

21 October 2020

## **HSBC SURVEY UNCOVERS LINKS BETWEEN FRAUD AND WEAK OWNERSHIP OF PERSONAL DATA**

- \* Over 80 per cent of HK people have been the target of attempted fraud*
- \* Romance and digital payment scams causing the heaviest financial losses*

Over 80 per cent of Hong Kong's population have been the target of attempted fraud. Among these fraud targets, 26 per cent have fallen prey to scams and suffered an average financial loss of HKD3,800, according to the latest HSBC survey. It also highlights the importance for Hong Kong people to take stronger ownership on personal data and stay vigilant against social engineering traps which have become increasingly rampant in the online space.

HSBC launched its inaugural cyber security index in April this year. As part two of the initiative, the latest survey identified the most common scams including digital payments, romance, identity theft, impersonating officials, jobs and bogus calls, and studied how people react to these fraud scenarios.

Unravelling the data, romance and digital payments scams caused the heaviest monetary loss, swindling an average of HKD4,100 (the highest among all fraud scenarios) and HKD2,500 respectively from victims. Overall, 26 per cent of surveyed population were the target of attempted digital payment scams, which eventually victimised 13 per cent of survey respondents, the highest among all fraud categories. When it comes to romance scams, one in three respondents have been the fraud targets, with 7 per cent of surveyed population suffering a financial loss.

**Andrew Eldon, Head of Digital, Wealth and Personal Banking, Hong Kong, HSBC**, said: "The findings align with our observation that Hong Kong people have increasingly adopted a digitised lifestyle, whether it be shopping online or finding a soulmate. The outbreak of COVID-19 has prompted people to spend even more time online, but it also makes them more susceptible to scams, especially those associated with the use of social engineering techniques to manipulate victims and get them to share personal information or make a money transfer."

The survey finds that bogus calls (72 per cent) and scammers impersonating officials (64 per cent) are the top two most common scams in Hong Kong, having tricked over HKD1,000 on average from one in ten of the survey respondents. It is worth noting that social engineering techniques are commonly used in many of the fraud situations, whether it be developing a romantic relationship with victims or exploiting human tendency of obeying authority figures.

While not all respondents have actually suffered from monetary loss, the survey indicated a general negligence among victims, who have put themselves at risk by casually sharing personal and banking related information. To put it into context, a fraudster only needs to collect a combination of personal information – online banking credentials (i.e. username and passwords), recent photos, one-time password (OTP), date of birth, email address and HKID – in order to complete a fraud transaction.

In particular, the survey emphasises that two key pieces of information - online banking credentials and OTP should never be shared with unverified individuals. Sharing either of these can double the risk of fraud. Interestingly, 48 per cent of respondents shared OTP with other parties during the last 12 months, while 38 per cent provided their online banking credentials.

By age categories, Gen Z (18-24 years old) respondents appear to be digitally knowledgeable but more vulnerable to digital payments and jobs scams, in which they have a stronger tendency to share important personal information. Gen Y (25-39 years old) are more prone to romance scams because of their willingness to share HKID, OTP and bank account numbers with their online partner. Gen X (40-55 years old) are more easily victimised by impersonation scams and bogus calls.

**Eldon concluded:** “Fraud is as prevalent as it is preventable. It is important to check the identity of whom you are interacting with and think twice before sharing any personal information or making a money transfer. By offering your information, you will leave your digital footprint and create a weak link for fraudsters to pull social engineering techniques on you. It is also too late for a U-turn once you have initiated a money transfer.”

Conducted in August and September 2020, the HSBC survey covers a sample size of 800 respondents aged 18-55 years old, which is representative of the Hong Kong population in terms of age and gender based on Hong Kong census data.

*ends/more*

### **The Hongkong and Shanghai Banking Corporation Limited**

The Hongkong and Shanghai Banking Corporation Limited is the founding member of the HSBC Group. HSBC serves customers worldwide from offices in 64 countries and territories in its geographical regions: Europe, Asia, North America, Latin America, and Middle East and North Africa. With assets of US\$2,923bn at 30 June 2020, HSBC is one of the world’s largest banking and financial services organizations.

*ends/all*