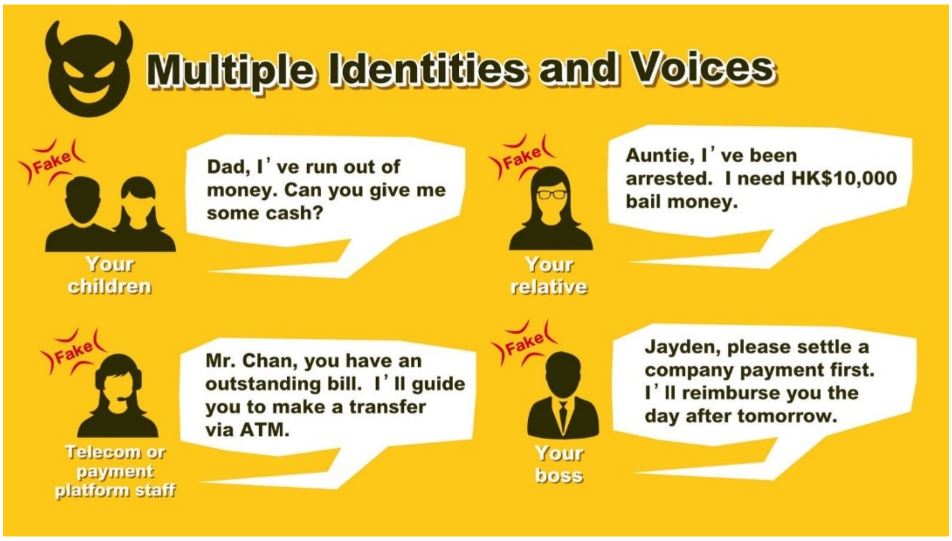
25th September 2026

Beware of "Guess Who" scams and phishing SMSs impersonating government healthcare platforms

Stay with Trusty, Stay Safe from Scams! As BOCHK's Anti-Fraud Ambassador, "Trusty" is here to assist you in staying alert and safeguarding your wealth. To protect your assets, Trusty has compiled the following tips based on recent fraud prevention information provided by the Hong Kong Police Force to help you prevent "Guess Who" scams and phishing SMS messages impersonating government healthcare platforms. Please stay alert and vigilant.

Beware of "Guess Who" Scams: Stay Alert to Any Request for Money Transfers, No Matter How Familiar the Caller Sounds!



The Police have recently received multiple reports of “Guess Who” scams, cases are on the rise. Elderly victims have suffered losses ranging from several thousand to tens of thousands of dollars. Many elderly individuals, with limited exposure to anti-scam information, believe callers simply because the voices sound familiar.

Three Common Scam Tactics:

1. **Scripted Approach**
   - After illegally obtaining personal information, scammers fabricate identities, invent excuses for transfers, and may even mimic voices
   - They contact victims via phone/messaging apps to request money transfers

2. **Account Takeover**
   - Scammers hijack victims’ messaging accounts and review chat histories to learn about contacts and relationships
   - They then request money transfers from the victim’s contacts via the compromised account

3. **Cold Call Deception**
   - Scammers make casual phone calls without revealing their identity, tricking victims into guessing who they are
   - Once the victim makes a guess, the scammer immediately assumes that identity

Recent Cases:

(1) A retiree received a call from a scammer posing as "a staff member of a law firm", claiming that the victim's husband had been involved in a traffic accident last year (the accident was genuine, and the scammer had unlawfully obtained the victim's personal data). The scammer stated that compensation matters were being handled and demanded an upfront "handling fee" of HK$20,000. The victim transferred the money without verification and was defrauded.

(2) An elderly person received a call from a scammer claiming to be her "daughter" who had recently changed her phone number. Due to the similar voice, the victim did not suspect anything. The following day, the scammer called again, claiming to be short of money and asked the victim to bring cash to a designated housing estate for collection. The victim complied and met a middle-aged man who claimed to be collecting money on behalf of the "daughter." After calling the scammer to confirm, the victim handed over the cash and was defrauded, losing approximately HK$35,000.

(3) An engineer received an instant message from someone claiming to be his "cousin", stating an urgent need for HK$12,000 and promising repayment in two days. As the victim was busy with work, he transferred the money to an unfamiliar bank account without further verification. The scammer later requested an additional HK$80,000. The victim became suspicious and attempted to call his cousin via instant messenger, but there was no answer. The scammer then sent a voice message urging the transfer again. Fortunately, the victim remained alert and contacted his cousin directly by phone, discovering that the Instant messaging account had been hacked.

(4) A scammer imitated the voice of a retiree's "nephew" and claimed to have been detained by the police, urgently requesting HK$10,000 for bail. Believing the voice to be genuine, the victim followed instructions to scan a Payment QR code at a convenience store to make the transfer. Later that day, the victim contacted his niece and discovered it was a scam, resulting in a loss of approximately HK$6,000.

(5) A scammer posing as a telecommunications company customer service officer called a restaurant worker, falsely claiming that the victim owed HK$250 and would face a penalty of HK$5,000 if not paid immediately. Believing the claim to be true, the victim followed instructions to transfer money via an ATM while remaining on the call throughout. After transferring HK$10,000, the scammer demanded a further HK$50,000. The victim became suspicious and promptly reported the case to the police.

Police Advice:

- When receiving urgent requests for money transfers, verify the caller's identity regardless of familiarity or voice similarity. Confirm by calling back directly or meeting in person.
- Scammers often collect your personal and family information in advance, then impersonate acquaintances to make their approach more convincing.
- Be highly cautious if asked to transfer money to unfamiliar bank accounts.
- For elderly persons without online banking, scammers may suggest that a "friend" or "lawyer" collect cash on their behalf. Do not comply.
- Always stay calm and verify any request involving money. Never rush into making transfers.
- Show care for elderly acquaintances and share anti-scam information regularly.
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

<u>Beware of Phishing SMS Messages Purportedly Issued by HA Go / eHealth</u>

The Police 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 financial services institution website and was immediately defrauded of over 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 (HHB) 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 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 or credit card information to “cancel membership”.
- Once the scammers obtain personal and/or banking information, they immediately conducting unauthorised credit card transactions or transferring funds from victims’ accounts.

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 or 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 personal or banking information to any suspicious third party, please contact your bank immediately to freeze the relevant accounts and minimize losses, and report it to the Police.

Police Advice:

- Do not click on hyperlinks embedded in suspicious SMSs or call the numbers provided;
- Apart from verifying with the relevant organisaion, the public can also enter suspicious information on “Scameter” on CyberDefender website or “Scameter+” mobile app for verification;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

Bank of China (Hong Kong) Limited