LCQ11: Security issues of the use of QR codes

Following is a question by the Hon Jimmy Ng and a written reply by the Secretary for Financial Services and the Treasury, Mr James Lau, in the Legislative Council today (May 22):

Question:

It has been reported that while electronic payment systems whose transactions are conducted by scanning QR codes have become increasingly popular in recent years, this mode of transactions involves certain security risks. For instance, hackers can make use of fake QR codes to trick members of the public into downloading malware, thereby stealing their electronic identities, carrying out overhearing and position tracking, conducting surveillance via their mobile phones, and blackmailing them after stealing sensitive information. In this connection, will the Government inform this Council:

(1) of the respective numbers of cases received by the Police in each year from 2014 to 2018 about, and the amounts of money involved in, the technology crimes concerning (i) thefts of credit card information via the Internet, (ii) hacking of computers for stealing information and (iii) blackmailing by using encryption ransomware; among such cases, the respective numbers of those which involved the use of QR codes;

(2) whether it will consider enacting legislation to stipulate the required format for QR codes (e.g. the inclusion of information for authentication of the provider's identity) to facilitate users to identify the sources of QR codes, if so, of the details; if not, the reasons for that; and

(3) of the targeted measures that the Government will introduce to ensure that adequate information security protection is in place to dovetail with the growing popularity of financial technology applications such as QR codes?

Reply:

President,

In consultation with relevant bureaux and financial regulator, we have prepared a consolidated reply to Hon Jimmy Ng's question as follows:

(1) The number of cases and amounts involved as mentioned in the question and received by the Police between 2014 and 2018 are listed at the Annex. The Police do not maintain the breakdown of technology crime cases involving QR codes.

(2) and (3) The Government has all along through public education reminded

the public to be vigilant in protecting their personal and sensitive data when using Fintech, such as using QR Code technology for payment, in order to reduce the risk of data theft. The Office of the Government Chief Information Officer (OGCIO) has been working closely with the Hong Kong Computer Emergency Response Team Coordination Centre and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force to enhance public awareness and knowledge of information security, including security related to mobile payment services, through different activities such as seminars, talks and competitions. In 2018, the OGCIO also promulgated the security risks and appropriate preventive and responsive measures regarding the use of mobile payment services (Note 1) and QR Code (Note 2).

In addition, banks and stored value facility (SVF) licensees are required to implement adequate payment security measures pursuant to the supervisory guidelines issued by the Hong Kong Monetary Authority. In processing QR code payments initiated by user scanning a QR code with its payment app, a bank or a SVF licensee should verify whether such a code is genuine and valid, and display the payee's name and relevant information so that the user can identify the payee. The public should also check the payee information before making payment with QR code in order to ensure that payment will reach the correct payee.

We will continue to closely monitor the market development and strike an appropriate balance between promoting Fintech innovation and protecting the interest of the public.

Note 1: For more details, please visit:
www.cybersecurity.hk/en/learning-epayment.php
Note 2: For more details, please visit:
www.infosec.gov.hk/english/yourself/carefully.html