Defrauding Tricks

Many victims in Hong Kong have fallen prey to scams through social media or instant messaging applications. Some clicked on fraudulent advertisements on Facebook and some were added to scam groups on WhatsApp, with some suffering losses worth millions of dollars.

Reminder from the Anti-Deception Coordination Centre (ADCC): Scammers are extensively using social media advertisements and groups of instant messaging applications to target potential victims. Members of the public are advised to be particularly cautious about contents published on social media and instant messaging applications such as Facebook and WhatsApp.

Below are some common types of fraudulent investment advertisements on Facebook:

Type 1: Bogus investment platforms

Case example: A victim saw an advertisement purportedly from Futubull on Facebook. After clicking on it, they were automatically added to a WhatsApp group named “Hang Seng Index Pointers”. The group frequently shared investment tips, but all transactions were conducted on the same fraudulent investment platform. Tempted by members’ shares of making handsome profits, the victim made multiple deposits and ended up losing HK$950,000.

Type 2: AI investment

Case example: A victim saw a Facebook advertisement promoting AI-powered coaching in making money through investment. After clicking on it, they joined an investment group named "Hong Kong-US Stocks". The group had up to 100 members, one of whom recommended an investment platform to the victim, claiming that it offered discounts on stock purchases. Following instructions from customer service, the victim made multiple transfers to designated accounts. It was only when the account was frozen and withdrawals became impossible that the victim realised they had been scammed, by which time they had lost over HK$1.2 million.

Type 3: Investment tips

Case example: The victim was attracted by a Facebook advertisement promoting "stable investment, stable dividends". They clicked on it and a WhatsApp chat window popped up. After they expressed interest in stock tips, the other party immediately replied that an advance reservation was required and provided a link to another chat group where "mentors" shared daily stock tips. Wrongly believing it to be true, the victim clicked on the link to create an account and made multiple transfers to the scammer's account, ending up losing over HK$1.2 million.

Type 4: Impersonating celebrities

Case example: The victim was attracted by a Facebook advertisement posted by a bogus investment expert. They clicked on it and a WhatsApp chat window popped up. The other party claimed to be an investment expert and offered to teach the victim how to make money, but required a deposit up front. Following the scammer's instructions, the victim made multiple transfers and ended up losing over HK$4 million.

WhatsApp scam groups

Case example: A victim was added to an unfamiliar WhatsApp group with up to 100 members. The group administrator shared stock tips every day. Some members posted screenshots showing profits they claimed to have made from following the tips. The administrator later sent private messages to the victim to lure them into using a fraudulent investment platform and making multiple transfers to designated bank accounts. After some time, the victim tried to withdraw money but failed. They were even asked for deposits. Only then did the victim realise that they had been scammed. They ended up losing HK$1 million.

[Strengthen anti-scam protection on mobile phones] Three steps to avoid being added to WhatsApp scam groups

Investment scams have been rampant. The ADCC advises members of the public to make good use of WhatsApp's privacy settings to avoid being added to scam groups.

Use the following WhatsApp tips now:

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. Since strangers will not be able to add you to groups directly, you will be less likely to fall for scams.

Our 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.