Security Advisory: New Malware (22nd March 2013)

Dear customers,

We would like to inform you of a recent discovery of new malware attacks targeting internet banking websites and mobile banking applications. The malware infects customers' computers or devices and will attempt to steal customers' login and transaction authorisation information such as the Username, Password and One-Time-password (OTP).

If your computer is infected by the malware, you may encounter unusual requests for personal or account information while logging onto your bank account online or via the mobile banking application. Here are some possible ways that the malware may try to steal this information:

Indicators that your computer is infected with malware	Normal online banking process
You may be prompted repeatedly for login information even after you have entered them.	You will only be prompted once for login information.
You may be asked to enter login information (Username, Password, One-Time-Password (OTP)) on a single page.	The legitimate UOB Internet Banking has a 2-page login process. The first page requests for your Username and Password and the second page requests you to enter your One-Time-Password (OTP).
You may be asked to press an incorrect button on your hardware token to generate a One-Time-Password (OTP). E.g. the fraudulent screen will ask you to press the ⏶ button on your hardware token during login.	You will be asked to press the ⏻ button on your hardware token for login purposes.
You may be prompted to enter the One-Time-Password (OTP) from your SMS or hardware token even if you did not perform any online or mobile transactions from your account.	You will only be prompted to enter the One-Time-Password (OTP) from your hardware token or your SMS if you add payee(s) or perform any other online transactions in your account.
You may receive SMS or email alerts for transactions you did not perform.	SMS or email alerts on transactions will only be sent if you have performed a transaction.

Please inform our contact centre immediately at 1800 222 2121 (or +65 6222 2121 if calling from overseas) if you encounter any of the following situations:

- You receive SMS or email notifications for transactions that you did not perform or payees that have been added to your account that you do not know.

- You experience difficulty accessing your account after you have entered your login information or see repeated login requests.

We would like to assure you that our UOB Internet Banking website and mobile application remain secure and are not the source of this malware. Customers are reminded to stay vigilant when banking online. Below are a few tips and guidelines to protect yourself against such malware attacks: -

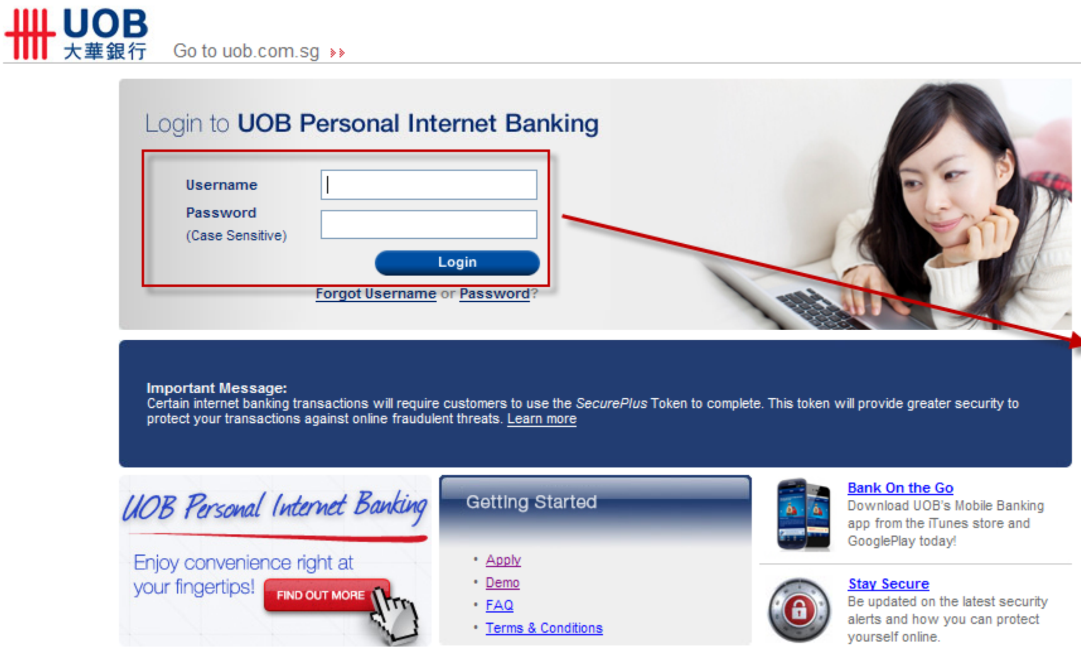
- Protect your computer and mobile device from being infected by installing anti-virus software, and updating it regularly with the latest anti-virus signatures.

- o Manually type out the full website address of the internet banking site (http://www.uob.com.sg) and verify that the site is authentic before entering your Username and Password.
- o For mobile devices, always download the legitimate UOB Mobile Banking application from authorised sources such as Apple App Store or Android Google Play Store. You are also advised not to access Mobile Banking using 'jail-broken' or 'rooted' mobile devices (i.e. the phone's Operating System has been tampered with), as it poses potential risk of malicious software infection.
- o Check your last login and transaction history regularly for any suspicious or unauthorized transactions.
- o Do not enter any One-Time-Password (OTP) if you did not initiate or request any transaction.
- o Verify the transaction details in the SMS or email alerts that the messages reflect your transactions.
- o Avoid visiting unknown and unsecured websites and avoid downloading unknown mobile applications.
- o Do not open unknown or suspicious attachments, or click on website links sent to you via emails, even if they are from senders you know.

If you suspect that your computer has been infected by the malware, you are advised **NOT** to proceed with your online or mobile banking activities until your computer or device has been checked and disinfected.

As a precautionary measure, we suggest changing your password immediately for your UOB Internet Banking or Mobile Banking before continuing with any online or mobile banking transactions.

Legitimate UOB Personal Internet banking website:

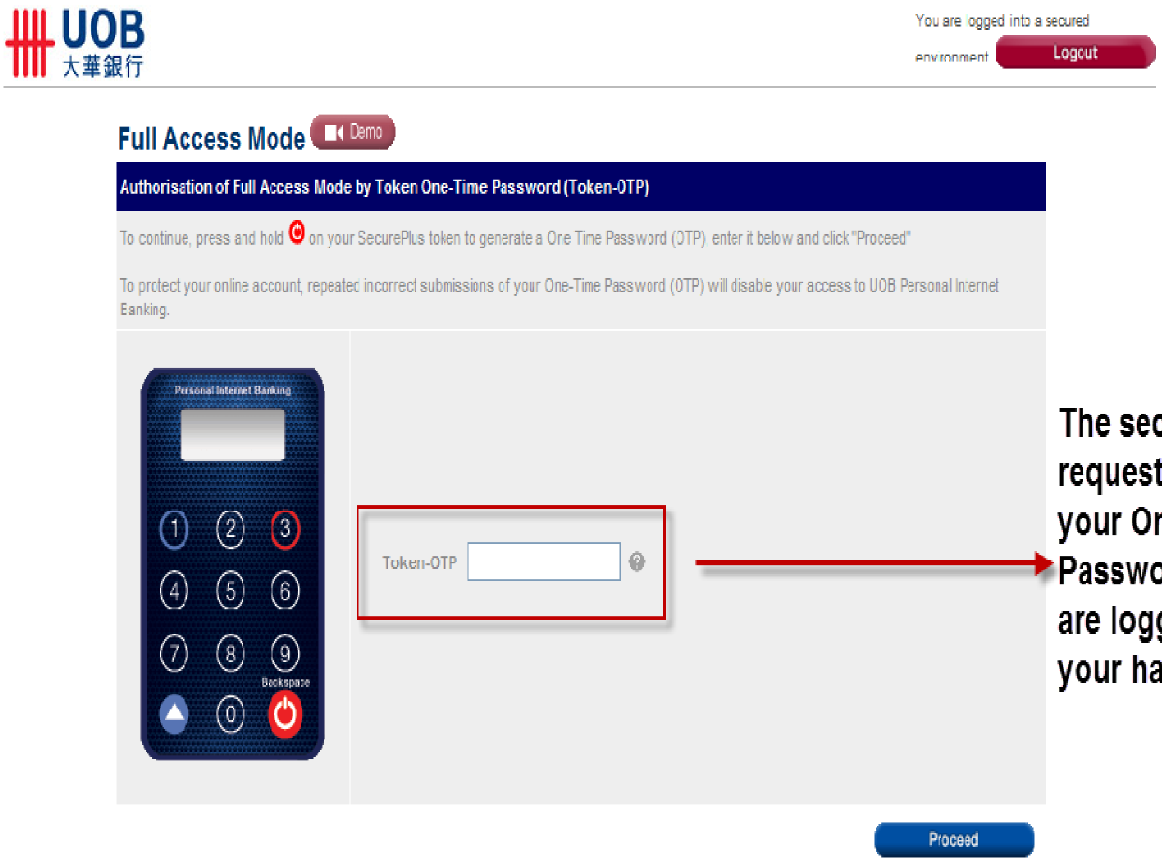


Important Message:
Certain internet banking transactions will require customers to use the *SecurePlus* Token to complete. This token will provide greater security to protect your transactions against online fraudulent threats. Learn more

Download UOB's Mobile Banking app from the iTunes store and GooglePlay today!

Be updated on the latest security alerts and how you can protect yourself online.

The legitimate UOB Internet Banking has a 2-page login process. The first page requests for your Username and Password



UOB 大華銀行

You are logged into a secured environment.

Full Access Mode

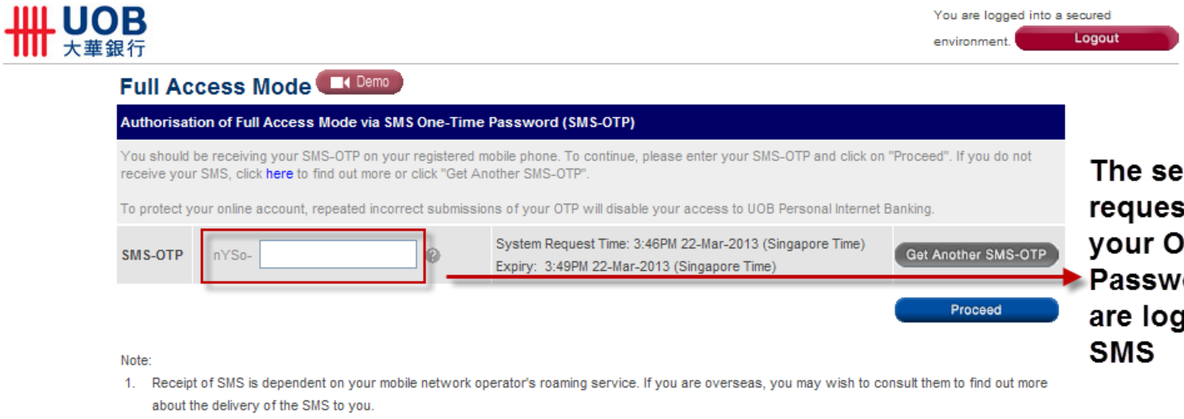
Authorisation of Full Access Mode by Token One-Time Password (Token-OTP)

To continue, press and hold on your SecurePlus token to generate a One Time Password (OTP), enter it below and click "Proceed"

To protect your online account, repeated incorrect submissions of your One-Time Password (OTP) will disable your access to UOB Personal Internet Banking.

Token-OTP

The second page requests you to enter your One-Time-Password (OTP) if you are logging in with your hardware token



UOB 大華銀行

You are logged into a secured environment.

Full Access Mode

Authorisation of Full Access Mode via SMS One-Time Password (SMS-OTP)

You should be receiving your SMS-OTP on your registered mobile phone. To continue, please enter your SMS-OTP and click on "Proceed". If you do not receive your SMS, click here to find out more or click "Get Another SMS-OTP".

To protect your online account, repeated incorrect submissions of your OTP will disable your access to UOB Personal Internet Banking.

SMS-OTP nYSo-

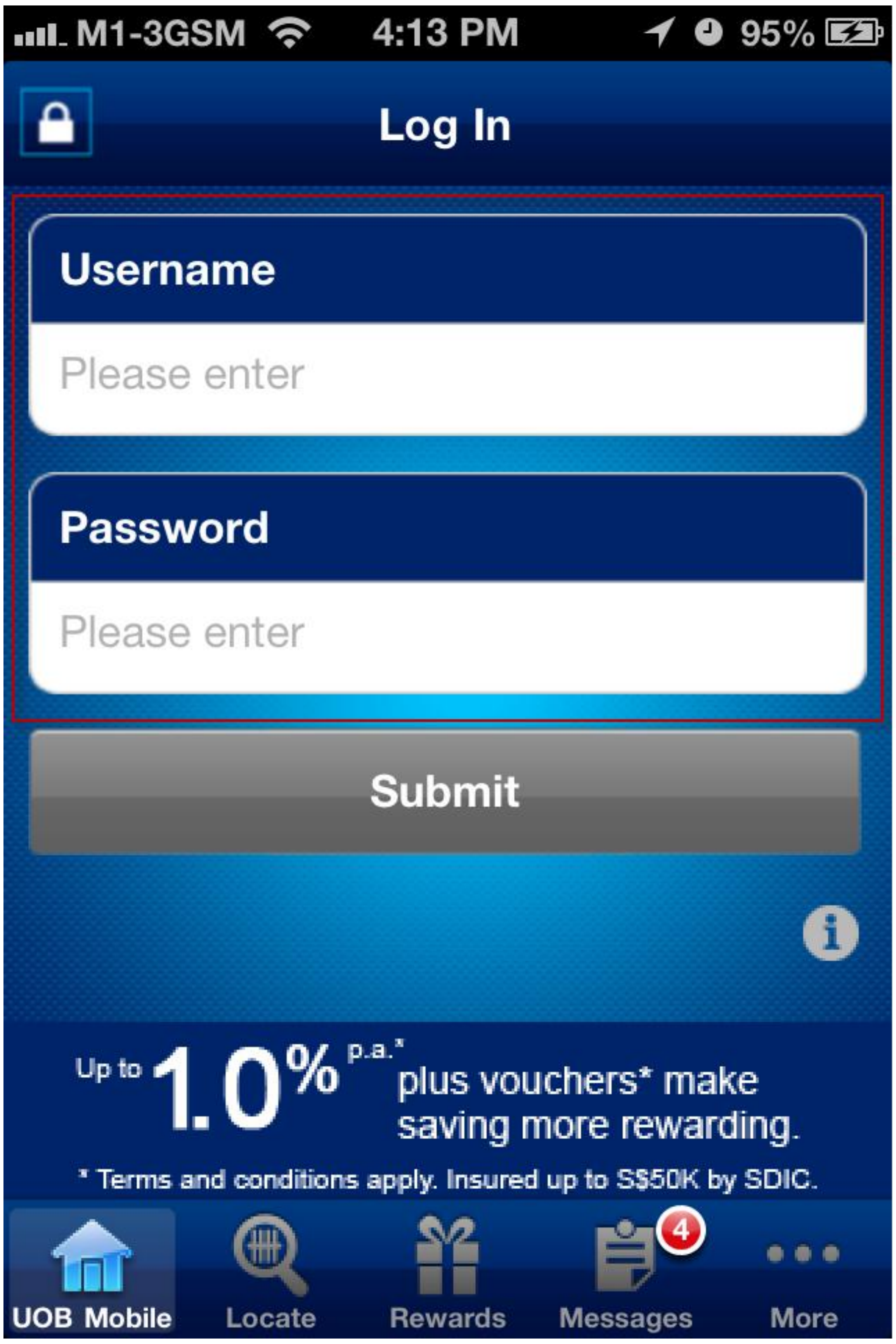
System Request Time: 3:46PM 22-Mar-2013 (Singapore Time)
Expiry: 3:49PM 22-Mar-2013 (Singapore Time)

Note:

1. Receipt of SMS is dependent on your mobile network operator's roaming service. If you are overseas, you may wish to consult them to find out more about the delivery of the SMS to you.

The second page requests you to enter your One-Time-Password (OTP) if you are logging in using SMS

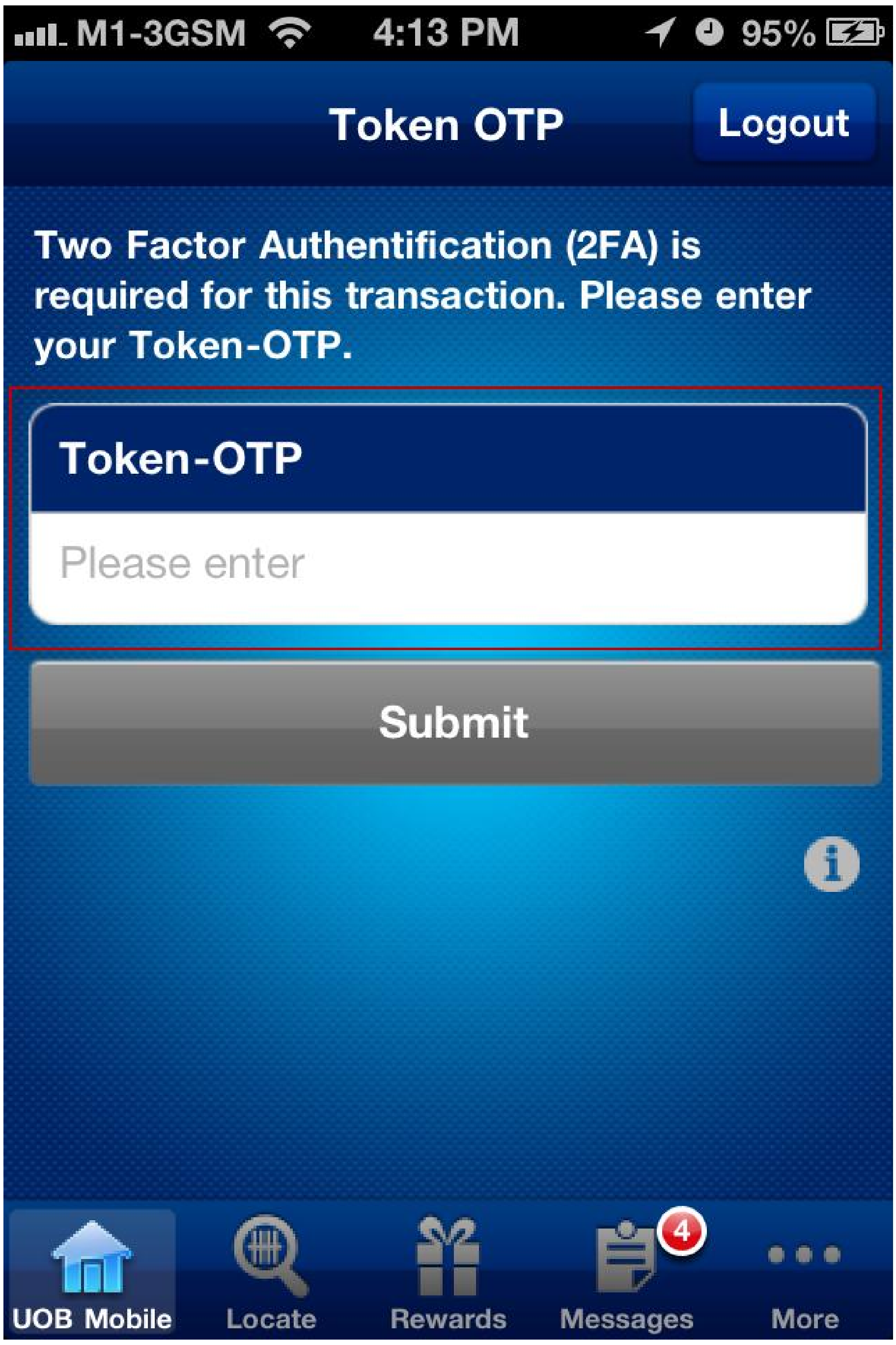
Legitimate UOB Mobile banking application:



Up to 1.0% p.a.* plus vouchers* make saving more rewarding.

* Terms and conditions apply. Insured up to S$50K by SDIC.

The legitimate UOB Mobile Banking has a 2-page login process. The first page requests for your Username and Password



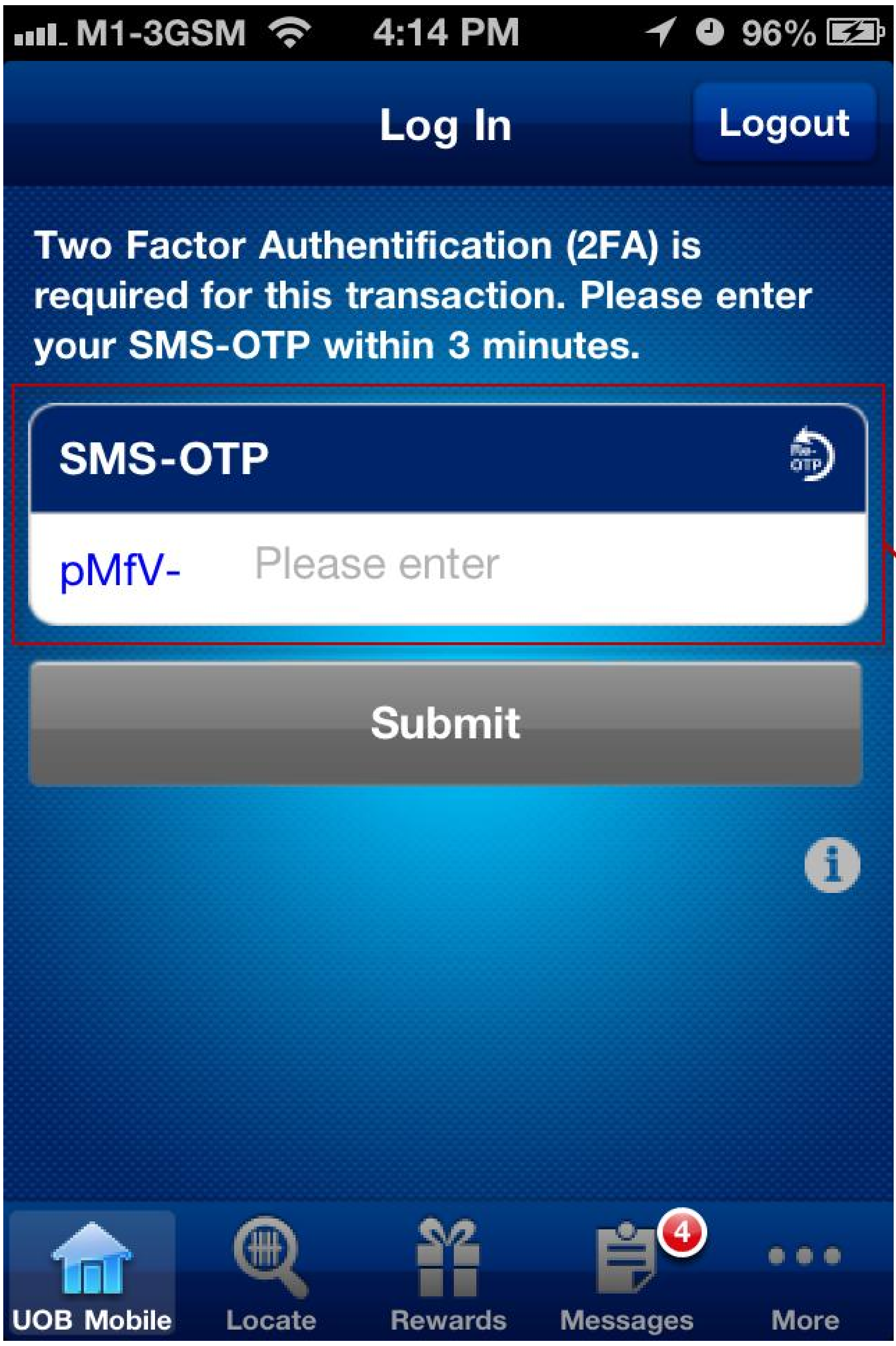
Token OTP

Two Factor Authentification (2FA) is required for this transaction. Please enter your Token-OTP.

Token-OTP

Please enter

The second page requests you to enter your One-Time-Password (OTP) if you are logging in with your hardware token



Two Factor Authentification (2FA) is required for this transaction. Please enter your SMS-OTP within 3 minutes.

SMS-OTP

pMfV- Please enter

The second page requests you to enter your One-Time-Password (OTP) if you are logging in using SMS