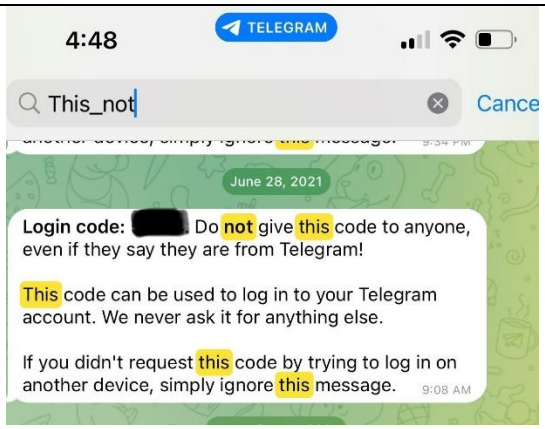
6 For more information on scams, members of the public can visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688. For more information on securing your Telegram account, members of the public can visit https://www.csa.gov.sg/alerts-advisories/Advisories/2022/ad-2022-013 for more information. Fighting scams is a community effort. Together, we can *ACT* Against Scams to safeguard our community.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
31 AUGUST 2023 @ 1.20 PM

Annex A

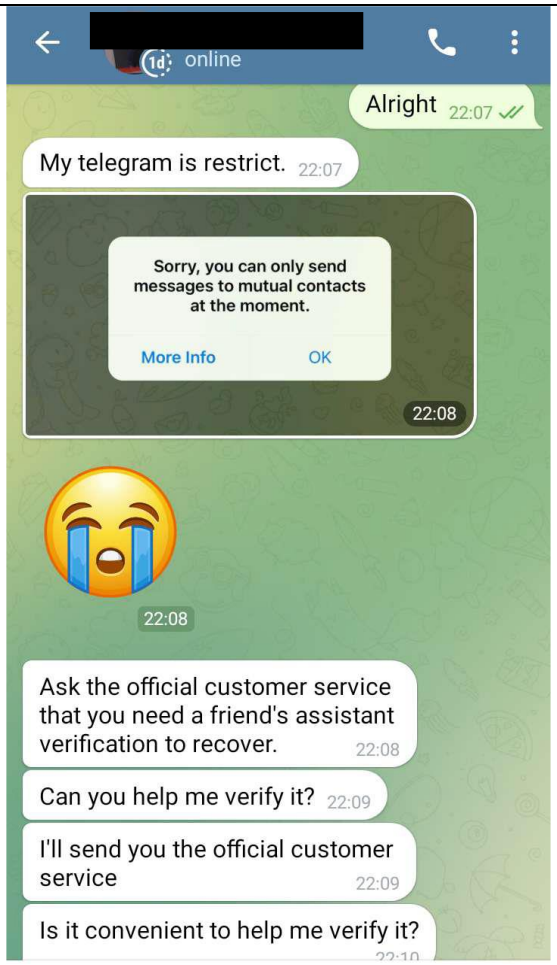
MO (i): Victims are added into a secret chat by scammers pretending to be a known contact of the victims. Scammers will then ask for a screenshot of the victims' Telegram chat history. Unknown to victims, the screenshot will reveal a Telegram generated login code because the scammers will simultaneously trigger a Telegram login code for the victim's Telegram account.


MO (ii): Victims are asked by the scammer pretending to be a known contact to assist in locating someone on Telegram.



Screenshot of Telegram login code after searching username 'this_not'

MO (iii): Victims are asked to help verify or unblock the Telegram account of the known contact that has been restricted.



MO (iv): Victims are asked by the known contact to secure a free Telegram membership.