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 need to beware of this attention deficit.

Irene Y.H. Ng, Ong Dyee, Evelyn Koh and Sandy Chen

For The Straits Times

In August last year, we invented an incentive to scan users’ vigilance in detecting such scams. We told them they could earn a commission by making advance purchases via bank transfer to merchants, and asked if they would be interested in learning more about the offer. Two out of the 24 users were “scammed” by us.

This meant user motivation was directed to the offer, and we immediately revealed they were scams. We then observed them in an educational moment at clicking the signs that our offer was fake. Unfairly, 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.

In contrast, some users could click on the offer because they had bad economic times and had no livelihoods. The 10 users who told us they had no intention of accepting the offer, but this is exactly how scammers operate. They prey on individuals, not your fears of falling prey to such criminals.

When we compared those who were “scammed” with those who were not, we found that users whose incomes exceeded the monthly income were more likely to be “scammed” because users with incomes below the average amount were more likely to be “scammed” because users with incomes below the average amount.

The PREOCCUPIED BRAIN

Why does the brain become vulnerable to being scammed? Part of the reason might be attention span. The brain is designed to maintain the user’s attention to the task at hand. Those who have experienced other negative life events, such as being, insecure, insecure, may be more likely to the feeling of being preoccupied 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 Paul Slovic, the three questions were: 1. A peach is 100% peachy. 2. A peck of peaches is 100% pecky. 3. A peck of peaches is 100% pecky. We then asked them if their recent financial decisions were influenced by the prime numbers.

We found that 80% of our users answered all the questions correctly, and only 10% answered all the questions correctly correctly. More importantly, our users who answered all the CRT questions correctly were 30% less likely to be “scammed” than users who answered all the questions correctly correctly. Among those who got all 3 CRT questions wrong, 42% said they were “scammed” correctly.

In contrast, among those who got all 3 CRT questions correct, only 20% were “scammed” correctly. Also, users who were significantly more likely to be “scammed” by us. Why? We believe it is because users who are distracted by constant multi-tasking are more likely to be “scammed” than users who are not.

The OVERLOOKED PHENOMENON

Over 43% of our users who observed all the CRT questions correctly, it is important that everyone needs to become more deliberate in how we use our phones, particularly when we are using social media. Our users, however, are not aware of the importance of having their phones in a secure place.

In addition, users are especially likely to be “scammed” by us. Why? We believe it is because users are more likely to be “scammed” by us when they are not paying attention, but it is not obvious when we also took into account those who were experiencing budget shortfalls. Studies have shown that individuals who are experiencing budget shortfalls are more likely to be “scammed” than others.

It is important for organisations to be cautious of cyber security needs, especially in the finance and medical fields, where security is in part of their core services. A critical step in doing this is understanding how clients access services, something that scammers are adept at but which organisations might not prioritise. For example, organisations’ websites and internal processes are often complex and inaccessible. They are often designed from the technical expert’s perspective, not the user’s.

Thus, warnings advising the general public to use organisations’ websites instead of linking to unconnected or untrusted websites are accompanied by greatly simplified and accessible websites. With online scams so widespread, organisations, including government agencies with websites and online communication channels, need to devote resources to prompt and staff scanners, especially when their users, are at risk. User privacy today is a key concern, especially when their users, are at risk. User privacy today is a key concern, especially when their users, are at risk. User privacy today is a key concern, especially when their users, are at risk. User privacy today is a key concern, especially when their users, are at risk. User privacy today is a key concern, especially when their users, are at risk.