PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: I was nearly scammed twice
Publication/Portal: New Straits Times
Date: 12 December 2019

Language: English
Section: Letters
Page: 17

ONLINE CASES

I was nearly scammed twice

ONLINE banking has become convenient as it eases transactions with just a few clicks. Gone are the days when one has to queue or wait hours to carry out banking transactions.

However, online banking has also opened up another industry — online scams. They come in many forms but the most popular is phishing (pronounced "fishing"), as if one is going to catch a fish using the rod.

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

Previously, phishing used fake emails asking for contact details or offering products at bargain prices. Those who are not tech-savvy may succumb easily to these online predators.

I have heard many cases involving online scams, either through email or phone calls. In fact, a relative also fell victim to a scam, losing a few thousand ringgit in the process.

With my financial background, I am vigilant of these criminal activities. However, as careful as I am, I almost fell victim twice to such scams.

The first was in April, with a four-step technique: i) log into my account; ii) transfer the cash into their account; iii) request a six-digit online banking code sent by the bank to me; iv) call me with an urgent tone to get the code that sent to my phone.

It happened at 6.45am. I was caught unaware as I was preparing for a course.

I told the caller to call me back a few hours later.

Then I received a lot of text messages in one of the social applications.

I then realised that the scammer had hacked into my account and attempted to transfer cash into their account. I quickly changed my password and thought that was it.

Then I encountered another attempt with a different modus operandi and with a different bank.

I received a text message asking for a six-digit online banking code requested through the social application.

The similar four-step technique was applied but I was prepared this time. I answered the scammer's call and said that I was busy.

The caller texted me to inform that my money was gone and advised me to call back if I wanted my money back. I checked my account and discovered that money was missing.

I called the bank and reported my case.

I was told that this was a new phishing technique, where the scammer would use a feature in the online banking for a periodical payment to one of the established virtual malls in Malaysia. Again, I changed my password.

After these two incidents, I come to this conclusion:

USE a sophisticated password, one that differs from the username; and,

LIMIT daily transaction to just RM1,000 so that my account appears unappealing to scammers.

Using an easy-to-remember password is not only convenient to me but also to scammers.

Nothing is impossible in advanced technology.

Scammers can come in many forms, but as long as we realise the threat and take precautionary measures, nothing can harm us.

DR RAZIFF J.
Shah Alam, Selangor