SBM

communiqué

Card Fraud Awareness

1. What is card skimming?

Card skimming is the copying of encoded information from the magnetic stripe of a card by fraudsters to create counterfeit cards to make illegal purchases and cash withdrawals to the detriment of the legitimate cardholders.

2. How do fraudsters skim cards?

Card skimming happens at the ATM or Point of Sale (POS) where the fraudsters conceal sophisticated devices on the card slot or use hand held devices to copy the card information. A small camera is often used to obtain your PIN or a person may be watching you while you are entering your PIN.

3. Where you need to be more vigilant?

You ALWAYS need to be vigilant, no matter where you are. But there are specific places where you need to be particularly alert:

- Restaurants
- Bars
- Hotels
- Retail stores / Supermarkets
- Petrol stations
- Other busy areas

You should also exert more precautions at remote ATM sites which are also vulnerable, especially at night.

4. When do you need to be more vigilant?

- During the festive season

It is a known fact that during festive seasons people have the tendency to:

  - Spend more money using their credit cards.
  - Visit crowded places to make purchases.

- When travelling.

Most skimming cases happen overseas.

5. How to protect yourself:

(a) Do not lose sight of your card when paying at the till – treat your card as you would for cash

(b) Do not lose sight of your card when you pay at a restaurant – request for the machine to be brought to your table else accompany your card to the POS machine.

(c) Make sure your card is swiped only once.

Hotline : 207 0111 [jours de semaine de 08h00 à 18h00]
E : sbm@sbm.intnet.mu | www.sbmgroup.mu

(d) Do not accept assistance from anybody at ATMs, even from security staff.

(e) Never assume your card has been retained by an ATM. Always contact the bank and request the card to be blocked immediately – a skimmed card can be replicated in minutes and used immediately.

(f) Do not share your PIN to anyone.

(g) Memorise your PIN and never write it down or store it electronically on your cell phone, tablet, laptop or any other portable/wireless devices.

(h) Do not keep your PIN and card together if you are unable to memorise the PIN.

(i) Protect your PIN - Always shield your hand when entering your PIN, regardless of whether you feel secure or protected.

(j) Stand close to the ATM and use your body as a shield as extra security to protect your card and PIN.

(k) Be on the lookout for anything suspicious at ATMs.

(l) Do not use an ATM if the area is unlit, if there are people lingering at the ATM and if you notice something suspicious.

(m) Register for the Mobile Banking Services so that you can monitor for unusual transaction on your account. Verify your account and card statements regularly.

(n) Save the bank's Customer Service number on your phone - +230 202 1256

(o) Report any suspicious activity / tampering at the ATM to the bank immediately.

(p) Inform Customer Service on +230 202 1256 whenever you are out of country and do give them a hint about the places you will be visiting.

(q) Apply for SBM E-secure password now if you are not enrolled yet in case you purchase online.

6. What to do if you think that your card has been skimmed?

If you suspect a skimming device is being used or that your account has been compromised, report it immediately to the Bank's Customer Service on +230 202 1256 or visit your nearest SBM Branch.

7. Have a question?

Call our Customer Service on +230 202 1256