LCQ14: Combating online and telephone frauds

Following is a question by the Hon Kenneth Leung and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (November 15):

Question:

It has been reported that the number of online and telephone frauds has been increasing in recent years and, among them, the number of frauds committed through instant messaging applications and the hijacking of other people's accounts has increased drastically in recent months. In this connection, will the Government inform this Council:

(1) of the following information on online and telephone frauds in each of the past three years: the number of reports and requests for assistance received, the nature of the cases, the age distribution of the victims, and the amount of defrauded money involved;

(2) of the number of frauds in the past three years involving the use of groups on instant messaging applications or the hijacking of other people's accounts, as well as the number of victims, the amount of loss and the age distribution of the victims in such cases;

(3) as the Police have pointed out that there has been a surge in the number of frauds committed through hijacking the accounts of WhatsApp, an instant messaging application, in recent months, of the measures put in place by the authorities to step up efforts to combat such frauds; whether the authorities have immediately stepped up publicity (e.g. in television programmes and on different media platforms) targeting members of the public of different age groups (including the elderly and young people), so as to raise the public's vigilance of such frauds;

(4) as there are views that quite a number of online frauds are related to fraudsters placing links to fraudulent websites at the top of Internet search engines by means of sponsorship or advertisement, but currently Internet search engine companies are not required to take up any responsibility in this regard, whether the authorities will consider enacting legislation to regulate the contents of advertisements placed on Internet search engines and require such companies to take up the relevant responsibilities for the frauds involved in the advertisements placed on their Internet search engines; if not, of the reasons for that; and

(5) whether it will consider enhancing the functions of "Scameter+", a mobile application launched by the Police, including expediting the updating of the database and adding functions such as blocking risky calls and links, so as to strengthen the protection of members of the public against frauds?

Reply:

President,

With the global trend of Internet proliferation, many countries and regions have seen a significant increase in fraud cases in recent years. The Police are very concerned about the situation and have been adopting a multipronged approach, through enhanced law enforcement measures, publicity and education, multi-agency co-operation, intelligence analysis as well as cross-boundary collaboration, to combat all types of frauds and to enhance public awareness in full force.

In consultation with the Commerce and Economic Development Bureau and the Police, the reply to the Member's question is as follows:

(1) The number of online and telephone fraud cases received by the Hong Kong Police Force and the amount of losses incurred from 2020 to September 2023, with a breakdown by nature of the cases, are set out in Annex 1. The Police do not keep figures on the number of reports and requests for assistance or maintain a statistical breakdown on the age of victims.

(2) In general, cases involving the fraudulent use of accounts on social media, online payment facilities, emails, etc., are collectively defined as "unauthorised access to online service accounts" cases, a category under technology crime statistics. Scams involving losses due to fraudulent use of accounts are included under this category. In view of the recent surge in frauds committed through hijacking of instant messaging application accounts, the Police have incorporated the figures of such fraud cases into "unauthorised access to online service accounts" for statistical purposes since August this year. The number of "unauthorised access to online service accounts" cases received by the Hong Kong Police Force from 2020 to September 2023 and the amount of losses incurred are set out in Annex 2. The Police do not maintain any statistical breakdown on the number and age of victims.

(3) & (4) In the light of frauds perpetrated through instant messaging applications, social media platforms and search engines, the Office of the Communications Authority, the Police and major telecommunications service providers jointly set up a designated working group in early September last year. The working group is dedicated to devising and introducing different measures from the perspective of telecommunications services with a view to combating fraudulent messages transmitted through telecommunications networks. Among others, telecommunications service providers have established a liaison protocol with the Police in September 2022. Based on the deception records and information provided by the Police, telecommunications service providers can block users from accessing suspicious websites. By analysing the reports made by members of the public, the Police have so far assisted the telecommunications service providers in successfully intercepting more than 5 300 website links involved in fraud cases.

In recent months, the Police have noticed a surge in the number of account hijacking cases involving instant messaging applications (e.g. WhatsApp), and have stepped up efforts to combat the frauds on various fronts. Fraudsters perpetrate the crime by placing advertisements of false WhatsApp websites in search engines, with "WhatsApp" as the keyword, in order to deceive members of the public into logging in the false websites and then obtain their account information. In this regard, the Police have promptly alerted telecommunications service providers to intercept the relevant websites, and have requested the search engines and overseas authorities concerned to remove the false WhatsApp website advertisements.

As regards publicity and education, the Police have been adopting a multi-channel, extensive publicity strategy to heighten public awareness against fraud. Targeting frauds committed through hijacking of instant messaging application accounts, the Police have enhanced publicity via various channels such as their "CyberDefender" website and Facebook. Among others, relevant anti-fraud messages have been disseminated weekly on social media platforms since this September, and the Cyber Security and Technology Crime Bureau (CSTCB) conducted a major press interview in this October. At the press interview, fraudsters' modus operandi of hijacking instant messaging application accounts was demonstrated, and a victim of such fraud was arranged to share his personal experience of falling into the fraudster's trap as well as to advise the public on ways to prevent their accounts from being hijacked.

In October this year, the CSTCB issued a "Letter to Parents" titled "Online account hijacking" through the "CyberDefender" website, schools, as well as Crime Alerts Network Database of the Crime Prevention Bureau, discussing the relevant modus operandi and advising parents on how to prevent their children's accounts from being hijacked. Meanwhile, we call upon members of the public who have received suspected fraudulent messages via online platforms and services to block or report them through the functions provided by the respective platforms. They should also report the suspicious links to the Police so that telecommunications service providers can prevent users from accessing the websites based on the Police's investigation results.

The Government will continue to closely monitor the trend of fraud cases and review fraud combating measures and strategies from time to time, so as to enhance protection for the public.

(5) Since its launch in October 2022, "Scameter" has seen continuous enhancements to its functions. So far, it has recorded a total of more than 1.8 million searches and issued more than 280 000 alerts on frauds and cyber security risks.

The Police will continue to optimise the functions of the application and is planning to incorporate automation elements, including issuing alerts when users browse suspicious websites and receive suspicious calls, to help members of the public identify suspicious calls and websites. To further enrich the content of its database, the Police will also introduce a public "reporting" mechanism for "Scameter+" early next year for members of the public to report suspicious calls or websites through the application.

Besides, the Hong Kong Monetary Authority will launch the first phase of a "Suspicious Indicator Alert Mechanism" at the end of November this year. Under the mechanism, the Police's "Scameter" will be connected to the Fast Payment System (FPS) platform. During online fund transfer via FPS, the matching function of the database can identify payees whose information is related to scam reports. In such cases, an alert message will appear on the confirmation page to ask the depositor whether or not to proceed with the transaction. With this mechanism, users can save the procedure of inputting suspicious mobile phone numbers and other information into the "Scameter" for verification, and alerts can hence be issued to members of the public in a more direct manner.