Publication: The Straits Times, Pg B3
Date: 11 September 2023
Headline: Want to cyber-secure your firm? Make the training smarter

A cyber-security firm's office in Singapore. With all the time that we are spending online, everyone, young or old, is equally vulnerable to cyber-security threats, says the writer. PHOTO: ACRONIS

Want to cyber-secure your firm? Make the training smarter

Scammers are becoming more sophisticated and the threat of breaches is rising, but cyber-security training is stuck in a rut.

Lim Sun Sun

Question: You get a call from your colleague asking you to share your network password because she accidentally locked herself out of her account and needs urgent access to some corporate financial documents. What do you do?
A. Share your password with her as she is a good friend.
B. Decline her request because it violates company policy.
C. Suggest that she gets hold of the documents by buying the CFO coffee.

Raise your hand if you have been made to answer similarly elementary questions in the dreaded annual cyber-security test that your organisation runs in the equally dreaded cyber-security training course. It is an incongruity of working life that as scams become more sophisticated, cyber-security training seems to be getting dumber.

And yet, the need for more effective cyber-security training for employees across all organisational levels has never been more pressing. As the Covid-19 pandemic jolted organisations into digitalisation, widespread connectivity has also made them more prone to cyber attacks and cyberthreats.

Corporations have responded to these risks by stepping up cyber-security awareness training, contributing to a boom for such instructional programmes. The global cyber-security market is valued by some estimates at US$222 billion (S$303 billion). Meanwhile, the market for workforce cyber-security awareness training is expected to exceed US$10 billion by 2027.

These training programmes are designed to educate individuals within organisations about the potential threats and best practices to mitigate cyber-risks. Typically, they aim to enhance employees' understanding of phishing, social engineering, password security, data protection and other key cyber-security principles. Ideally, they should also seek to foster a culture of vigilance and informed decision-making and to inoculate participants against cyber-security scams.

Cyber-security scams essentially function on the basis of emotional manipulation and constitute social engineering of the most devious kind. They prey on human frailties such as greed, impulsiveness, carelessness, gullibility and unconscious cognitive biases that make us more vulnerable to such deception. Companies may spend a small fortune on sophisticated cyber-security infrastructure but these digital fortresses cave under the weight of human inadequacies.

According to Verizon's 2023 Data Breach Investigation Report that analysed 16,312 security incidents and 5,199 breaches from around the world, 74 per cent of all breaches have a human element involving errors, misuse of privileged accounts, use of stolen credentials, or social engineering that enables cyber criminals to covertly install malware, obtain login information and access confidential data.

Cyber attacks, therefore, succeed when employees fail to adhere to security protocols or engage in activities that jeopardise both their own security and that of the company.

That is why it is confounding that the training programmes that organisations use to buttress their employees' cyber-security hygiene are often amateurish. Rather than getting users to recognise the human conditions that make us more susceptible to deception, these training programmes instead put employees through the drudgery of answering blatantly obvious questions with even more obvious answers.

To add insult to injury, they often involve viewing atrocious videos featuring childish animation or stock images with dull and robotic voices. Little wonder then that employees are known to complete these training programmes while performing a multitude of other tasks simultaneously, watching explanatory videos on 2X speed, skipping straight to the quizzes without perusing the educational materials, or procuring cheat sheets from colleagues who have already passed the test. It is not surprising that such training is treated with disdain. Prior research has shown that employees consistently underestimate the likelihood that they will fall victim to a cyber-security breach.

Bearing in mind such optimism bias, how can cyber-security training be made more interactive and effective?

Various methods have been proposed to raise the cyber-security awareness and competencies of employees. Gamification, where employees can play customised games set within the organisational context, perhaps even customised to employees' specific organisational roles, has been found to be far more engaging than generic informational videos and quizzes with stock answers.

Another promising method is termed the constructivist approach, where employees are tasked with developing their own cyber-security training programmes. Not only are they more invested in what is taught, they have greater insight into knowledge gaps that must be filled, which assessment approaches work better, and what strategies will get a buy-in from their colleagues. This method, while highly resource intensive in the first instance, nevertheless yields long-term benefits and can help engender organisational regard for cyber-security awareness.

The advent and growing application of generative artificial intelligence (AI) also offer distinct possibilities for more customised cyber-security training and interventions. For instance, every online user could be supported by a personal AI-powered cyber-security buddy which can dynamically identify suspicious e-mails, texts and notifications, and alert users to the potential hazards of their different online actions. Much like how our e-mail apps filter out suspicious e-mails or our Web browsers alert us when we are visiting websites that are not secure, a cyber-security buddy should be able to caution users about engaging in risky transactions, and track and correct individual behaviour that predisposes us to security breaches. Such personalised advice will be taken more seriously than the generic cyber-security reminders that organisations incessantly send to employees.

Another way to raise an organisation's cyber-security preparedness could be conducting fire drills and tabletop exercises involving personnel across all levels. These drills, which incorporate simulated cyber attacks, enable employees to perform their respective roles and can help uncover weaknesses in security structures. They may also uncover shortcomings in response plans and deficits in the cyber-security knowledge of employees.

Broadly speaking, the norms for cyber-security compliance must be consistent, with top management fully committed to it. It should not be a case of "do as I say and not as I do". Organisational policies for cyber security must be easily accessible and clearly communicated so that employees follow them.

With all the time that we are spending online, everyone, young or old, is equally vulnerable to cyber-security threats. Working adults, in particular, bogged down by work and family obligations, are hyperconnected via multiple platforms and inundated daily with a flood of messages and notifications. Short on attentional bandwidth, we are excellent targets for cyber attacks.

That is why they must be sensitised more cleverly to the risks of human fallibility in the face of cyberthreats. We cannot afford for cyber-security training to remain ridiculously formulaic and overly simplistic.

• Lim Sun Sun is vice-president of partnerships and engagement and professor of communication and technology at Singapore Management University. She is also a member of the Media Literacy Council.