

CUSTOMER TIPS: HOW TO GUARD AGAINST FRAUD WHEN USING ONLINE BANKING OR ATM'S



ATM Fraud - Watch out for the following scams.

Scam 1 - you find you are having difficulty with your card. Someone will come to your aid and likely wipe the card, put it in the machine and offer to 'try the number for you'. They will seem helpful and non-threatening. The chances are that they will switch cards on you or **clone** it and use your pin.

Scam 2 - as you approach the cash machine, people dressed in the bank's uniforms will tell you that you must swipe your card with them as the machine isn't working. They will swipe your card, cloning it, then try it in the cash machine. The card will work and they will offer to put the pin in for you or watch you do it.

Scam 3 - leaflet holders and the ATM's face can contain small cameras designed to catch your pin number. Remember there should be no loose wires, no containers or leaflet holders, and no loose fittings.

Scam 4 - your card gets stuck and a passerby suggests you try the pin one more time or may offer to try it for you. Then with no success the passer by offers to stand guard while you report it to the bank, or ask to retrieve the card from the machine inside the bank. The passerby gets the card from the machine and leaves with your pin number.

Other scams

- Be aware of hardware devices such as "key Loggers" which could have been placed in between the PC and Keyboard.
- Do not open any unknown emails or attachments
- Choose a user ID and password that cannot be easily guessed and change these regularly. Password should be combination of numerical and alphabetical characters.
- Check for the padlock in the lower right of your browser window (it indicates a secure site). You can click on this padlock to verify the site "owners"
- when you complete your online banking tasks, log off and close the browser window
- Never provide your password over the internet (by email) or over the telephone to anyone (including persons identifying themselves as bank officials. Banks will ask you to verify information and not to supply information)
- Don't trust a PDF payment proof unless verified by the bank - these documents can be manipulated by fraudsters.
- Conducting your banking and/or banks shopping with card details should never be done on a public computer.
- Only use recognized websites via authenticated web-links and do not click on "pop up" messages that appear while on websites.
- Be aware of "Phishing". Phishing is a fraudulent activity to obtain personal details like identity numbers, passwords and credit card information through unsolicited e-mail. Phishing e-mails ask the recipient to click on a link given in e-mail which takes the recipient to a "spoof" (false) website that asks for personal information.
- Always, manually type in Banks internet link address and never click on a link provided.

- When making card purchases, make use of sites that uses security questions for verification as part purchasing.
- Be aware of hardware devices such as “key Loggers” which could have been placed in between the PC and Keyboard.
- Do not do any money conversions with un-known people or institutions

How to avoid these scams You can avoid them!

- **PIN protection:** always protect your pin number, never write it down or give it to anyone.
- Card in your hand: have the ATM card for your transaction ready and in your hand. Opening your wallet or purse can be time consuming and provides a potential thief with easier access to your valuables.
- Cover keypad and security cameras: carefully cover the keypad while entering the number, and check where the security cameras are located. While many ATM have cameras, they won't be positioned to record the keypad
- Reject the offer: be wary of any offers of 'help' with ATM transactions, even if it appears the help is coming from a bank official.
- Confirm card and don't count cash: make sure the card you get back from the ATM after your transaction is yours, and don't count or expose your money after your transaction. As soon as you receive your money and bank receipt, put them away and leave the ATM area
- Lights out; don't use: only use ATMs in well-lit, high-traffic areas. If the lights aren't working, don't use that machine and stay alert.
- Report immediately: anything or anyone that seems suspicious or strange about the ATM. This could include anyone offering help, trying to look over your shoulder or taking pictures in the area. Also, call the bank right away if the machine retains the card. Do not allow someone you don't know to 'stand guard' while you report it in the bank

Internet Fraud – this has to do with fraudulent transactions which occur via the internet on your visa card, without the consent of the “real” cardholder.

In order to prevent and/or identify such transactions, kindly ensure to do the following:

1. **Statement Review** – review your statement(s) thoroughly on regular basis to ensure all transactions therein were authorized/undertaken by you.
2. **Password protection** – set passwords to contain both alphabets and numbers and change passwords on a regular basis.
3. **Unknown attachments** – to avoid unknowingly downloading malicious codes (Spyware); please refrain from opening any unknown email or attachments.
4. **Virus Protection** – keep your virus programs up to date in order to protect against the latest viral and malicious software attacks.
5. **Personal Information disclosure** - Never disclose Personal Information on e-mail or over the phone to any strange person/body. Banks will ask you to verify information and not to supply information.
6. **Public Usage** – never conduct your banking and/or shopping with card details on a public computer.
7. **Recognized websites** - only use recognized websites via authenticated web-links and do not click on “pop up” messages that appear while on websites.
8. **“Phishing”**- Phishing is a fraudulent activity to obtain personal details like identity numbers, passwords and credit card information through unsolicited e-mail. Phishing e-mails ask the recipient to click on a link given in e-mail which takes the recipient to a “spoof” (false) website that asks for personal information. Always, manually type in Banks internet link address and never click on a link provided.
9. **Secured sites** - when making card purchases, make use of sites that use security questions for verification as part of purchasing.
10. **Hardware devices** - be aware of hardware devices such as “key Loggers” which could have been placed in between your PC and Keyboard.

In addition to the above, please note the following if you travel abroad with your Visa Card.

1. Copy of cards - before leaving home; kindly make copy/copies of both sides of the card(s) you intend travelling with, as well as passports and travel itineraries. These details should then be left in safe keeping with a family member or friend.
2. Assistance - never accept any assistance at ATMs and beware of "shoulder surfing", which occurs when somebody is watching you entering your PIN.
3. ATM location - only use ATMs in well lit and populated areas and take note of people who may bump into you and pick your cards, wallet, cash, mobile phone etc.
4. Safe for cards and other important documents - If you have access to a safe in your chosen accommodation, use it for all your cards, important documents and valuables. Only go out with enough money, not all your money and only take one card with you if required.
5. Important Phone Numbers - keep a copy of all important phone numbers (for instance, number behind card and SCB's Contact Centre number) with you, preferably not on your mobile phone, in case you lose your phone.
6. Keep your branch informed - inform your branch of your travel dates and destinations so that suspicious transactions can be identified on time.
7. Keep your card at all times - do not let your card out of your sight in restaurants, bars, clubs, hotels or anywhere else you may use them.
8. Report immediately - if you suspect something untoward may have happened to your card(s), quickly call the SCB Contact Centre (+ 233 030 2667447) or the Visa Call Centre (toll free +1 410 581 9994) immediately, even if it is in the middle of the final!
9. Statement review – peruse your statement(s) and balances on an ongoing basis.

For more information, call 0302-740-100 or visit your nearest branch.