

LCQ7: Identifying calls from government departments and public organisations

Following is a question by the Hon Duncan Chiu and a written reply by the Secretary for Commerce and Economic Development, Mr Algernon Yau, in the Legislative Council today (May 28):

Question:

It has been reported that telephone frauds have occurred frequently in Hong Kong in recent years and to avoid being defrauded, quite a number of members of the public prefer not answering calls from non-traditional telephone numbers with prefixes of "3" or "5", etc, telephone numbers not found in their phone contacts and without caller numbers. However, there are views pointing out that such calls may also include those from government departments and public organisations, such as public hospitals, the Police and Immigration Department, etc, and refusal to answer these calls may result in wastage and ineffective use of some public resources as well as affect the use of public services by members of the public. In this connection, will the Government inform this Council:

- (1) of the major prefixes of existing fixed-line telephone numbers of government departments, public organisations and public hospitals, and the respective percentages of telephone numbers with the relevant prefixes;
- (2) whether it has examined the actual situation of the effect of frequent occurrence of telephone fraud on the contact made by various government departments and public organisations with members of the public by phone, including the telephone number prefixes which were most affected, the five government departments and public organisations which were most affected, and the estimated number of members of the public who have not been successfully contacted;
- (3) regarding the failure of staff of government departments and public organisations to effectively contact members of the public by their office fixed-line telephones, whether follow-up mechanism and guidelines have currently been put in place, including the circumstances under which the responsible personnel are allowed to follow up using their private mobile phones; if so, of the details; if not, the reasons for that, and whether it will formulate the relevant mechanism and guidelines in the future; and
- (4) whether consideration will be given to reorganise and centralise the allocation of telephone numbers of government departments and public organisations with specified prefixes, so as to facilitate identification by members of the public and reduce the chance of refusal to answer calls?

Reply:

President,

The Office of the Communications Authority (OFCA) has been devising and implementing a series of preventive measures from the perspective of telecommunications services to assist the Hong Kong Police Force (Police) in combating phone deception at the source. In response to the question raised by the Hon Duncan Chiu, having consulted OFCA and the Innovation, Technology and Industry Bureau, our consolidated reply is as follows:

Government departments and public organisations will enter into commercial service contracts with telecommunications service providers respectively based on their own operational needs for suitable telephone services and obtain office phone numbers. In addition, OFCA has established a mechanism to provide designated telephone numbers for government departments or public organisations in need of hotline numbers or communication with the public. Examples include the Government's one-stop service hotline 1823, the Police's Anti-Deception Coordination Centre hotline 18222, the Customs and Excise Department's reporting hotline 1828080, the Immigration Department's service hotline 1868, and the Home Affairs Department's "Care Team" inquiry number 182111. The operational arrangements for these phone numbers and actual interface with the public will be determined by the respective government departments and public organisations in accordance with their mode of operation, service nature and needs for communicating with the public. OFCA does not centrally collect or maintain related data or information.

Currently, government departments and public organisations involve hundreds of thousands of telephone numbers and users, with varying nature and requirements for phone services when communicating with the public. If all government departments and public organisations needed to restructure and be uniformly allocated with telephone numbers of designated prefixes, and massively revamp the existing telephone systems as well as hotline/office phone numbers, the whole process would be complex and time-consuming. In particular, there would be a need to put in place transitional arrangements, and all users should be informed of the updated phone numbers. It could instead cause confusion and inconvenience to the public during such a period. Therefore, the suggestion to uniformly allocate telephone numbers with designated prefixes for all government departments and public organisations may not be the most effective way to prevent phone deception. In fact, the tactics of phone deception are ever-changing. Criminals may use other means to impersonate government calls. In this connection, OFCA will continue to work with the telecommunications industry and the Police to mitigate the risk of phone deception on various fronts, including requiring telecommunications service operators to block/suspend suspected fraudulent phone numbers and websites, intercept suspicious calls starting with "+852", send voice alerts or text messages to all mobile users for overseas calls prefixed with "+852", and play voice alerts for newly activated prepaid SIM cards, so as to assist the public in guarding against suspicious calls and messages.

To enhance the regulation and security of mobile device usage by

government staff members and to effectively mitigate the risk of leaking sensitive government information, the Digital Policy Office has issued the "Practice Guide for Mobile Security" (Guide). Among others, the Guide requires government bureaux and departments, when considering the adoption of mobile devices in their operations, should first assess their needs for mobile devices and evaluate how mobile solutions can support their business operations. In addition, government bureaux and departments should establish a mobile security policy (including specifying the scope of mobile device use, business needs and security requirements) and formulate appropriate procedures to manage the use of such devices.

For privately owned mobile devices, the Guide specifies that, considering the associated security risks and the risk of data leakage caused by device loss, government bureaux and departments should not use privately owned mobile devices for official business in the absence of appropriate protective measures.