Keeping fraudsters at bay

In the fight against fraudulent online transactions and malware attacks, the country's financial institutions led by Bank Negara are beefing up security measures but consumers too must be more alert and proactive.

By CHRISTINA CHIN
sunday@thestar.com.my

AS Malaysia moves forward to embrace cost-effective electronic payment methods necessary in achieving a high-income economy, the country's central bank together with leading financial institutions want consumers to be more vigilant in their banking habits to prevent fraud.

And while these institutions continuously make efforts to enhance online security, consumers themselves have a crucial role to play in protecting their hard-earned ringit from fraudsters lurking in the World Wide Web.

Last month, teacher Joan Ng, 28, almost became a victim. Luckily, the smart consumer kept her wits about her and contacted the authorities, thus preventing the loss of RM5,000 to an online fraudster.

"I received a call from a Hong Kong number congratulating me and saying I had won a gemstone worth RM96,000. The caller even had my identity card number and full name, which was put up on a mall's website, and she told me to log in to the site.

"It was very believable because I had visited the mall before and even filled out a customer survey form when I was there," she relates.

Initially excited, she gave her bank account details to the caller and asked for cash to be banked into her account in lieu of the gemstone.

It was only when the caller asked for a cash deposit that alarm bells started to ring.

"I checked *www.scamadviser.com* and found the mall's website there with a '60% caution' trust rating. I still didn't want to believe that it was a scam until the police and Bank Negara confirmed it," Ng says.

Coincidentally, her sister Melody, 32, was also targeted a few months before her.

Sharing her experience, Melody relates how she had received a text message from a local bank telling her that her credit card had been swiped to pay for a RM7,000 bracelet in Hong Kong. In her case, it was a clear attempt at fraud because she was in Penang at that time, and she did not have a card from the bank.

"Within minutes of the SMS, a lady called requesting I confirm the transaction. She also claimed that I owed the bank more than RM6,000 and asked me to call what she said was Bank Negara's hotline," Melody, an assistant manager, says.

She decided to play along and dialled the number. When she got through, someone claiming to be a Bank Negara officer put her on hold. It was a very elaborate scam that would have easily conned an unsuspecting person.

Later, she checked Bank Negara's website and found that the number she had called was not on their list.

Stressing on the importance of understanding the risks associated with credit cards and how to protect against suffering fraud losses, Bank Negara wants consumers to use the relevant security tools and authentication methods, ensure proper safekeeping of cards and personal data, and monitor their own payments to identify any possible suspicious transactions.

Fraudulent transactions related to credit cards remained the most common form of payment fraud, Bank Negara reveals. Despite this, losses due to credit card fraud are low, with total losses amounting to RM29.4mil – or an average loss of 0.03% of total transaction value of over RM100bil – last year, a spokesperson from Bank Negara says.

"If fraudulent transaction is detected, the consumer should quickly alert the credit card issuer and lodge a police report," the spokesperson stresses.

"Generally, if the investigation finds that it is a fraud case, the cardholder will be compensated for the loss."

To protect against fraudulent transactions, cardholders are required to enter a one-time password (OTP) to authorise payment, the officer says. A text message from the bank would then be sent to the cardholder's telephone number registered with the bank to confirm the transaction.

When offline, credit cardholders are protected by the Europay-Mastercard-Visa (EMV) chip which has contributed significantly to a drop in counterfeit credit card cases since 2004, she points out.

"(However), consumers are reminded to always keep an eye on their credit cards during point of sale transactions, like when paying at a restaurant.

"Together with the (online) authentication method, the EMV protects consumers through the 'liability shift' rule whereby losses are absorbed by the party with weaker security measures."

The Association of Banks Malaysia (ABM) feels that affordability, convenience and efficiency are benefits that far outweigh online banking risks given the low level of fraud.

ABM executive director Chuah Mei Lin explains that accelerating the migration to e-payments is a primary agenda for the country as it has the potential to drive further efficiency gains and cost savings for the nation's economy.

The ABM believes that it will improve the country's competitive position as successful migration to e-payments can save up to 1% for gross domestic product (GDP) for the country annually.

Incidents of fraud related to the use of payment cards, electronic money (e-money) and cheques are low, she stresses, adding that these accounted for less than 0.006% of the total volume and value of retail payment transactions in 2013.

"This is a very small percentage," Chuah points out while also reminding consumers to "be smart".

"All stakeholders, including bank customers, must play their part in combating fraud and to safeguard themselves from becoming victims of fraud.

"Banks constantly enhance the security of their online banking services but consumers may still fall victim to fraudsters if they panic or are careless," she says.

Be cautious and responsible when using credit cards and revealing personal information, she reminds, adding that banks have stepped up communication with customers and taken many initiatives, even on social media, to create awareness on the latest scams.

The association, together with the National Cards Group, had on Oct 7 launched an awareness campaign (*www.abm.org.my/NCGthinkcard/*) to increase consumer confidence in cashless transactions.

Since last year, it has been working with the Police and Association of Islamic Banking Institutions Malaysia to launch the "Crime Prevention Campaign: Partner with the Private Sector to Communicate New Crime Fighting Initiatives".

"Our members are also monitoring the spending patterns of credit cardholders," Chuah says.

"Prompt actions are taken to protect their interests, which may include the banks contacting credit cardholders to confirm a transaction that seems outside of the usual spending pattern."

Global online payment solutions provider PayPal is also reminding its users to adopt "safe e-mail behaviour" to protect themselves.

Its spokesperson says e-mail from PayPal will always address users by their first and last names or business name.

"We never say things like 'Dear user' or 'Hello PayPal member. Our e-mail don't link directly to pages that ask for your bank account, credit card and ID card numbers," she says.

Users who receive a fake PayPal e-mail or website are advised to forward the original e-mail or URL to *spoof@paypal.com*.

"Users who receive e-mail about PayPal transactions must confirm if a payment has been received or made by logging into their PayPal accounts and checking their account balance," she adds.

For more information, contact Bank Negara Malaysia via telephone (1300-88-5465), fax (03-2174 1515), SMS (type BNM *TANYA [your enquiry/complaint]* and send to 15888) or e-mail *bnmtelelink@bnm.gov.my*.

The Dos and Don'ts of Online Banking

Dos

- Check credit card, account statements and all SMS notifications from your banks to identify fraudulent transactions.
- Report dispute(s)/ unauthorised transaction(s) to the bank as soon as it is detected.
- Protect and change your passwords regularly.
- Install anti-virus, anti-spyware and Internet firewall tools purchased from trusted suppliers.
- Be wary of downloading free files, programmes, software or screensavers and avoid unsolicited or provocative messages (via e-mail, Internet pop-ups or phone messages).
- Ensure that you are in a secure environment when doing financial transactions online.
- Look for the closed-lock/ unbroken-key icons on your browser when entering sensitive data and double-click on the icon to ensure it is registered to your financial institution.
- Protect your connection especially if you are directly connected to the Internet for an extended period of time through a cable modem or digital subscriber line (DSL). Disconnect once done.
- Clear your cache to prevent addresses stored in the computer's memory from being viewed.
- Check with the staff when using free wireless Internet connections in public places to ensure that you are connecting to their wireless network instead of WiFi networks set up by fraudsters to access your personal information.

Don'ts

- Never send personal and financial information by e-mail.

Common Online Scams

Phishing e-mail

- Fraudster randomly sends phishing e-mail asking for updated information.
- Customer opens the e-mail and clicks the hyperlink in the phishing e-mail. After clicking the hyperlink, the landing page of the Internet banking website which looks almost exactly like the bank's Internet banking website appears.
- Customer logs into the fake site and fraudster captures the username and password.
- A new page appears asking the customer to request for a Transaction Authorisation Code (TAC).
- After receiving the TAC, customer types code into a message box given.
- After fraudster obtains information (username, password and TAC), he will have access to the customer's Internet banking account and make transactions such as registration of third party account, fund transfer to third party, prepaid reload, etc.

SMS scam

- Customer receives SMS informing him that he has won a cash prize from a renowned petroleum company.
- He calls the number in the SMS and a lady claiming to be from the company picks up the call.
- He follows her instructions to go to nearest bank's ATM, enters a few numbers which the caller claims is a 'code' to get the prize.
- By following the instructions, he is actually applying for an Internet banking account via the ATM and the number which he has entered is the Personal Identification Number (PIN) to open the Internet banking account.
- The 'staff' says the prize will be delivered soon but his bank account balance is reduced instead.

Phone scam

- Customer receives a call from fraudster claiming to be a bank officer.
- Fraudster informs the customer that he has outstanding balance on a credit card, alleging that someone had used the customer's identification card to apply for the said card.
- Fraudster advises the customer to bank in money to an account (managed by the fraudster) to prevent being blacklisted.
- After money is banked in, the fraudster transfers the cash to another account/ withdraws the money.

for the

Source: ABM