ANNEX B

MEDIA FACTSHEET

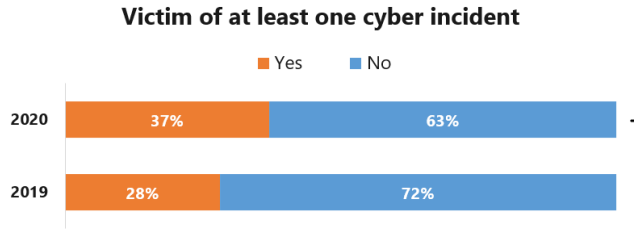
CSA'S CYBERSECURITY AWARENESS SURVEY 2020

The Cyber Security Agency of Singapore (CSA) conducted the Cybersecurity Awareness Survey 2020 over one week in December 2020, polling 1,052 Singapore citizens and permanent residents aged 15 years old and above online to better understand their general attitudes and behaviours towards cybersecurity practices and incidents.

The findings are as follows:

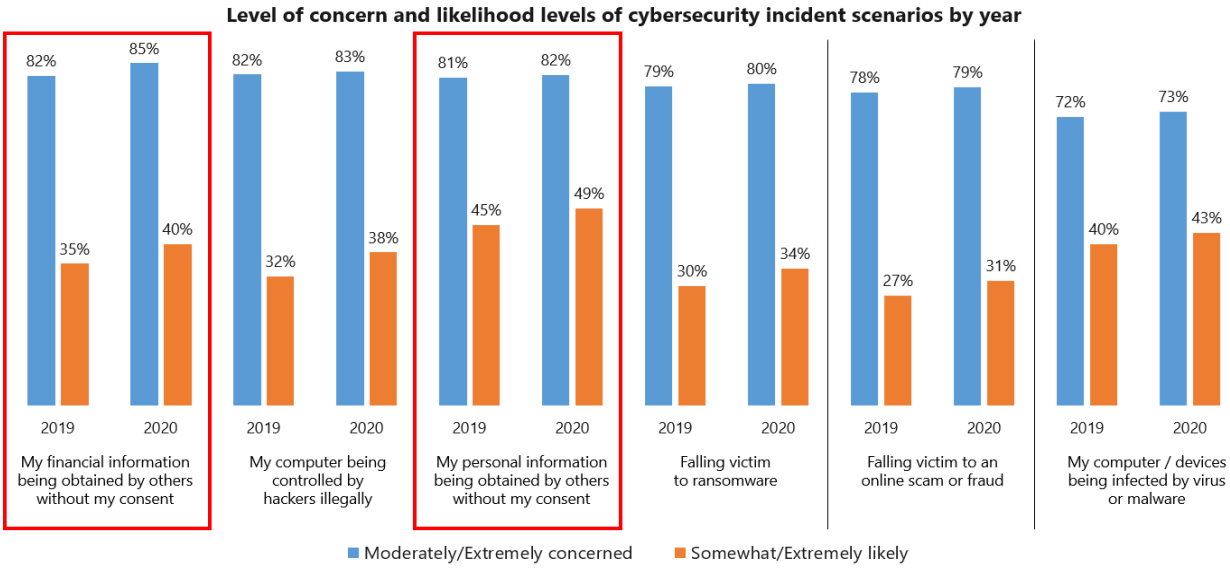
A. KNOWLEDGE OF AND ATTITUDES TOWARDS CYBER INCIDENTS

More fell victim to a cyber incident at least once in past year



The top three most common cyber incidents: (i) unauthorised attempts to access online accounts; (ii) being informed by others that online accounts were used to contact them; and (iii) being locked out of online accounts/files as a result of a cyber incident.

Respondents concerned about cyber incidents but continued to believe that it would not happen to them

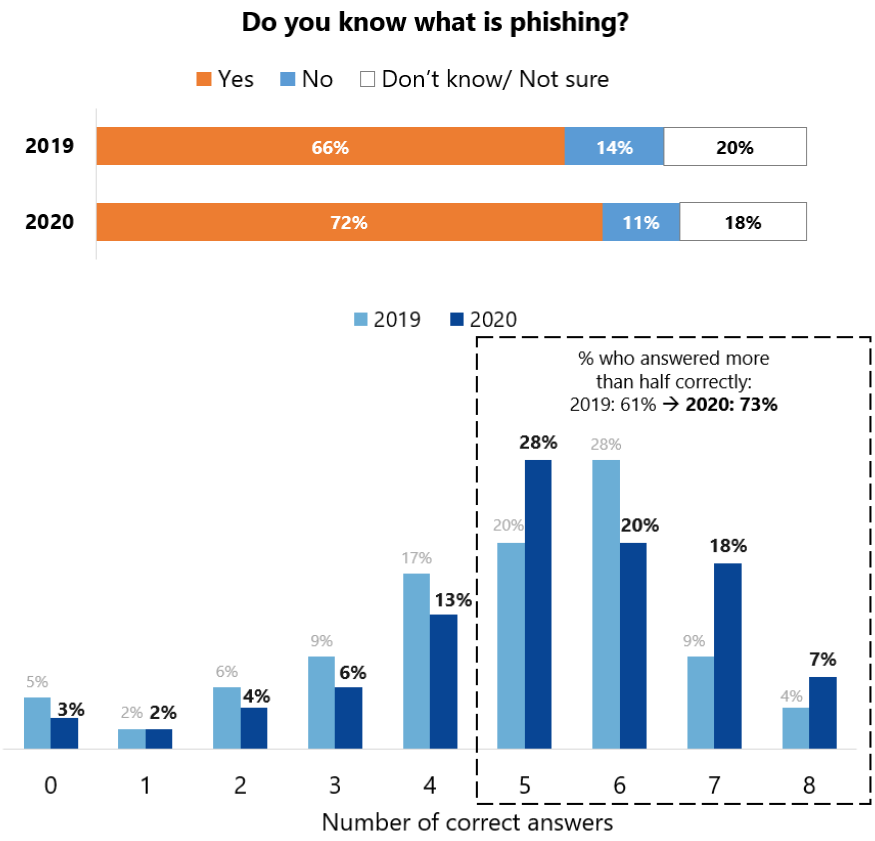


Respondents were polled on their sentiments to six cyber incidents. They continued to show high levels of concern for these cyber incidents, with an increase by 1 to 3 percentage points. 85 per cent of respondents were most concerned about their financial information being obtained without consent, followed by their personal information being obtained by others without their consent (82 per cent).

However, most continued to believe that such incidents would not happen to them. From 2019 to 2020, while a slight increase was seen in respondents' perceived likelihood of various cyber incidents happening to them by 3 to 6 percentage points, respondents thought that these incidents were unlikely to happen to them. For example, while 80 per cent of respondents were concerned about falling victim to ransomware, only 34 per cent felt that there was a likelihood of this happening to them.

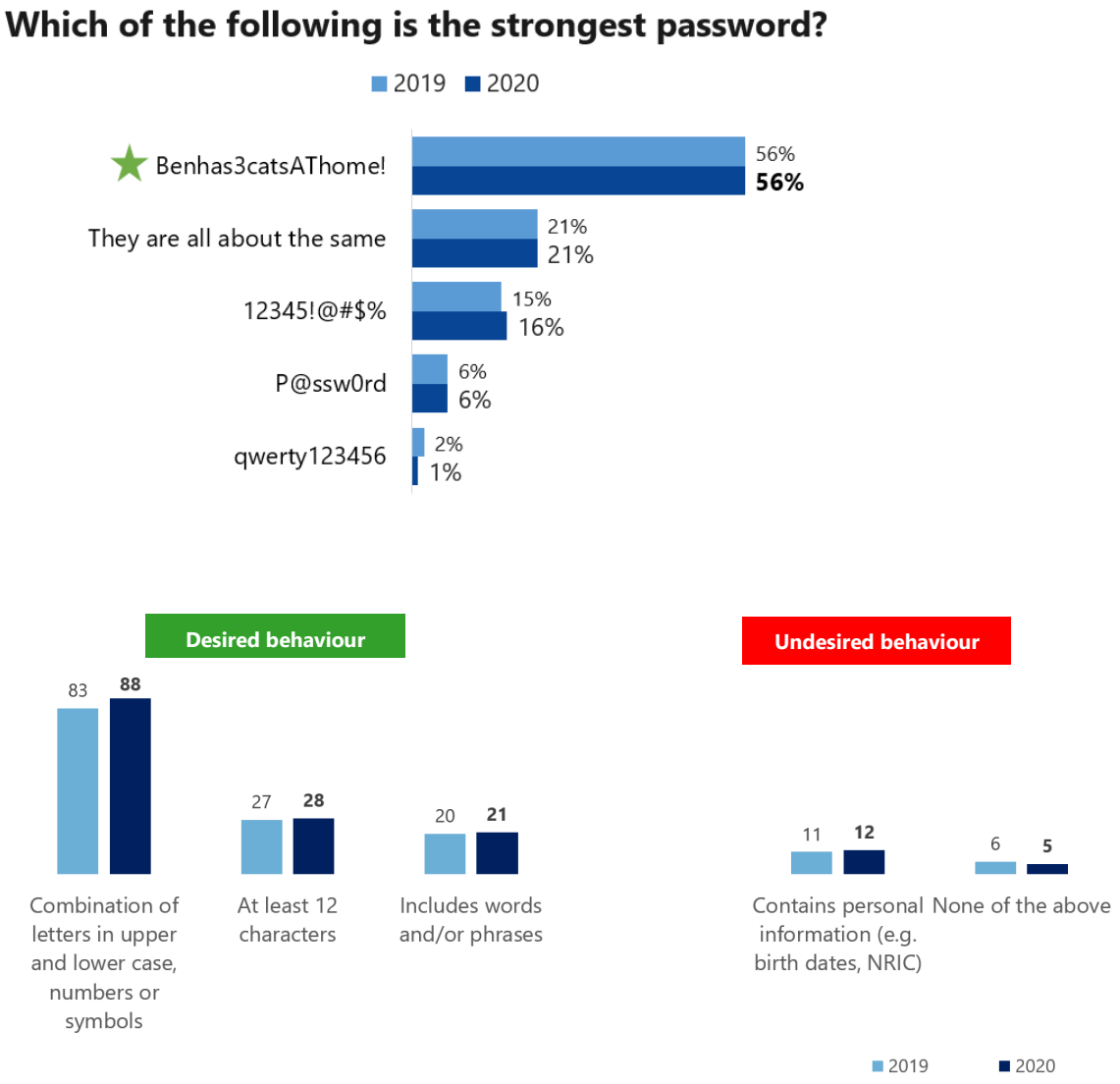
B. AWARENESS AND ADOPTION OF GOOD CYBERSECURITY MEASURES

Awareness of phishing increased



Respondents' awareness of phishing saw an increase, with seven in 10 respondents knowing what phishing was - a six percentage point increase from 2019. Three-quarters of respondents were able to identify more than half of the eight emails correctly, an improvement of 12 percentage points over 2019.

More used a combo of letters in upper and lower cases, numbers and symbols in their passwords

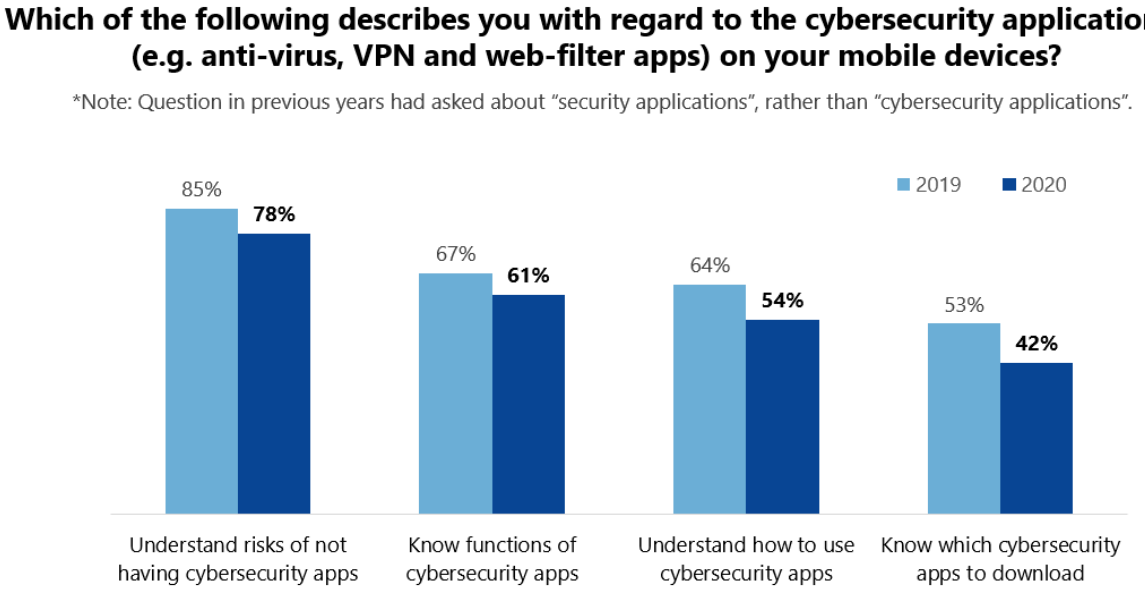


Slightly more than half of the respondents (56 per cent) were able to identify a strong password, unchanged from the year before. Close to nine in 10 respondents used a combination of letters in upper and lower cases, numbers and symbols in their passwords, an increase of five percentage points from the year before.

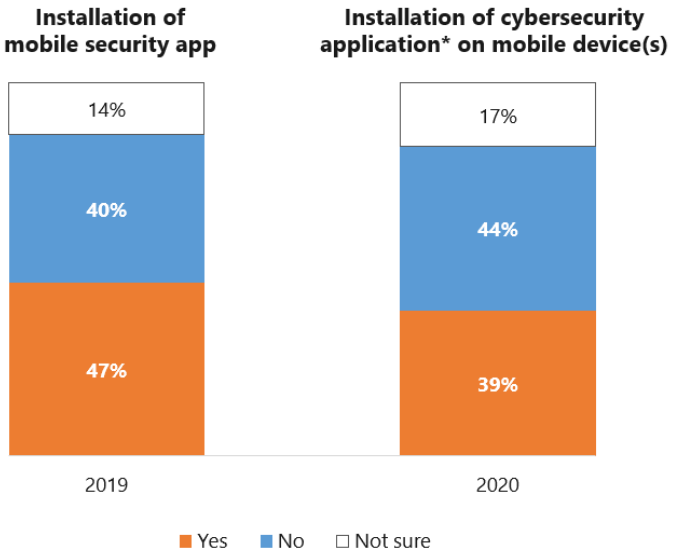
Increase in 2FA activation for personal emails and social media

Overall, no change was seen in the proportion of respondents who activated 2FA for online banking and shopping. About half continued to go without 2FA for their communication accounts (social media, emails, messaging), although there was an increase of 7 per cent and 5 per cent in 2FA activation for personal emails and social media respectively.

Most understood the risks of not having cybersecurity apps, but installation of such apps has to catch up



Installation of cybersecurity apps by year



Close to eight in 10 respondents were aware of the risks of not having **cybersecurity apps**, but only 39 per cent of respondents had installed cybersecurity apps in their mobile devices, a drop from 47 per cent in 2019. A lower proportion of respondents professed to knowing the functions of such apps, how to use them and which ones to download.

###