LCQ17: Measures to combat deception cases

Following is a question by Dr the Hon Chow Man-kong and a reply by the Secretary for Security, Mr Tang Ping-keung, in the Legislative Council today (November 22):

Question:

The Police's information shows that 18 743 deception cases were recorded in Hong Kong in the first half of this year, representing an increase of 52.1 per cent compared with the same period last year, and among them, about 75 per cent were online deception cases, with the cases being mainly telephone deception cases, phishing scams, etc. Regarding measures to combat deception cases, will the Government inform this Council:

(1) as it is learnt that many incoming calls from outside Hong Kong have appeared in the community, but the numbers of such incoming calls do not have a "+" sign and are 8-digit Hong Kong telephone numbers, and the callers impersonate government officers to defraud members of the public, of the measures currently put in place by the authorities to combat such deception cases, and whether they will consider adding, for example, a "*" symbol in the calling number display in respect of all telephone calls made by government departments and public organisations, or sending out voice alert in respect of such incoming calls, so as to facilitate identification and verification of incoming calls by members of the public; if so, of the details; if not, the reasons for that;

(2) (i) of the training programmes which the various disciplined services and relevant government departments provide for serving and newly-appointed officers to enhance their capability to combat deception cases, and (ii) whether the various disciplined services and relevant government departments will consider collaborating with post-secondary institutions (especially self-financing institutions) on offering more degree or continuing education programmes which are mainly for upgrading cybersecurity skills, with a view to nurturing more cybersecurity professional talents, thereby tackling the trend of technology-related deception cases becoming rampant; if so, of the details; if not, the reasons for that; and

(3) as the Police indicated at the special meeting of the Panel on Security of this Council on February 14 this year that they had already liaised with a film production company and intended to produce a film with the theme of common deception tactics, of the progress and details of the relevant work, and whether they will draw reference from the Mainland's experience in producing anti-telephone deception films (e.g. No More Bets), with a view to achieving the effect of educating the whole community and going deep into people's hearts; if so, of the details; if not, the reasons for that?

Reply:

President,

The Police have all along been adopting a multi-pronged approach, through enhanced law enforcement measures, publicity and education, multi-agency co-operation, intelligence analysis, cross-boundary collaboration as well as joint efforts with relevant policy bureaux and departments, to combat all types of frauds and to enhance public awareness in full force. In consultation with the Commerce and Economic Development Bureau, the Innovation, Technology and Industry Bureau, the Education Bureau, the Hong Kong Police Force, the Customs and Excise Department, the Immigration Department, the Office of the Communications Authority (OFCA) and the Office of the Government Chief Information Officer (OGCIO), the reply to the Member's question is as follows:

(1) The OFCA has made dedicated efforts to assist the Police in their law enforcement operations to combat fraudulent messages. In this connection, the OFCA, the Police and major telecommunications service providers jointly set up a working group in early September last year. The working group is committed to combating deception cases by devising and introducing different measures from the perspective of telecommunications services. A series of measures are implemented to tackle the problem at source, including:

(i) the telecommunications service providers will intercept phone numbers and websites suspected to be involved in deception cases based on the deception records provided by the Police;

(ii) the OFCA has formulated the Code of Practice on Management of Scam Calls by Telecommunications Service Providers, which requires the telecommunications service providers to monitor calls originated from their networks and systems, and to suspend the telephone services of phone numbers with calling modes suspected to be involved in deception;

(iii) the Real-name Registration Programme for SIM Cards (RNR Programme) has been officially implemented, which enables the law enforcement agencies to detect crimes involving the use of SIM cards, including telephone deception cases. The OFCA has been collaborating with telecommunications service providers to ensure that the RNR Programme is effectively implemented. Among others, telecommunications service providers are requested to conduct sample checks from time to time and follow up on the verification of suspicious pre-paid SIM cards, with a view to assisting the Police in combating telephone deception.

As regards incoming calls from outside Hong Kong as mentioned in the question, telecommunications service providers have, targeting non-local fraudulent calls, intercepted more than 1.4 million suspicious incoming calls with prefix "+852" since end March this year. In addition, starting from May 1 this year, telecommunications service providers have started to send voice alerts or text alerts for non-local incoming calls prefixed with "+852" to alert mobile service users that the calls are from outside Hong Kong, so that

receivers can stay vigilant against those non-local calls with calling numbers masqueraded as Hong Kong phone numbers. Up to September, telecommunications service providers have sent about 18 million voice or text alerts.

It is suggested in the question that consideration can be given to adding a sign of, for example, "*" or sending out a voice alert for incoming calls involving government services and public organisations. There are technical constraints in implementing the suggestion concerned, as calling number displays do not support special characters other than numbers. Moreover, many fraudulent calls are now containing bogus voice messages that claim to be government departments and public organisations. If voice alerts are put in place, they may be exploited by lawbreakers to mislead the public.

The Government will continue to closely monitor the latest trend of deception cases and keep the public informed of the latest modus operandi of the fraudsters. Regarding fraudulent calls claiming to be government departments, the Police have been enhancing public awareness by publicising in a high profile manner that government departments will not ask the call recipients to provide personal or bank information.

All in all, the most effective anti-deception means for members of the public is to remind themselves, their families and their friends to stay highly vigilant at all times. If members of the public receive calls from strangers, regardless of the displayed number, they should stay highly vigilant and should not disclose personal information or transfer money to unknown callers to avoid suffering from losses. If in doubt, they should report the cases to the Police immediately. They can utilise free call-filtering applications available in the market to screen suspicious calls and call-filtering services provided by telecommunications service providers to protect themselves.

(2) Various disciplined services departments will take account of law enforcement needs and regularly provide serving and newly recruited officers with professional training on technology crime investigation, digital forensics and cyber intelligence gathering, including professional certificate courses, regular training courses and internal training materials. In addition, the OGCIO and the information technology (IT) sector will also jointly organise thematic seminars, technical workshops, information security certificate courses, cybersecurity incident response training and cybersecurity summits on a regular basis to enhance the IT security skills and knowledge of IT officers. For details, please refer to the Annex.

As regards the post-secondary education sector, under the principle of institutional autonomy, institutions have the flexibility to develop programmes that meet market needs and adjust the contents and intake places of relevant programmes. In recent years, tertiary institutions have developed different programmes on IT security such as Bachelor of Science in Information Security offered by the Hong Kong Polytechnic University and Higher Diploma in Information Security offered by the HKU SPACE Community

College, with a view to nurturing local talents on information security.

(3) The Police have been adopting a multi-channel, extensive publicity strategy to heighten public awareness against various kinds of deception cases as well as relevant risks relating to computer, cybersecurity, Internet and social media. From time to time, anti-deception messages are updated and publicity programmes on various fronts are devised in response to the latest crime trends. As for multimedia, in view of the wide coverage of television publicity, the Police and TVB have jointly produced a series of ten episodes titled "All-round CyberDefence" in April this year to explore various issues on cybersecurity and technology crime. The latest techniques of different cyber pitfalls are unveiled with real examples and viewed from the perspectives of experts. The Police have also been working with some of the cinemas to arrange for the screening of an anti-fraud publicity video before the showing of movies, so as to remind the public to stay vigilant against deception.

The Police have also launched different types of thematic anti-deception publicity campaigns, such as the "All-round CyberDefence" campaign and the "Anti-money Laundering Month" campaign to promote digital literacy and awareness of anti-deception among the general public. In February this year, the Police launched a mobile application "Scameter+" as a one-stop scam and pitfall search engine, held a large-scale seminar "How to Strengthen Students' Resilience Against Cyber Pitfalls" in collaboration with the Education Bureau for more than 290 principals and teachers across the territory, and launched an account on Xiaohongshu to further expand the coverage of anti-deception publicity work. The Police also regularly launch large-scale thematic anti-deception campaigns under the "Anti-Deception Season" and "Anti-Deception Month". For example, in the third quarter of this year, the Police launched a publicity campaign titled "Don't Click On Embedded Links in SMS messages without Hesitation" targeting phishing scams, invited renowned local musician Harry Ng to write a promotional song "There's no free lunch", and launched a simulation game on online deception. In December this year, the Police will organise a large-scale Winter Market Anti-Scam Charity Run in the West Kowloon Cultural District to promote anti-deception message across the territory.