



Credit and Debit Cards Security Tips

How to Safeguard Your Credit / Debit Card

- In the event the sealed package containing your credit/debit card is tampered/compromised, please contact UOB121 Phone Banking immediately at :-
Kuala Lumpur 03-26128 121
Penang 04- 2401 121
Johor Bahru 07 -2881 121
Kuching 082-287 121
Kota Kinabalu 088 - 477 121
- Upon receipt of your new credit/debit card, sign on the signature panel immediately using a non erasable ball point pen
- Ensure you know where your credit/debit card is at all times as it is as good as cash
- DO NOT lend your credit/debit card to anyone as it is exclusively for your own usage
- DO NOT give details of your credit/debit card number to unauthorized third parties especially during online or internet transactions
- Destroy your credit/debit card properly by cutting across the magnetic stripe and the chip in the event you wish to cancel your card and return it to the issuing bank
- DO NOT respond to email, website or phone inquiry requests for details of your credit/debit card
- DO NOT write down your PIN number at the back of your credit/debit card or keep it in your wallet. Memorize your PIN number
- DO NOT leave your credit/debit card lying around in your office or at home
- DO NOT leave your credit/debit card in your wallet or handbag unattended in your car when you go jogging, golfing, fishing, exercising or stop on highway rest areas



Credit and Debit Cards Security Tips

Before Signing the Transaction Slip

- Check the details on the transaction slip before signing to prevent any unauthorized charges
- Ensure that it is your credit/debit card that is returned to you after a card purchase
- Make sure that your credit/debit card is returned to you promptly after a purchase
- Keep your transaction slips to reconcile with your credit/debit card statement as soon as you receive it. If you discover any billing discrepancy, call your issuing bank immediately
- Never reveal or input your credit/debit card information in a website that is not secured
- DO NOT sign on a blank transaction slip to prevent unauthorized billings

When You Receive Your Monthly Credit/Debit Card Statement

- Check your monthly debit/credit card statement and reconcile with your transaction slips
- Contact UOB immediately if there is any discrepancy
- Notify UOB of any changes in address or contact number to allow us to contact you promptly for verification of transactions
- Keep UOB121 Phone Banking telephone lines for emergency reporting like lost, misplaced, stolen cards or unauthorized transactions

Report Lost / Stolen Credit Card

To report lost or stolen UOB credit card, kindly call 603 - 2612 8100

For more tips on fraud protection and credit card security, please click at the links below:

[My Money Skills- Card Security & Security Theft](#)

[Fraud Protection – How to use your card safely and securely](#)



Credit and Debit Cards Security Tips

Hi.....just to remind ourselves

Be sure to read Scene 3. Quite interesting.

This is a new one. People sure stay busy trying to cheat us, don't they?

Scene 1

A friend went to the local gym and placed his belongings in the locker. After the workout and a shower, he came out, saw the locker open and thought to himself, 'Funny, I thought I locked the locker....

Hmm, 'He dressed and just flipped the wallet to make sure all was in order.

Everything looked okay – all cards were in place.

A few weeks later his credit card bill came – a whopping bill of \$14,0000!

He called the credit card company and started yelling at them, saying that he did not make the transactions.

Customer care personnel verified that there was no mistake in the system and asked if his card had been stolen.

'No,' he said, but then took out his wallet, pulled out the credit card, and yep – you guessed it – a switch had been made.

An expired similar credit card from the same bank was in the wallet.

The thief broke into his locker at the gym and switched cards.

Verdict: The credit card issuer said since he did not report the card missing earlier, he would have to pay the amount owed to them.

How much did he have to pay for items he did not buy?

\$9,000! Why were there no calls made to verify the amount swiped? Small amounts rarely trigger a 'warning bell' with some credit card companies. It just so happens that all the small amounts added up to big one!



Credit and Debit Cards Security Tips

Scene 2

A man at a local restaurant paid for his meal with his credit card. The bill for the meal came, he signed it and the waitress folded the receipt and passed the credit card along.

Usually, he would just take it and place it in his wallet or pocket. Funny enough, though, he actually took a look at the card and, lo and behold, it was the expired card of another person.

He called the waitress and she looked perplexed. She took it back, apologized, and hurried back to the counter under the watchful eye of the man.

All the waitress did while walking to the counter was wave the wrong expired card to the counter cashier, and the counter cashier immediately looked down and took out the real card.

No exchange of words ---- nothing! She took it and came back to the man with an apology.

Verdict: Make sure the credit cards in your wallet are yours. Check the name on the card every time you sign for something and/or the card is taken away for even a short period of time. Many people just take back the credit card without even looking at it `assuming' that it has to be theirs.

FOR YOUR OWN SAKE, DEVELOP THE HABIT OF CHECKING YOUR CREDIT CARD EACH TIME IT IS RETURNED TO YOU AFTER A TRANSACTION!

Scene 3

Yesterday I went into a pizza restaurant to pick up an order that I had called in.

I paid by using my Visa Check Card which, of course, is linked directly to my checking account. The young man behind the counter took my card, swiped it, then laid it on the counter as he waited for the approval, which is pretty standard procedure.

While he waited, he picked up his cell phone and started dialing.

I noticed the phone because it is the same model I have, but nothing seemed out of the ordinary? Then I heard a click that sounded like my phone sounds when I take a picture.

He then gave me back my card but kept the phone in his hand as if he was still pressing buttons. Meanwhile, I'm thinking: I wonder what he taking a picture of, oblivious to what was really going on.



Credit and Debit Cards Security Tips

It then dawned on me: the only thing there was my credit card, so now I'm paying close attention to what he is doing.

He set his phone on the counter, leaving it open.

About five second later, I heard the chime that tells you that the picture has been saved. Now I'm standing there struggling with the fact that this boy just took a picture of my credit card.

Yes, he played it off well, because had we not had the same kind of phone, I probably would never have known what happened.

Needless to say, I immediately cancelled that card as I was walking out of the pizza parlor. All I am saying is, be aware of your surrounding at all times.

Whenever you are using your credit card take caution and don't be careless.

Notice who is standing near you and what they are doing when you use your card.

Be aware of phones, because many have a camera phone these days.

FORWARD THIS TO AS MANY PEOPLE AS YOU CAN THINK OF. LET'S GET THE WORD OUT! JUST BE AWARE. Never let your card out of your sightcheck and check again.

.....

Phishing is a way of attempting to acquire sensitive cardholder / customer information through popular social web sites, online payment processors or IT administrators to lure the unsuspecting public into believing that they are from genuine vendor or service provider. Phishing is carried out by e-mail and it directs users to enter passwords at a fake website whose look and feel are almost identical to the genuine one. There are even emails from Visa/MasterCard International to direct the unsuspecting public to link to the website. You are advised not to fall into such phishing scams.

Kindly take the following steps of action:

- Be suspicious of any email with urgent requests sent to you. Only your financial institution will verify or update you account status and not 3rd party service provider;
- Do not click on any email or account details links, if you are not sure of the originating sender;
- Avoid filling out forms in email that request for personal information;
- Always ensure that you're using a secure website when submitting credit card information;
- Be aware of phishing or spoofed or spam mails;
- Ensure that your browser is up to date and security patches are always in place to prevent unnecessary intrusion.