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

16 January 2026

Beware of scams involving impersonating officials and fraudulent investments

Based on the information from the Hong Kong Police Force, following are some anti-fraud tips for scams involving impersonation of officials and social media investment schemes. Please stay alert and vigilant.

Disguised Police with Fake Uniform Trap: International Postgraduate Loses Over HK$1 Million

Recently, an international postgraduate student was deceived by a disguised police officer who wore fake uniform and presented his fake "Police officer ID number" during a video call. In fact, presenting fake police uniforms and arrest warrants are common tactics used in scams! Remember that Mainland Public Security Bureau Officer will not call you in Hong Kong to handle cases, nor will ask you to pay "guarantee fees".

Recent Case

The victim, who is a postgraduate studying finance in Hong Kong, received an unknow call in August. The caller claimed that the phone number registered under the student's

name in Chinese Mainland was involved in a fraud case and demanded the victim cooperation in an investigation. The call was then transferred to a person who identified themselves as being from the “Xiamen Municipal Public Security Bureau”.

During the process, the scammer not only stated an “Officer ID Number” but also initiated a video chat to gain the victim’s trust. The victim believed them and made multiple transfers for “fund verification” and stayed in contact for regular updates.

Finally, the victim realised he had been scammed at the end of October. After reading online anti-fraud information, by which time he had lost over HK$1 million.

Deception Statistics

As of September, there have been 1,711 deception cases involving university students, with total losses reaching HK$180 million. Among these, local students lost approximately HK$16 million to telephone deception, while mainland students lost around HK$87 million.

Police Advice

- If the caller claims to be a "Mainland Public Security Bureau Officer" hang up immediately.
- Remember: Mainland Public Security Bureau Officers or law enforcement agencies will not call you in Hong Kong to handle cases.
- Mainland Public Bureau Security officers will never ask you to pay a "guarantee fee" or provide banking details and passwords.
- Do not disclose personal information, including your ID number, bank account details, etc.
- Even if the strangers who send you messages are able to tell your information, it does not mean they are genuine law enforcement officers. Scammers can obtain the public personal information by unlawful means.
- If you suspect that you have fallen prey to a scam, please call the "Anti-Scam Helpline 18222" for enquiries.

Social Media Becoming Hotbed for Scams:
Fake Investment Expert Advertisement, and Scammers Adding People to Investment Groups

When using social media or instant messaging software in daily lives, citizens can easily fall into scam traps due to carelessness. For example, by curiously clicking on a scam advertisement or being added to an instant messaging chat group by scammers. In some cases, victims have lost up to millions of Hong Kong dollars.

Reminder from the Hong Kong Police Force Anti-Deception Coordination Centre (ADCC): Scammers are extensively utilizing social media advertisements and instant messaging software to approach potential victims. Their tactics are constantly evolving, making them difficult to distinguish from the genuine article. Citizens should enhance their vigilance and be particularly wary of content from social media and instant messaging software.

Common types of investment scam advertisements on social media

Type 1:
Impersonating an Investment Platform
Case example: The victim saw an investment advertisement on a social media platform that claimed to be from a well-known securities firm. After clicking on it, he/ she were automatically added to a chat group named "Hang Seng Index Pointers". Scammers frequently shared investments tips in the group, and lured the victim to make investments on a designated fraudulent investment platform. Deceived by the cases of gaining profit shared by the other group members, the victim believed them to be true and continuously added funds to invest, ultimately losing as much as HK$950,000.

Type 2: AI Investment Scams
Case example: The victim mistakenly trusted an advertisement on a social media platform that promoted "AI-Powered Coaching" in making money through investment. After clicking on it, he/ she was added to an investment group named "Hong Kong-US Stocks". There were many members in the group, and one recommended an investment platform which claimed to offer trading discounts to the victim. The victim followed the instructions of the platform's customer service and made multiple transfers to designated accounts. He/ she only realised he/she has been scammed when the investment account was frozen and withdrawals became impossible, resulting in a loss of over HK$1.2 million.

Type 3: Investment Tips

Case example: The victim saw an advertisement on a social platform that claimed to provide investment opportunities with "Stable Investment and Stable Dividends". The victim clicked on the advertisement and entered a chat window of an instant messaging software, he/ she expressed a desire to receive investment tips. However, scammers claimed that reservation is needed and induced him/ her to join another investment chat group, where a "mentor" would share stock tips every day. The victim believed the information and clicked the link provided by the "mentor" to registered an account. The victim also made multiple transfers to the scammer's designated account, resulting in a loss of over HK$1.2 million.

Type 4: Impersonating Celebrities

Case example: The victim was attracted by an advertisement on a social media platform that impersonated an investment expert. Upon clicking on it, an instant messaging chat window opened. The other party claimed to be an investment expert and offered to share investment knowledge, but required a deposit first. The victim made multiple transfers as instructed and resulting in a loss of over HK$4 million.

Case of Instant Messenger Scam Groups

Case example: A victim was added to an investment chat group that had over a hundred members. The group administrator posted daily investment tips and members uploaded screenshots of "profits". Later, the administrator privately messaged the victim and recommended him/ her to use a specific investment platform. The victim followed the instructions, making multiple transfers to designated bank account. The victim realised he/ she had been scammed until he/ she was asked to pay a deposit when withdrawing money, with a loss of HK$1 million.

Three Steps to Avoid Being Added to Instant Messenger Scam Groups

Investment scams are rampant. The ADCC advises the public to make good use of instant messenger privacy settings to avoid being added to scam groups.

Using WhatsApp as an example, here are the setup steps:

1. Tap "Settings"
2. Tap "Privacy" > "Groups"
3. Select "My contacts"
4. If prompted, tap "Done"

After you complete the above steps, only contacts in your phone's address book can add you to groups, you will be less likely to fall for scams.

Police Advice

- Do not hastily believe investment opportunities offered on social media and instant messaging applications;
- You are advised to make investment through registered investment institutions. You may check out the public register of licensed persons and registered institutions on the web page of the Securities and Futures Commission;
- Stay alert and do not rashly believe the so-called "investment experts" you meet online;
- Do not hastily click on hyperlinks, download mobile applications, log on to any suspicious websites or download any attachments;
- The bank accounts provided by scammers usually belong to individuals or third-party companies, with names different from the trading platforms';
- You may enter suspicious phone numbers, URLs or transferees' account numbers on "Scameter" of CyberDefender or "Scameter+", the mobile application 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.

Bank of China (Hong Kong) Limited