NST Online &#65533; Frontpage 2009/04/26
 <h5>Phone scam that empties your account </h5> By : Sonia Ramachandran

  <table border="0" cellspacing="2" cellpadding="2" align="center"> <tr> <td id="aphoto" class="caption"> </td></tr> </table>
   Fraudsters are emptying the bank accounts of people by tricking them into divulging their personal financial information. KUALA LUMPUR: You receive a call, purportedly from a bank, asking if you had just conducted a credit card transaction for goods or services. When you answer in the negative, the caller then tells you in a concerned tone to call an agent of a commercial bank and you are given the number. Upon calling, the agent gives you the telephone number of the "bank" and tells you to call the bank itself. You call and someone picks up, identifying himself as an officer of the "bank". You then tell him that you did not conduct the transaction and you do not have such card. But he informs you that the records, however, show that the transaction had been carried out and that the card belongs to you! He suggests you call Bank Negara's "Unit Kad Kredit Palsu" (Credit Card Fraud Unit) and gives you the number. You then reach an automated voice message service which says you have contacted "Bank Negara". A Bank Negara "officer" then comes on and identifies himself. He asks for your banking and credit card information so that he can lodge a complaint on your behalf. You then give your details over the phone and finally assured that "Bank Negara" will "look into your problem", you heave a sigh of relief. But what you don't realise is that as soon as you have put down the phone, the fraudsters are already emptying your account, thanks to the information you had just furnished them. This is the latest scam that Malaysians are falling prey to. Last year, Bank Negara received 165 complaints on unauthorised withdrawals. As of mid-April this year, there have been 265 complaints. The losses range from a minimum of RM4,000 to a maximum of RM10,000. The Association of Banks in Malaysia received 42 complaints from April 1 to Friday on the scam which uses Bank Negara's name alone. "One of the victims who walked in a few days ago lost RM7,000," said Bank Negara corporate communications director Abu Hassan Alshari Yahaya. There is no such "Unit Kad Kredit Palsu" in Bank Negara, he added. Abu Hassan said the fraudsters used a different approach before. They would SMS potential victims informing them that they had won prizes and to collect these prizes, they had to open an Internet banking account. If you fall for this scam, the fraudster then provides a step-by-step guide on how to register and activate an Internet banking account using an automated teller machine (ATM) terminal. At the ATM terminal, you will be given an Internet banking personal identification number (PIN) which will be given to the fraudster. Based on the fraudster's instructions, you also key in his or her mobile number into the ATM. When a person conducts Internet banking, he would receive a Transaction Authorisation Code (TAC) from the bank via SMS. Since you have keyed in the fraudster's mobile number, this code will also be sent to him. "People are vulnerable when they are told they have won prizes and these fraudsters take advantage of that vulnerability. There are no shortcuts to prizes. The public need to be aware at all

times." Abu Hassan advised people to never respond to any SMS, phone calls or email asking for personal information such as PIN and passwords for banking accounts. "Banks will never request for such personal information through email, SMS or phone calls." In June last year, the New Sunday Times reported that the SMS scam was so serious that the police were receiving at least one report a day. The police said the number of scams was increasing with some victims losing up to RM1.2 million. Email scams, said Abu Hassan, were those where email were sent out, purportedly from the banks asking the recipients to update their personal banking information or accounts. To do that, the recipient would have to click on a link provided in the email and be led to a site that looks exactly like the bank's site. When you key in your personal information on this duplicate site, the fraudster retrieves it and withdraws the money from your account. Bank Negara is now working with the telecommunications operators to warn their subscribers via SMS not to fall prey to such scams. HOW TO AVOID BEING CONNED - Do not respond to any request for your login ID, password or PIN over the phone, through fax, email or pop-up messages. - Take down the name, phone number and any other information you can from the caller who asks for the information - Call your bank if you are not sure of the authenticity of a call, SMS or email. ATM machines also provide numbers that you can call. - You can also call the Association of Banks in Malaysia's toll-free hotline at 1300-88-9980 and Bank Negara's at 1300-88-5465. - Always enter the Universal Resource Locators (URLs) directly into the web browser. Avoid being redirected to the website or hyperlinked to it from an email or another website. - Ensure that you are in a secure website by checking the URLs to ensure that it begins with "https://'" instead of "http://'" and look for a display of a closed padlock symbol on the status bar of your browser. - Protect your personal computer from hackers, viruses and malicious programmes. Source: Bank Negara corporate communications director Abu Hassan Alshari Yahaya.   <table border="0" cellspacing="3" cellpadding="0" width="200" align="right"> </table>