Beware of Phishing SMS Messages Purportedly Issued by HA Go / eHealth Claiming "Medical Protection Plans Are Expiring; Automatic Charges Are Imminent"

The Anti-Deception Coordination Centre has received multiple reports of fraudulent SMS messages purportedly from "HA Go" or "eHealth". Scammers claim that the trial period of "Voluntary Health Insurance Scheme", "Greater Bay Area Hong Kong and Macao Medical Protection Plan", "Hong Kong and Macao Medical Protection Plan" or "Cross Boundary Medical Protection Plan" subscribed to by the victims has expired, and that monthly charges will be incurred. They also provide a phone number to lure victims into calling back.

Recent victims include a healthcare professional and a university lecturer. The former followed instructions to enter credit card details on a fraudulent UnionPay website and subsequently suffered unauthorised transactions exceeding HK$6,000. The latter was deceived into believing that a bank transfer was part of a "cancellation procedure" and lost nearly HK$340,000.

The Health Bureau and the Hospital Authority (HA) have solemnly clarified that they have never sent the relevant SMS messages and have reported the matter to the Police. Both eHealth and the HA are registered in the SMS Sender Registration Scheme. All official SMSs will bear the prefix "#" in the SMS Sender ID (e.g. #HA Go or #eHealth), enabling members of the public to verify the identity of the senders. In cases where the HA requires contact with the public by phone, a staff member will place the call and

provide relevant information to verify their identity. The HA is gradually adopting 18285 or 18286 as the prefix for its caller ID display numbers.

Common Defrauding Tricks:

- Sending bulk fraudulent SMS messages claiming that medical protection plans are about to expire and that charges will be incurred, thereby luring victims into calling designated phone numbers.
- Impersonating customer service officers and instructing victims to log in to fraudulent websites and input banking/credit card information to "cancel membership".
- Conducting unauthorised credit card transactions or transferring funds from victims' accounts.

ADCC's Five Reminders:

1. Official SMS messages must include a "#" prefix (#HA Go / #eHealth). Be vigilant of any message without "#"!
2. Do not click on hyperlinks embedded in SMSs, call unknown numbers, or provide personal/banking information on suspicious websites.
3. Scammers may speak fluent Cantonese and even initiate video calls to "guide" victims through fund transfers. Do not trust them.
4. Claims such as "trial period expiring" and "automatic charges imminent" are common phishing tactics. Stay alert upon receiving such messages.
5. If you have provided information to suspicious messages, contact your bank immediately to mitigate losses and report to the Police.

Our Advice:

- Do not click on hyperlinks embedded in suspicious SMSs or call the numbers provided;
- You may enter suspicious information on "Scameter" of CyberDefender or "Scameter+", the mobile app of "Scameter", for security check in addition to seeking verification from relevant organisations;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.