Source: *The Straits Times,* pB3
Date: 12 September 2023

An anti-scam advertisement at Newton MRT station. One way to increase digital trust is to improve digital literacy, say the writers. Online users with high levels of digital literacy are better at recognising phishing e-mails and have greater awareness of the existence of malicious actors online. They are more likely to avoid negative experiences online. ST PHOTO: CHONG JUN LIANG

Where to park my bicycle? The mindset needed to beat scammers

Digital trust is hard won and easily lost. Improving literacy remains our best shot at shoring up digital trust.

Chew Han Ei, Carol Soon & Jeanne Tan

Can you put a dollar value to trust? Perhaps.

In Singapore, a phishing scam targeting OCBC Bank users resulted in a loss of $13.7 million and shook customer confidence in digital banking services. Although OCBC later made a goodwill gesture, acknowledging that its response fell short of expectations, the damage was done.

Such episodes, where a digital service fails to function in a consistent and secure manner, can weaken trust in everyday organisations. Users may consequently lose confidence in the product and potentially discontinue usage or refuse to share their personal data.

In recent years, widespread cyberscams, misinformation campaigns, and prominent security and data breaches have eroded people's trust in technology.

The Edelman's 2021 Trust Barometer reported that between 2012 and 2021, global trust in the tech sector has dropped from 77 per cent to 68 per cent and understandably so. Every day, citizens are increasingly wary of new technology that erodes their ability to make a living, artificial intelligence biases that are baked into the information they consume and transgressions against their privacy.

To arrest this decline, stakeholders, including leaders of technology companies and governments, must commit to building more trustworthy technologies, shoring up their defence perimeters and strengthening their security systems.

Even so, better technological solutions are insufficient to rebuild and enhance digital trust – a key finding from our recently published policy review on Digital Trust And Why it Matters.

Digital trust – defined by the World Economic Forum as expectations by individuals that digital technologies, services, and the organisations providing them will protect stakeholder interests and uphold societal values – is the oil keeping the wheels of the economy turning.

Although trust is fundamentally a human quality, current discussions around solutions to preserve digital trust have unfortunately been predominantly technocentric, meaning that they focus on technology to stem the tide against cyberthreats.

Digital trust remains typically defined and evaluated along mechanical dimensions such as cyber security, safety, privacy and transparency. Even the Digital Trust Centre established in 2022 aims to strengthen Singapore's status as a trusted hub in the digital economy by, developing trust technology such as privacy-enhancing technologies that store and analyse data while preserving data privacy through cryptographic algorithms or data-masking programmes.

FOCUSING ON THE HUMAN DIMENSION OF DIGITAL TRUST

Even with state-of-the-art trust technology, new security and privacy breaches cannot be fully prevented. Malicious actors will continue to adapt and evolve their tactics. A more lasting solution is to look at human-centric dimensions of improving digital trust, such as providing for avenues for redress and improving digital literacy.

Organisations must prepare for occasions when technology fails, reduce the transaction costs of seeking restitution, and make trust-driven decisions that hardwire redressability into the technologies they are building.

Providing users with easily accessible and user-friendly recourse when something goes wrong can help to rectify the losses suffered. Case in point: Since the OCBC phishing scam, many major local banks have implemented emergency "kill switches" allowing customers to freeze their bank accounts if they suspect that their accounts have been compromised.

The concurrent inclusion of new security measures on websites, such as clear security policies, can help assuage concerns. A simple statement that the company will not reach out to collect personal information via text messages or phone calls will help users distinguish authentic from fraudulent communications. Multi-stage authentication procedures can also help assuage concerns because they give agency to the users to be part of a coordinated system of security applications and policies.

Professor of Internet Studies Bill Dutton at the University of Oxford likens digital trust to the problem of bicycle security in Oxford, where everyone has a "bicycle security mindset" on how to protect their bikes from being stolen. This second nature can be extended to online activity. PHOTO: PIXABAY

This move by banks takes dressing from tech companies. Users can report objectionable content on social media platforms. We can also easily access support functions, such as automated self-service options like frequently asked questions and reach out to customer service offices through e-mail, phone calls or chat messages with agents.

A second human-centric approach to increase digital trust is to improve digital literacy. Digital literacy is key to helping users navigate the online world in a safer manner.

Users with lower levels of digital literacy have been found to spend less time online and tend to be more cautious. On the other hand, those with high levels of digital literacy are better at recognising phishing e-mails and have greater awareness of the existence of malicious actors online. They are more likely to avoid negative experiences online.

However, higher digital literacy does not always lead to higher digital trust. Research shows those with higher digital literacy can also be distrustful and sceptical of the information received online because they can better recognise malicious acts or harmful content. Mistrust in these cases can be a positive disposition.

Singapore must find a Goldilocks balance in cultivating digital trust in the country. Trust in technology cannot be so low that it deters people from wanting to use platforms and digital services. This kind of distrust in technology owing to a lack of awareness of digital opportunities needs to be reduced.

Singapore must find a Goldilocks balance in cultivating digital trust in the country. Trust in technology cannot be so low that it deters people from wanting to use platforms and digital services. This kind of distrust in technology owing to a lack of awareness of digital opportunities needs to be reduced.

At the same time, digital trust cannot be so unquestionably high that people let their guard down. A healthy dose of scepticism and distrust is good at building resilience to scams and other online threats.

CULTIVATING A WHOLE-OF-NATION MINDSET FOR DIGITAL TRUST

How can we build a whole-of-nation mindset for digital trust? Professor of Internet Studies Bill Dutton at the University of Oxford likens digital trust to the problem of bicycle security in Oxford.

Cycling is a very common way of getting around in the city. Still, citizens have learnt over the years that not all places are safe to ride or to lock their bikes in. Everyone has a "bicycle security mindset" on how to protect their bikes from being stolen. Some lock them in visible areas; others avoid riding in unsafe areas.

This second nature of "we have to protect our bikes" can be extended to "we have to protect our data and online activity". For example, when using unknown websites or unfamiliar apps, we should be vigilant and wary of malicious actors who may attempt to compromise our devices, access our data and "steal our bikes".

To cultivate this whole-of-nation mindset for digital trust, companies must commit themselves to being trustworthy stewards in digital environments. This would entail long-term digital trust programmes, identifying current capabilities and deficits, developing necessary workforce skills and strategies, and consistent monitoring and improvement.

An example would be organisational certification for the Cyber Trust mark by the Cyber Security Agency of Singapore to recognise that the cyber security measures implemented in the organisation are up to industry standards.

Government intervention – through imposing regulatory requirements and ensuring compliance through oversight mechanisms – is another key pillar in establishing digital trust.

In Singapore, we have witnessed a collaborative approach to regulation with consultations involving technology companies and civil society organisations when implementing policies like the Online Safety Act passed in 2022.

While this approach is a step in the right direction, the Government must also be prepared to step in and implement stricter regulations when self-regulation and codes of practice fall short of societal expectations. For instance, the codes of practice regulate the providers of online communication services and currently offer no recourse for when recalcitrant users engage in "awful but lawful" behaviours such as offensive parodies or dark memes that mock real-life people or situations.

Finally, digital users must embrace a cyber security mindset to take proactive measures to protect themselves against malicious digital activities. They must practise cyber hygiene habits, such as actively thinking about what they can do to protect themselves. An example of such a habit could be to check the permissions settings on new apps we download to ensure that only essential information is shared with the app to maintain the privacy of our personal data.

Fostering digital trust in an ever-evolving digital landscape requires cooperation and shared responsibility among all stakeholders. Even as organisations and governments work to enhance digital trust along dimensions such as cyber security, privacy and redress, digital trust remains fragile unless individual traits such as digital literacy and mindsets improve over time.

• Chew Han Ei is senior research fellow and Carol Soon is principal research fellow at the Institute of Policy Studies at the National University of Singapore and principal investigators at the NUS Centre for Trusted Internet and Community. Jeanne Tan is research assistant at the Institute of Policy Studies.