Tips to safeguard against Fraud

PUBLIC NOTICE

Vodafone M-Pesa Limited is an authorized payment and settlement system under the Payments and Settlement Systems Act, 2007. We issue semi-closed system Prepaid Payment Instruments to Users/Holders (like yourself) on which they can load and transfer funds in Indian Rupees within India and to make purchases and or avail of certain services ("Services") as defined in the detailed Terms and Conditions made available on our website.

Tips for Safe and Secure transactions @ M-Pesa

1. Safety from Fraud Calls

If you get an SMS or call asking for personal or M-Pesa account related information, like PIN or OTP or user ID etc., please do not provide this information. Report it to M-Pesa, be suspicious of any caller who appears to be ignorant of basic personal details like first and last name.

2. Safe usage of M-Pesa Application

- Set up a strong 4 digit Pin and password of your choice to access M-Pesa. For ex: we recommend that it should not be 1111 or 2222 or 1234 etc
- If you have to share your mobile with anyone else or send it for repair/maintenance: Clear the browsing history, cache and temporary files stored in the memory as they may contain your account numbers and other sensitive information.
- Do not save confidential information such as your bank account number, debit/credit card numbers, CVV numbers or PIN's on your mobile phone.
- Keep your mobile's operating system and applications, including the browser, updated with the latest security patches and upgrades.
- Do not enable auto-fill or save user IDs or passwords.
- Turn off wireless device services such as Wi-Fi, Bluetooth and GPS when they are not being used.
- Avoid using unsecured Wi-Fi, public or shared networks.
- Be extra careful while typing confidential information such as your account details and password on your mobile in public places.

3. Safe M-Pesa Portal usage

- Communicate personal information only via secure web sites - When directing online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".

- Do not open spam mails. Be especially cautious of e-mails coming from unknown sources.
- Check your statements regularly to ensure that no unauthorized transactions have been made.
- Protect your computer by installing effective anti-virus / anti-spyware / personal firewall on your computer and update it regularly.
- If you received an email asking for personal or credit/debit card information, please do not provide this information no matter how 'genuine' the page appears to be. Such pop-ups are most likely the result of malware infecting your computer. Please take immediate steps to disinfect your device.
- M-Pesa or their representative will never send you emails or SMS to get your personal information, password or one time SMS (high security) password. Such e-mails or SMS are an attempt to fraudulently withdraw money from your account through Internet Banking.
- In case you have used a cyber cafe / shared computer, change your passwords from your own computer.

In case you fall victim to any such instance of fraud you can reach us on the following available modes and report any fraudulent transaction immediately.

Email - fraudsupport.vmpl@vodafone.com
Phone – 079-71250017

Please also note that this dedicated hotline is for transaction blocking purposes, and has been setup specially to ensure that customers, card holders and banks are able to transmit information on fraudulent transactions without any delay and with ease.

If someone has reported a misuse of their Credit Card / Debit Card or Net Banking for any kind of transaction on M-Pesa, we request you to kindly send the transaction details to fraudsupport.vmpl@vodafone.com so that we can expedite the verification.

We also advise you to register a Complaint / FIR at nearest Police station / Cyber cell and send us a copy of the same so as to initiate any reversal of funds subject to availability in M-Pesa wallets. Please note any reversal will be made to the source Debit / Credit card / Bank account.