



Headline: Close call with scammers
Publication/Portal: New Straits Times
Date: 1 January 2021

Language: English
Section: News
Page: 15



In his panic, Albert (not his real name) divulged banking details he had often reminded himself not to reveal to anyone. FILE PIC

Close call with scammers

KUALA LUMPUR

“THE SMS came at 9.50am on Dec 28 and it shocked me,” said Albert (not his real name) as he recalled what he referred to as a haunting scam experience.

The message was an alert telling him that someone with a credit card ending with a certain number had cashed out RM3,000 on Dec 28 and said if he did not perform the transaction he should call customer care at 1800-81-9388.

“I was at my wit’s end,” said the 65-year-old retiree.

He noticed that the last four digits of the credit card mentioned in the message were slightly different from those on his card, but he had begun doing everything he should not have.

He called 1800-81-9388. That was the first mistake, he said.

“I should have called the bank that issued me the credit card.”

Still in a state of shock, he did not realise that the call had not gone through the automated answering system that banks use nor was there a verification process. This was his second mistake.

The person who answered the call, who he referred to as “Scammer No. 1”, said someone had used his name and particulars to successfully apply for a credit card in Nilai, Negri Sembilan.

The scammer provided detailed information, including the date of application for the card (Dec 7), date of approval for the card (Dec 14), the three-digit card verification code and the address where Albert had once lived more than 30 years ago.

The scammer “advised” him to lodge a report with Bank Negara Malaysia and gave him a number to call (03-9212 7361), saying he should give all the details that he (the scammer) had given him about the credit card to the central bank.

Albert did not verify this telephone number. It was his third mistake.

As though under a spell, he called the number. This was his fourth mistake.

Someone who identified himself as “Mohd Abdullah Nordin” asked Albert to read out the SMS he had received.

In hindsight, Albert realised that the man was prepping him for something similar he had to do later on.

After reading out the SMS, “Mohd Abdullah” said someone working at the bank

that issued the purported credit card must have worked with the card applicant.

“Mohd Abdullah”, or “Scammer No. 2”, told Albert there was a possibility that his account with another bank might have been hacked as well and asked for his username and password.

Albert realised later that in his panic, he had divulged that information. This was his fifth mistake.

He had been reminding himself never to divulge his username and password to anyone, so he could not understand what made him do it that day.

He said Scammer No. 2 told him that his account was hacked at 6.40am, the fund transfer limit was raised to RM30,000 and an unsuccessful attempt was made to transfer out RM10,000.

Albert said any attempt to transfer out RM10,000 would have been unsuccessful as he had only a little over RM4,000 in his account then.

“He told me he could block my account from any further hacking attempt. As we talked, I constantly heard the tapping of the computer keyboard.

“I became suspicious and suspected that it was a scam when the fluent Malay accent of this “Mohd Abdullah” changed during the conversation to a Chinese accent, indicating that there was more than one person on the other end of the line,” said Albert.

He said soon after, the scammer asked him to check whether he had received any SMS.

“Sure enough, there was one from my bank, stating a TAC (transaction authorisation code) for a payment of RM4,000 to a certain company.

“The scammer asked me to read out what was exactly in the SMS so that he could block the payment.

“Remember, he had prepared me earlier for this part. All this happened so fast that there was little time to think. But I tried to remain composed.

“I was not about to make my sixth mistake. I kept asking him if he was actually from Bank Negara, to which he kept replying in the affirmative. I told him I would ask my bank to handle it from now on and ended the call. I immediately asked my bank to block my account’s online transaction facility,” he said.

Albert said he did not report the matter to the police because he had not lost any money. **Bernama**