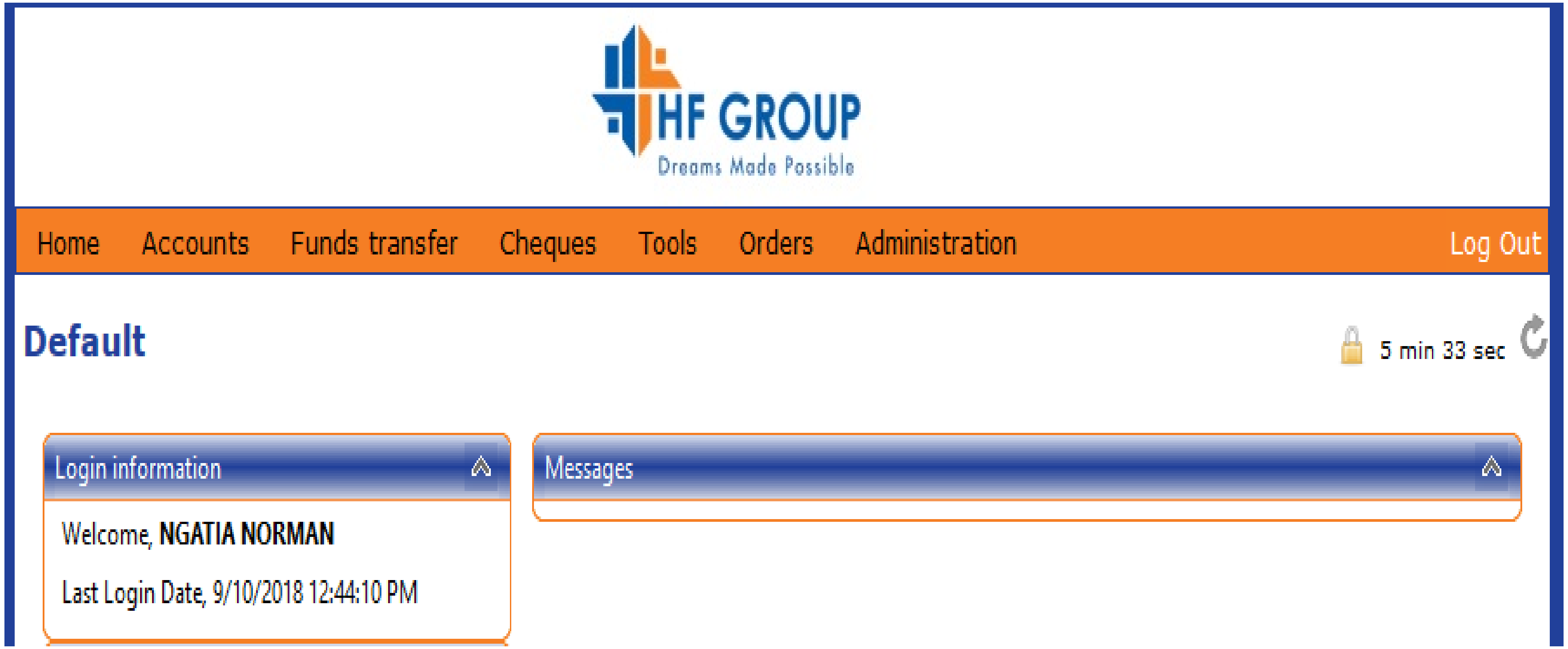
Tips on Internet Banking Security

1. Confirm Your Last Login

Always check the log in information on the welcome page of Internet Banking which shows you the most recent activity using your log in details. If date and time for the last login is different from your ACTUAL last login, report this immediately to HF Call Centre on +254 709438888 or email customer.service@hfgroup.co.ke. See below screen displaying "Your Last Login" details on the welcome page.

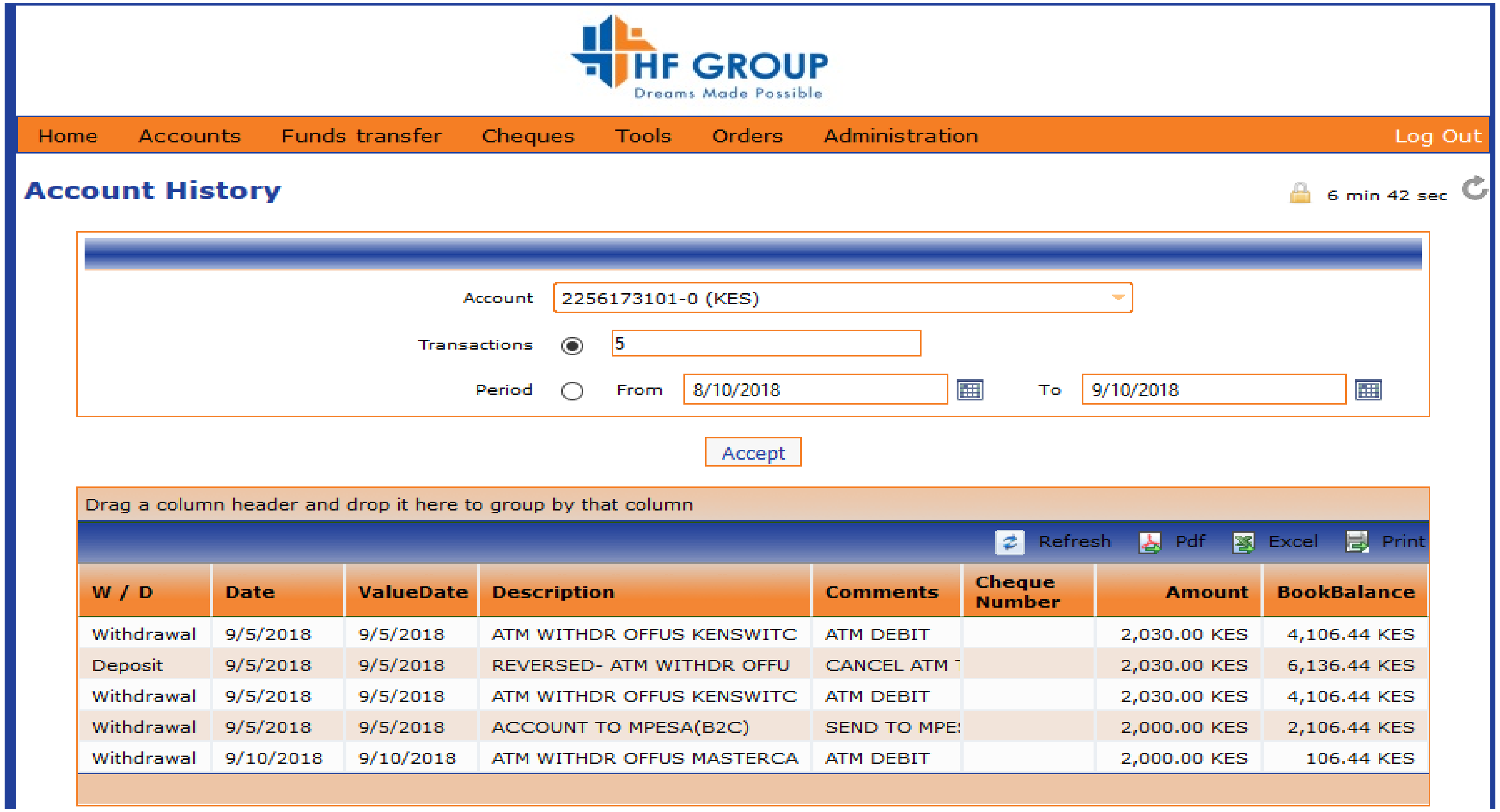


Welcome, NGATIA NORMAN

Last Login Date, 9/10/2018 12:44:10 PM

2. Monitor your internet banking account transactions

The **Last Five Transactions** menu on your home page will give you an opportunity to confirm if there are any fraudulent transactions. See below screen on how this is accessed. Any suspicious account should be reported to HF Call Centre on +254 709438888 or email customer.service@hfgroup.co.ke.



Account History

Account 2256173101-0 (KES)

Transactions ● 5

Period ○ From 8/10/2018 To 9/10/2018

W / D	Date	ValueDate	Description	Comments	Cheque Number	Amount	BookBalance
Withdrawal	9/5/2018	9/5/2018	ATM WITHDR OFFUS KENSWITC	ATM DEBIT		2,030.00 KES	4,106.44 KES
Deposit	9/5/2018	9/5/2018	REVERSED- ATM WITHDR OFFU	CANCEL ATM 1		2,030.00 KES	6,136.44 KES
Withdrawal	9/5/2018	9/5/2018	ATM WITHDR OFFUS KENSWITC	ATM DEBIT		2,030.00 KES	4,106.44 KES
Withdrawal	9/5/2018	9/5/2018	ACCOUNT TO MPESA(B2C)	SEND TO MPE:		2,000.00 KES	2,106.44 KES
Withdrawal	9/10/2018	9/10/2018	ATM WITHDR OFFUS MASTERCA	ATM DEBIT		2,000.00 KES	106.44 KES

Tips on Internet Banking Security

3. Avoid becoming a victim of phishing

- ❖ Do not respond to emails from people/places that you do not recognize. HFC will never send you an unsolicited e-mail containing a link to any of its log–on pages. If you receive one, it will not actually be from the bank and should be deleted immediately.
- ❖ Do not click on any links – always type the full internet banking website address e.g. *https://internetbanking.hfgroup.co.ke/iProfits2PROD* rather than click a link. Disable the 'Autocomplete' within your browser.
- ❖ Do not enter personal information into websites that you do not know and/or do not trust
- ❖ Do not send sensitive information (such your user name and PIN) via email. Please note that HFC will NEVER send you an email asking you to enter, reconfirm or change your security details or other personal information. If you receive such an email or if you believe you may have disclosed your details in any way, please report to HF Call Centre on +254 709438888 or email customer.service@hfgroup.co.ke.

Tips on Internet Banking Security

5. Maintain good computer and mobile phone security

- **Keep your operating system and browser patches up to date -** these include important security enhancements, which now assist with the detection of phishing sites and malicious software.
- **Install and maintain up-to-date anti-virus and anti-spyware software** - such software can reduce the likelihood of someone accessing your personal information stored on your personal computer/laptop.
- **Use a personal firewall -** A personal firewall is another small program that helps protect your computer and its contents from outsiders on the internet. When installed and correctly configured, it stops unauthorized traffic to and from your computer. There are many effective programs to choose from. Common commercial examples include Windows Firewall and Check Point Zone Alarm (free), McAfee Personal Firewall and Norton Personal Firewall.

6. Avoid unsecured access to Internet Banking

- Do not use Internet Banking on public computers, or via an unsecured Internet connection (including free WiFi)

7. Practice good password/pin security

- It is important to keep your access codes confidential. This includes your Internet Banking Password and PIN. A good security precaution is to change your passwords regularly. Passwords should not be easy for anyone else to guess (whether they are family, friends or strangers).
- Use discretion when sharing information online, and never share passwords or security codes with anyone. Personal information can be used by fraudsters to verify themselves and make unauthorized changes to accounts