Guide

Protecting My Assets – Digital Banking Security

money savvy

www.moneysavvy.co.za

Digital Banking

1.1. What Is Digital Banking?

Digital banking is the moving of banking services that were previously provided manually in a branch to easily accessible platforms such as the phone and computers. Besides digital banking being convenient and cheaper for customers, banks are also moving to the digital way for the following reasons:

- Banks can improve customer relationships through digital engagement.
- Banking has now become available anywhere you are and any place in the world.
- It is a new marketing platform to attract customers and to cross sell the banks various products.
- It affords the customer the convenience of banking anywhere, anytime. These benefits can be passed on to customers.

1.2. Digital Banking Options

Digital banking allows you to send and receive money, manage your money, and buy goods and services faster and at a cheaper cost than walking into a branch to deposit or withdraw money. It also allows you the freedom to bank when and where you choose.

Online banking allows you to handle banking transactions safely and securely (you need a username and a secure password) without leaving the comfort of your home. Online banking gives access to online statements, allows you to make payment to other people or institutions and purchase airtime, change your balances and so much more.

Cell phone banking has enabled many customers to access their banking account from their homes without internet connection.

Contactless payment allows you to pay for goods and services without a Personal Identification Number (PIN) or signature by holding your smart device near a contactless reader or tapping your smart device on a contactless reader.

Card less payment (geo payment) allows you to transfer money from your app to the app of another user.

Card less ATM withdrawals are now possible. Send money via SMS pin code and the user withdraws from the ATM without having a bank card.

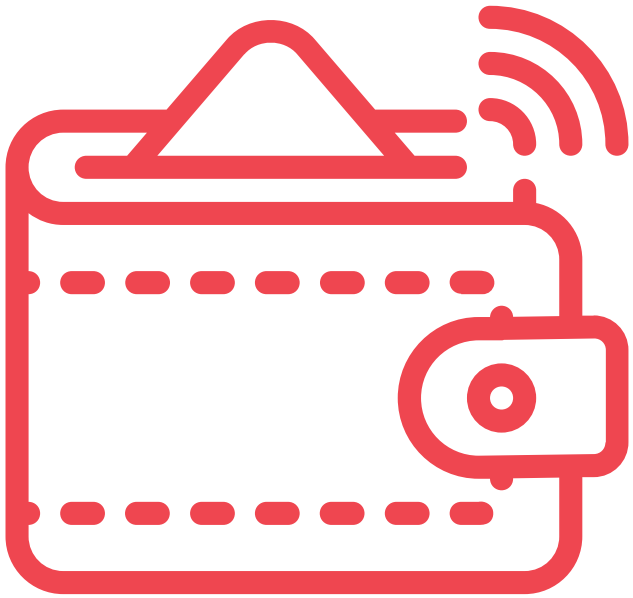
E -Wallet enables you to use your cell phone to make payments. You can send money to a cell phone number. The cell phone number becomes your account number. A pin is sent to the phone. You use the account number and the pin at an ATM to make a withdrawal.

You can simply scan a **QR code** with your smart phones at shops and restaurants to make a payment.

Digitisation has changed the way we make and receive payments.

1.3. What Is Digital Banking Security?

Digital security aims to protect your digital identity. Your digital identity is the online equivalent of your physical identity. Digital security is the tools used to protect your identity, as well as your assets in the online and mobile environment. These tools include anti-virus software, web securities, biometrics, the SIM card in your cell phone, username, unique passwords, the secure chip on your bank card.



1.4 How Safe Is Online Banking?

The banks will provide secure banking sites for safe and secure financial transactions. Safe online banking relies on you to make good choices and avoid costly surprises by becoming a victim of an online scam, theft, and fraud. It is important to learn about and take advantage of the security features offered by your bank.

Online living has become the norm and we spend more time online doing our banking and personal financial activities.

What banking scams do you need to look out for?

- **Phishing**- An attempt to steal personal details via email, fake websites, or SMS's. By enticing you to click on a link (that you do not know the source of), the scammer attempts to lead you to a fake website where you will be required to enter sensitive personal information (username, password, credit card details). The scammer will use this information to carry out fraudulent transactions (e.g., credit card fraud).
- **SIM swap**- When a criminal cancels your SIM card and links your number to a new SIM, to gain access to your OTP's.
- **Skimming**- When the numbers on your Credit Card are recorded and transferred to a duplicate card.
- **Vishing** is the attempt to steal personal detail using the telephone to scam the user into giving them personal information that will be used for identity theft. The scammer usually pretends to be a legitimate business and fools the victim into thinking he or she will profit.
- **Data theft** – This is when customer information (username, passwords, PIN, credit card detail, identity number, addresses) are stolen or copied illegally. This information is used to commit fraud.

Identity Theft

Identity fraud means that someone has managed to obtain your personal information and use it for their own personal gain. With your ID number, address, and some personal information it's easy to open accounts and get access to credit with other people's identity documents. With the growth of online identity theft is becoming more and more prevalent.

2.1 Safety On Social Media

Social media accounts are regularly hacked. Look out for language or content that does not sound like something your friend would post. Be careful about what you share. Don't reveal sensitive personal information i.e.: home address, financial information, phone number. When people ask for money, send a message to your friend to ensure the message really was from them.

2.2 Password Protection

- Don't have the same password for social media and banking sites
- Change passwords on a regular basis
- Don't use your name and numbers to create your password
- Don't use significant dates, names for your password
- Don't access private sites like banking sites in internet cafes

2.3 Benefits Of Mobile/ Cell Phone Banking

- Banking anytime, anywhere all you need is data or internet
- Instant access to cash without a bank card
- Multiple payment options
- Safe and secure if you protect your mobile device well
- No more standing in queues to do basic banking tasks like having a bank letter to authenticate your bank account.