Source: *The Straits Times,* pA28
Date: 5 March 2022

Public service ambassadors guiding seniors through the use of government digital services at an SG Digital Office in 2020. Recent phishing incidents have dented public trust in digitalisation efforts, say the writers. From the governance perspective, one way to rebuild digital trust is to better articulate the value of digitalisation through national benchmarks that go beyond digital access.
ST PHOTO: LIM YAOHUI

Rebuilding digital trust

Phishing scams like the OCBC one show that going digital is not just about access for all, but giving users, especially the vulnerable, the know-how to use that access wisely

Chew Han Ei and Carol Soon

For The Straits Times

High-profile phishing incidents recently have dented public trust in digitalisation efforts. After news of the phishing scam targeting OCBC Bank customers broke, some seniors were reported to have cancelled their Internet banking accounts.

Following the incidents, Finance Minister Lawrence Wong said financial institutions are expected to improve security measures, such as using artificial intelligence to enhance fraud detection. The Monetary Authority of Singapore is also working on a liability framework for scam losses.

These solutions are targeted at institutional players – but what about the consumers and citizens whose trust in digital banking has been damaged?

Data on victims of scams in Singapore indicate that different segments are susceptible to different types of scams. Young adults tend to fall prey to jobs, investments and phishing scams, while older adults tend to be victims of Internet love scams and social media impersonation scams.

A study by the second author of this commentary found that people aged 60 and above, and those living in one-room to three-room public housing flats, are also more susceptible to false information due to their lower IT literacy.

Having access to devices without having critical digital literacy and cyber-security know-how can bring more harm than good for many segments of society. Closing the digital divide in Singapore through the provision of access and connectivity is only a partial solution.

To eliminate the divide, we have to ensure that those who do not have the skills and ability needed to access and use digital devices and content can do so confidently, safely and effectively. A crucial part of this is rebuilding digital trust.

SINGAPORE-SPECIFIC NEEDS

The rapid transition to digitalisation during the pandemic has also led to the erosion of people's trust in technology.

The World Economic Forum (WEF) estimated that in 2020, there was a 358 per cent increase in malware attacks and a 435 per cent increase in ransomware ones. Last year's Edelman Trust Barometer reported that between 2012 and 2021, global trust in the technology sector dropped from 77 per cent to 68 per cent.

The public has become increasingly suspicious of digital society, and distrust can affect the motivation to adopt technology.

Regrettably, there is no global consensus on how to rebuild digital trust.

To address this, the WEF in November established the Digital Trust Initiative comprising key stakeholders in the technology sector to engender deeper trust in digital spaces. Some early suggestions include adopting more secure and trustworthy technologies to boost cyber security, strengthening privacy protection, creating norms for ethical and values-driven innovation and transparency in development.

However, there are immediate problems that need to be addressed locally.

For the most vulnerable segments in Singapore, public education efforts should be tailored to who they think are trustworthy and what kinds of information sources they trust.

Their awareness of the benefits of tapping digital intermediaries in society such as librarians, the Smart Nation Ambassadors, and trusted family experts needs to be heightened.

Having access to devices without having critical digital literacy and cyber-security know-how can bring more harm than good for many segments of society. Closing the digital divide in Singapore through the provision of access and connectivity is only a partial solution.

The phishing scam targeting OCBC customers is particularly thorny as the perpetrators exploited the consumers' trust in the banking institution, and we need more research to understand people's current behaviours and beliefs about security and privacy. The need to slow down so that people and skills can catch up is poignant for Singapore, which has been at the forefront of digital evolution.

Singapore needs to temper its headlong rush to provide digital access for all. Citizens who have been caught up in the tsunami of digital adoption should be given some space and time to develop online skills and cultivate their trust in the public and private institutions that build and regulate our digital ecosystems.

GOING BEYOND DIGITAL ACCESS

From the governance perspective, one way to rebuild digital trust is to better articulate the value of digitalisation through national benchmarks that go beyond digital access.

While we have data about those who are disconnected, what is missing are metrics and data about the effects of technology on the quality of life.

A clearer articulation of the value of digitalisation for Singaporeans cannot be had without a meaningful set of metrics. Global examples of metrics Singapore can adapt for our needs include the Value of the Internet index by the Economist Intelligence Unit and the Digital Inclusion Outcomes Framework by the New Zealand government.

By connecting digital activities to measured outcomes for citizens, there is transparency in the value that the Government ascribes to digitalisation.

The transparency is elevated when the voices of citizens – especially young people – are considered in the outcomes. This helps build trust in digital initiatives.

MAKING PEOPLE MORE AWARE

One of the first hurdles is that the focus is on universal digital access to devices and connectivity. There is less attention on motivation, higher-order digital skills and "useful use".

This is one of the research highlights in a study we did on the state of digital inclusion in Singapore.

We point out that the digital divide we are attempting to close is actually made up of several divides, such as the motivational (attitudes towards technology); the material (physical connection such as infrastructure and speed) and costs of being connected; skills (the ability to use technological hardware and software, and navigate and use the information available online); and usage (frequency and the type of online behaviour).

In Singapore, the most persistent digital access divides are among seniors with lower education and low-income families. Currently, there is a plethora of schemes and programmes directed at these groups to help them connect digitally.

However, even with connected devices, these groups often do not have the digital skills to benefit from digital opportunities or the motivation to use their connectivity for capital enhancing activities.

As the recent phishing incidents show, access without higher-order digital skills can expose citizens to online harm. We are not wrong in attempting to narrow the digital access gaps – we just need to do this in tandem with efforts to narrow the other digital divides.

When high-profile incidents such as phishing or viral fake news occur, public education is often intensified as a stopgap measure. A more enduring intervention would be to direct public education efforts at elevating the baseline digital literacy of all Singaporeans and demonstrate progress through national benchmarks.

The incidents also demonstrate the fragility of digital trust, and it is imperative that Singapore now directs more focus towards understanding what digital trust means to Singaporeans and fine-tuning current measures to rebuild and sustain trust.

The country's digital plans will be hobbled if citizens cannot even trust the digital banking system to be secure.

stopinion@sph.com.sg

• Chew Han Ei and Carol Soon are senior research fellows at the Institute of Policy Studies, National University of Singapore, and principal investigators at the NUS Centre for Trusted Internet and Community.

Source: The Straits Times © Singapore Press Holdings Ltd. Permission required for reproduction.