

One woman's bad experience should be a lesson for all of us who engage in online banking.

By SUBASHINI SELVARATNAM
intech@thestar.com.my

MELINDA (not her real name) didn't fully trust online banking, but opted in because she wanted the convenience of paying her bills from her computer instead of having to go personally to settle the amounts.

It all went well until the day she received an e-mail message, purportedly from the bank, prompting her to login into her bank account due to some problem or other. Without thinking, Melinda did as she was instructed.

"That same morning, I received an SMS stating that my transfer of RM5,000 to a third-party account was successful. I was horrified," she said.

In a panic, Melinda immediately called her bank branch. The bank personnel could only forward her report to headquarters.

She was also required to make a police report. At the station, she found out that she wasn't the only victim of such a scam. "I heard that some people have lost up to RM15,000 over three consecutive days," she said.

After that, the bank froze her account to prevent any other unauthorised electronic withdrawals and started the process of issuing her a new ATM card.

In her grief, Melinda lashed out at her bank. She claimed she sent numerous e-mail messages enquiring on the outcome of the bank's investigations and that these went unanswered.

After a trepidation-filled month, she finally got a response. The bank concluded that its online security system had not been breached; meaning the theft did not result from any fault of the bank.

Its investigations showed that a valid username and password were used to login to the online bank account — Melinda supplied this to the thieves herself when she followed the instructions in the e-mail purportedly from the bank.

Also, the bank found, two valid Transaction Authorisation Codes (TACs) were subsequently supplied, giving permission to perform the third-party money transfer.

Melinda claimed she never received the TACs although the bank's records showed that the TAC requests were sent to her mobile phone. But she could not prove that she did not receive the TAC requests.

She called her cellular service provider which informed her that it only keeps records of SMSes received by a customer for about three days and the period had expired by the time the telco was contacted.

The RM5,000 was gone. Later the bank told her that the money had been transferred to an offshore account, somewhere in Africa, and the trail ended there.

Who's to blame?

Such incidents when heard of make many people wary about banking over the Internet. And victims of the scam are likely to never engage in online transactions ever again.

The typical reaction of a victim is to blame the bank. But are the banks really at fault here?

It's true that banks stand to gain

DON'T BE A VICTIM



THE BUCK STOPS HERE: At the end of the day, the customer is the last and best line of defence in conducting safe online banking transactions. — AP

from customers opting for online banking; they reduce their staffing costs, reduce the cost of printing withdrawal slips and other paper forms, and benefit from easier transaction record keeping.

But the customer gains too. You can check your bank or credit-card balance almost instantaneously from your computer, pay bills without having to leave home, brave traffic or the weather, and transfer funds easily between accounts.

And therein lies the problem. If it's easy for you to transfer funds, it's also easy for someone posing as you to a bank's security system to transfer your money to another account.

Banks spend millions ensuring they have an online banking system that is as secure as humanly possible. The incentive? Well, they can be liable for up to millions as well, if a customer loses money and it turns out to be their fault.

The weakest link in that security chain, however, is you. That's why scammers target you and not the bank whenever they employ the scam.

You hold the key to your money. If you give it away, you have no one else to blame. You would not think to mail off your bank book if someone asked you to, right? If a stranger stopped you in the street and asked for your bank account number, would you tell it to him?

The same precautions apply in cyberspace as in the real world. This is stressed over and over again by banks and other financial organisations, but some people aren't listening, it seems. Your computer is no more secure than your car or closer yet, your wallet.

A drop in the ocean

Bank Negara Malaysia (BNM), which regulates the local banking sector, said losses due to online fraud was only 0.00002% of the total value of Internet banking transactions over the past three years. Internet banking was introduced in 2000.

There is the Internet Banking Task Force which keeps a watchful eye on online banking trends and developments, and takes measures

to mitigate any potential new risks, vulnerabilities or threats that may emerge.

BNM said banks have also implemented a Two-Factor Authentication (2FA) system for high-risk transactions such as bill payments and third-party fund transfers over the Web.

The 2FA system complements the "First Factor" security measure, which is the customer's username

and personal identification number (PIN) or password.

The banks, said BNM, also perform a second-level authentication by requesting users to enter a dynamic password. Examples of these are TACs and token-generated-PINs. They also make use of the latest technologies, such as smartcards with digital certificates.

Then there's the gamut of other

»I received an SMS stating that my transfer of RM5,000 to a third-party account was successful. I was horrified«

VICTIM OF ONLINE BANKING FRAUD

security measures adopted by the banks — user authentication and access controls, fraud alert systems, etc — and deployment of network securities like a firewall, antivirus programs, and intrusion detection systems.

The bottom line is that the sole responsibility of conducting safe banking transactions over the Internet lies with the customer.

Users of online banking services must be ever vigilant, cautious and suspicious. Paranoia is a downright useful trait here, we would add. There is no such thing as a foolproof system and one that can't be beat.

Remember that banks will never ask you for your account details via e-mail, SMS, or over the phone. And if in doubt, contact your bank branch over the phone or in person. No problem is so pressing that you cannot take the time to speak with your banker about it.

Perpetrators of this kind of scam rely on the victim working himself or herself into a panic and divulging vital data immediately, without thinking. Keep your head.

What some banks say

TO REASSURE ourselves on the security of online banking, we spoke to a few banks about the securities that they have in place, as well as the procedures they use whenever a customer's worst nightmare comes true.

All said they spare no effort in investigating every report that they receive and work closely with the authorities — the police and national cybersecurity specialist CyberSecurity Malaysia.

Maybank advises its online banking customers who suspect they have fallen victim to a scam to immediately report the incident to Maybank Group Customer Care at 1-300-88-6688.

Its senior executive vice-president and head of consumer banking, Lim Hong Tat, said the victim should also immediately change the username and password to the account, and report the matter to the police.

"Keep any communication, such as e-mail messages or SMSes, to any third party that may be a suspect and provide this information to the police or the bank to assist in the investigation," he said.

He said Maybank has a team that continuously monitors all security aspects of its Internet banking services. Any unusual transactions that are detected are investigated.

Another local bank, CIMB, said if a customer loses money online due to fraud, it starts its

investigation as soon as it is alerted because the bank wants to prevent the funds from being transferred, if possible.

If CIMB is able to hold on to the money, the customer is reimbursed as soon as the investigation is completed. This process usually takes several days, according to the bank.

Its head of retail banking, Peter England, said that while there have been cases of customers losing their money online due to fraud, the bank is unable to disclose how many times this has occurred.

"We can, however, state that on every occasion it was the customer who had compromised his or her own User ID and password, and had then responded to a fraudulent request to key in a TAC (Transaction Authorisation Code) that they had received on their mobile phone," he said.

"There is not a single incident of fraud that occurred as a result of any weaknesses in our Internet banking system."

CIMB is always on the look out for fraud attempts where a customer is duped into revealing Internet banking credentials, such as after receiving an SMS that he or she has won a contest.

It also monitors Internet banking transactions that it finds suspicious (even before monetary loss is reported) to proactively help prevent fraud.

And its customers are regularly reminded via messages on the

bank's website and other media, to never to respond to requests for personal information that come through e-mail, phone, or SMS.

The Citi never sleeps

US-based Citibank is ever vigilant against online banking fraud. Roy Heong, consumer e-business head for the bank's Malaysia branch, said the bank has stringent fraud prevention systems in place.

Citibank Bhd has a system that involves a one-time Online Authorisation Code number and requires that a series of security questions that only the customer involved would know, to be answered correctly before being allowed to log into his or her account.

If there are three incorrect attempts to login, the account will be temporarily disabled for security reasons. The account can be re-enabled when the customer calls in and a full verification is done.

The bank also employs a dynamic keyboard on the login screen to keep keyloggers at bay. Keyloggers use programs that track a computer user's key presses on the keyboard to deduce user names and passwords.

(PC users need to also be wary of a video-logging trojan program that can be used to capture a user's clicks on a dynamic keyboard.)

Also, each Citibank online session is terminated after six minutes of inactivity.