LCQ7: Cracking down on phishing scams

Following is a question by Prof the Hon Chow Man-kong and a written reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (January 15):

Question:

It has been reported that the transmission of fraudulent messages (phishing SMS) through telecommunications networks has become increasingly rampant in recent years. Some members of the public even received phishing SMS messages sent by fake government departments, and were lured by fraudsters to access fraudulent websites and consequently suffered pecuniary losses. There are views that the incidents reflect that it is necessary for the Government to build an additional barrier to minimise the chances of members of the public being defrauded and to safeguard the image of government departments. In this connection, will the Government inform this Council:

(1) of the total number of fraud cases received by the Police involving phishing SMS in the past two years (including the number of cases involving fake government departments and its percentage), the age distribution of the victims and the loss incurred, together with a breakdown by police region;

(2) whether the Police have stepped up law enforcement actions against phishing SMS in the past two years; if so, of the details (including the number of fraudsters arrested in each of the law enforcement actions, the age distribution of the arrested persons, the modus operandi of the criminals, as well as their trials, convictions and sentences); if not, the reasons for that;

(3) whether the authorities have assessed or compiled statistics on the effectiveness of "Scameter" and "Scameter+" in combating frauds in the past two years, such as the total number of enquiries and reports recorded by such devices, and the number of Call Alert and Website Detection notifications issued to members of the public by "Scameter+"; and

(4) given that there are views that even though the SMS Sender Registration Scheme has built the first barrier for fraud prevention, the chances of members of the public being defrauded will increase significantly when fraudsters have successfully breached this barrier (i.e. members of the public have failed to realise in time the emergence of phishing SMS and mistakenly accessed fraudulent websites), whether the authorities have considered enhancing the functions of "Scameter" or "Scameter+", such as co-operating with various web browser developers or antivirus software developers to share information on suspicious websites, so that when members of the public access (especially through their computers) such suspicious websites, their browsers or antivirus software can immediately block them, thus building a second barrier to prevent more people from being defrauded;

if so, of the details; if not, the reasons for that?

Reply:

President,

Fraud cases have become increasingly serious in recent years and the Government is very concerned about the situation. Phishing scams mentioned in the question generally refers to a crime where illegal elements sent out through SMS messages, emails, voice messages, QR codes, etc. to potential victims en masse, impersonating organisations such as telecommunication service providers, retail chains with membership reward schemes, online payment service providers or even government departments. Alleging that irregularities in the recipients' accounts are detected, bonus points for gift redemption are due to expire or account verification is needed, criminals lure recipients of the messages into clicking on an embedded link and entering a fake website to provide their account login credentials, credit card information, personal information, etc. The criminals will then use such information to make purchases with credit cards or transfer the bonus points out of the recipients' accounts. The Hong Kong Police Force has been making every effort to combat various types of fraud cases, including phishing scams, through intelligence-led enforcement actions and enhancement of public awareness.

ã€€ã€€The reply to the Member's question is as follows:

(1) In 2023, the Police received a total of 4 322 phishing scams reports, involving a monetary loss of 102.4 million Hong Kong dollars. Between January and November 2024, the Police received a total of 2 580 phishing scams reports, a decrease of 1 488 cases (a decrease of 36.6 per cent) when compared with the number in the same period in 2023 (4 068 cases). The monetary loss was 49.6 million Hong Kong dollars, representing a decrease of 48.1 million Hong Kong dollars (a decrease of 49.2 per cent) from the amount in the same period in 2023 (97.7 million Hong Kong dollars). The Government does not maintain statistical breakdowns of other information about phishing SMS-related scams as mentioned in the question.

(2) The Police have been actively combatting phishing scams with an intelligence-led approach. In 2023 and 2024, a total of five large-scale law enforcement operations were carried out. As most of the fraud syndicates were located outside Hong Kong, these operations include joint arrest operations in collaboration with law enforcement agencies on the Mainland. During the operations, the Police smashed a number of fraud syndicates involved in over 900 cases, with a total of 54 persons arrested in Hong Kong and the Mainland (49 were arrested in Hong Kong). In some cases, criminal syndicates made use of false identity documents to register pre-paid phone cards and impersonated customer service staff. The criminals sent SMS messages with embedded links of phishing sites to victims, alleging that the victims' membership points would soon expire, so as to lure them into providing their information. Arrested persons were suspected to have committed offences of conspiracy to defraud, using a false instrument and money laundering, with the amounts

involved exceeding 68.86 million Hong Kong dollars. Hundreds of thousands of phone cards and related computer equipment suspected to be used by the fraudsters in perpetrating the frauds were also seized in the operations.

(3) "Scameter" has yielded remarkable results since its launch in September 2022. As at November 2024, more than 6.48 million searches have been recorded and about 830 000 alerts on frauds and cyber security risks have been issued. Members of the public have also reported over 310 000 suspicious phone calls and over 32 000 suspicious websites through the public intelligence platform of "Scameter".

(4) The Police launched a one-stop scam and pitfall search engine, "Scameter", in September 2022, and its mobile application version, "Scameter+", in February the following year to help members of the public distinguish suspicious online platform accounts, payment accounts, telephone numbers, email addresses, websites, etc., and to provide anti-fraud tips. "Scameter" has undergone various upgrades and expansion of its functions since its launch. "Scameter+" is now equipped with blocking functions. The call alert and website detection functions in the application will automatically identify scam calls and fraudulent websites. If a potential scam or cyber security risk is detected, it will issue a real-time notification, reminding users not to answer the call or browse the website. There is also a public intelligence platform in "Scameter" for members of the public to report scams and pitfalls, thereby further enriching its database.

Furthermore, the Police will pass to telecommunications service providers the information in the database concerning telephone numbers and websites suspected to be involved in fraud cases. Based on the fraud records and information provided by the Police, the telecommunications services providers will block or suspend the services of such telephone numbers, and block users from accessing suspicious fraudulent websites. As at end November 2024, upon the Police's request, telecommunications service providers have successfully intercepted around 25 100 website links involved in fraud cases and blocked or suspended over 8 000 local telephone numbers suspected to be involved in fraud cases.

In addition, the Police work closely with the banking industry and make effective use of the information available from "Scameter". The Suspicious Account Alert mechanism was introduced in November 2023, with the first phase covering transactions via the Faster Payment System. The alert mechanism was further expanded in the second and third phases, which were launched in August and December 2024 respectively, to cover internet banking, physical branch transactions and automated teller machines (including cash deposit machines), hence offering a more comprehensive protection to the public. Before a transaction is confirmed, the mechanism will issue an alert to remind the customer of the associated fraud risk.

The Police will continuously review and enhance the functions of "Scameter", and are planning to explore the room for co-operation with developers of webpage/browser and anti-virus software, with a view to strengthening anti-fraud measures in a proactive manner.