

# Internet Banking 101

## Overview

Internet banking can make your banking experience a lot more pleasant and convenient. Despite many Internet banking scams, it is possible to conduct your banking safe and secure by means of the Internet. The following seven golden rules will help you towards safe Internet banking.

## Internet Banking Rules

### 1. Protect your computer

*As a minimum every computer should run an anti-virus program and a firewall. Very good anti-virus and firewall software is available free of charge. Visit our website for more info.*

### 2. Have a good password

*A good password should contain UPPER and lower case alphabetic characters, numbers, and some special characters. Try using the first letter of every word in a sentence combined with a few "twists" like using the last word in full.*

*For example: My name is Bob and I like to eat = MniBaIl2e@t.*

### 3. Never share your banking user ID and password with anybody

*Your user ID and password conveys your online identity. If anybody else gets hold of that, they can steal your identity and conduct banking transactions on your behalf!*

### 4. Never conduct Internet banking on a computer you do not trust

*As many computer viruses and malware might be stored on the 'untrusted' computer, your user ID and password might secretly be read and sent to online robbers. They will misuse your user ID and password and steal you money.*

### 5. Never respond on a sms or email received from a 'bank'

*Phishing is a well-known technique used by online robbers to trick you into submitting sensitive information (like your user ID and password) via sms or email. Never respond, rather phone or visit the bank if you are unsure.*

### 6. Rather use a mobile phone contract than 'pay as you go'

*Most banks make use of an OTP (one time PIN) to confirm your Internet banking transactions. As most 'pay as you go' SIM-cards can be swapped telephonically, and those on a contract not, it is easier for an online robber to compromise your mobile phone if you are on 'pay as you go'.*

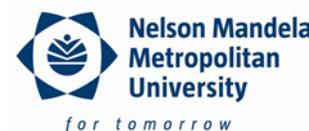
### 7. Limit 'available' funds on you accounts

*Many accounts, like credit card or bond accounts, have got huge amounts available for usage or transfer. Rather hide or remove such accounts or put such 'available' funds on 7- or 30-day notice.*

## Need more info?

We are very willing to help you meet your cyber safety needs. Please let us know what your needs are and we'll do our best to assist.

Contact the Cyber Security Research Unit at the Nelson Mandela Metropolitan University directly:



[cyberaware@nmmu.ac.za](mailto:cyberaware@nmmu.ac.za)

Or email the South African Cyber Security Academic Alliance:



[info@cyberaware.org.za](mailto:info@cyberaware.org.za)

## Our Website

For more information visit [www.cyberaware.org.za](http://www.cyberaware.org.za)