PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: A haunting scam experience
Publication/Portal: The Borneo Post (Sarawak)
Date: 4 January 2021
Language: English
Section: Home
Page: 10

A haunting scam experience

KUALA LUMPUR: "The SMS message came at 9.50 am on Dec 28 and it shocked me, to say the least", said Albert (not his real name) as he recalled what he referred to as a haunting scam experience.

It was an alert that a credit card ending in XXXX cashed out RM3,000 on Dec 28 and that if he had not performed the transaction, he was to call customer care at 1800-81-9388.

"I was at my wit's end," said the 65-year-old retiree. With the benefit of hindsight, he said he realised that the last four digits were slightly different from those on his card.

Nevertheless, he started doing everything that he should not have done in such a situation. He called 1800-81-9388. It was the first mistake, he said.

"I should have called the bank which had issued me the credit card."

Someone answered, of course. At that time, still in a state of shock, he did not realise that the call had not gone through the usual automated telephone answering system that banks use and that he was not subjected to the usual verification measures. This was the second mistake.

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

The scammer gave every detail that he would have asked for: type of credit card, number of the card, the date of application (Dec 7, 2020), date of approval (Dec 14, 2020), date of card expiry. He even disclosed the three-digit CVV (card verification value) code at the back of the card and the residential address where he had once lived, more than 30 years ago.

Up to that point, because of the state of shock that he was in, it never occurred to him that he was being scammed.

The scammer 'advised' him to lodge a report with Bank Negara Malaysia and gave him a telephone number to call – 03-92127361 – saying he should furnish BNM with all the details that he (the scammer) had given him about the credit card. Albert did not verify this telephone number. It was his third mistake.

He related that acting as though he was under a spell, he called the number. This was his fourth mistake.

Someone, who later identified himself as Mohd Abdullah Nordin upon his asking, enquired what it was all about and asked Albert to read out to him what was exactly in the SMS message that he had received.

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

After he had read out the SMS message, 'Mohd Abdullah' said someone at the bank where the purported credit card was issued must have been working in cahoots with the person who had applied for the card.

'Mohd Abdullah', whom Albert referred to as Scammer No. 2, told him there could be a possibility that his banking account (with another bank) could have been hacked as well and asked for his username and password.

Albert realised later that in a hypnotic state of mind, he had divulged that information. This was his fifth mistake.

He said he has been reminding himself never to divulge his username and password to anyone but he still could not understand what made him do it on that day.

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

Albert said that 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 could constantly hear the tapping of the computer keyboard.

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

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

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

"This scammer asked me to read out to him what was exactly in the SMS so that he could 'block the payment'. Remember, he had prepared me earlier for this communication. All these happened so fast that there was little time to think. I was like a fish that had taken the bait and was being hauled in fast. But I tried to remain composed.

"And I was not about to make my sixth mistake. I asked him repeatedly whether he was actually from Bank Negara, to which he kept replying in the affirmative. I told him I will ask my bank to handle it from now on and put down the phone. Immediately, I advised my bank to block the online transaction facility of my account," he said.

Albert said he did not report the matter to the police because he had not lost any money and, furthermore, the police have their hands full with such scams.

"However, I want to share my experience so that other people know one way of how a scam is played out and can take the necessary precautions.

"I read somewhere that relating your scam experience to your family members and friends is one of the best ways to take action because scammers rely on people being secretive. Whoever you relate your experience to will be better prepared to avoid similar scams in the future," he said.

— Bernama