Source: *The Straits Times,* p21
Date: 24 February 2022

Pay attention to avoid being scammed

A new study finds that if you are preoccupied, you are vulnerable to online scams. The state, firms and individuals all need to beware this attention deficit.

Irene Y.H. Ng, Ong Qiyan, Evelyn Kok and Sandy Chen

For The Straits Times

From fake love Internet conmen to the latest OCBC Bank phishing saga, online scams have increased sharply in the past few years.

Some research has shown that people who have experienced a negative life event such as economic loss or divorce are more susceptible to scams.

However, a study we conducted under the auspices of the Social Service Research Centre at the National University of Singapore found a deeper potential reason than simply economic loss for people falling for scams: lack of attention.

This ranged from being preoccupied by money worries or the demands of children to being unfocused while using mobile phones on the go.

With reduced attention, people become easy targets for fraudsters to draw them in with an opportunity to make a quick buck.

Our findings suggest that it may be an uphill task to stamp out scams simply by advising people to pay attention – and leaving the consequences of victimisation to individual responsibility.

After all, psychological resources are limited and everyone is at risk of losing focus when scammers strike. Hence, in addition to public education to improve awareness about scam tactics, we should embrace cognitive limitation as the norm and have strong state protection to mitigate the risks of scammers.

HOW WE GOT PEOPLE INTO OUR 'SCAM'

We used a mobile application we developed, called the Work-Life Tracker, to collect data from young adults to understand their experiences juggling work and life. We targeted non-degree holders as we were more interested in how they make decisions about work advancement than young people who had degrees. About 180 participants answered weekly surveys for nine months.

In August last year, we inserted an imitation job scam to test users' vigilance in detecting such scams. We told users they could earn a commission by making advance purchases via bank transfers to merchants, and asked if they would like to find out more about the offer. Two out of five users were "scammed" by us.

Those who were "scammed" clicked a button to be directed to the offer, at which point we immediately revealed it was a scam. We also turned it into an educational moment by listing the signs that our offer was fake.

In parallel, users who did not indicate interest were congratulated for avoiding a scam. They then answered a question to indicate what alerted them that our offer was suspicious.

Granted, some users could have clicked on the offer because they trusted our app, and some may have had no intention of eventually accepting the offer. But this is exactly how scammers operate. They get you interested, then lure you further in by playing on curiosity and familiarity.

When we compared those who were "scammed" with those who were not, we found that users whose expenses exceeded income in the past month were almost twice as likely to fall for our job scam as users whose net incomes were positive. Users whose incomes decreased in the past month were 1.5 times as likely to be "scammed" than users whose incomes did not decrease.

THE PREOCCUPIED BRAIN

Why do people who are experiencing financial strain become vulnerable to being scammed? Part of the reason might be attention span. The brain is busy ruminating over the problem, and is too distracted to pay attention to the task at hand.

Those who have experienced other negative life events, such as a break-up, a bereavement or even losing a wallet, may also relate to the feeling of not being present or in focus.

We found that our scammed users might have this attention deficit. We had accompanied the scam offer with a set of three cognitive reflection test (CRT) questions. Designed by psychologist Shane Frederick, the CRT measures users' "ability to resist reporting the response that first comes to mind".

There is one on how much the total cost of a bat and a ball is, another about lily pads in a pond, and one on widgets. We masked the questions by localising the items in the questions.

If someone is not paying attention, or just quickly answering our questions without deliberation, they could very easily go for the obvious but wrong answer. And many did. Half of the users answered all the questions wrongly, and only 14 per cent answered all three questions correctly.

More interestingly, our users who fared worse on the CRT questions were more likely to be scammed. Among those who got at least one CRT question wrong, 42 per cent fell for our "scam". In contrast, among those who got all the CRT questions correct, only 20 per cent were "scammed".

In addition, users with children were significantly more likely to have been "scammed" by us. Why? We believe it is because parents are distracted by constant multi-tasking to attend to their children and other needs. While more research is needed to test this link, it is striking that from the accounts of the OCBC scam victims, several were parents who said that they were attending to their children when they clicked on the fake OCBC link.

Finally, while lower educated users in our app were more likely to be "scammed", this effect disappeared when we also took into account those who were experiencing budget shortfalls.

So it is not low education that leads to higher susceptibility to scams, but that lower educated persons are more likely to have income shortfalls that drain their cognitive resources as their brains are preoccupied with worrying over finances.

PAY ATTENTION

Overall, with mobile phones, attention is often unfocused. With only 14 per cent of our app users answering all the CRT questions correctly, it is a reminder that everyone needs to become more deliberative in how we use our phones.

As app owners, the finding that close to half of our users were "scammed" by us is also an important reminder of the trust clients place in organisations and how this trust could be exploited by organisations or fraudsters to harm the clients.

It is important for organisations to be on top of cyber security needs, especially in the finance and medical fields, where security is part of their core services.

A critical step in doing so is understanding how clients access services, something that scammers are adept at but which organisations might not prioritise. For example, organisations' webpages and virtual processes are often complicated and inaccessible. They are often designed from the technical expert's perspective, not the user's.

Thus, warnings advising the public to go to the organisations' websites instead of clicking links need to be accompanied by greatly simplified and accessible websites.

With online scams so widespread, organisations including government agencies with websites and online communication also have a duty to their users to devote resources to preempt and stall scammers, besides warning their users.

Users need to pay attention. So do state agencies, public organisations and private firms.

stopinion@sph@com.sg

• Irene Y.H. Ng is associate professor in the department of social work and Social Service Research Centre at the National University of Singapore; Ong Qiyan is adjunct research fellow, Evelyn Kok is research assistant and Sandy Chen is senior executive at the centre.