Security Precautions for Mobile OTP Token

1. About the Application

Official name, version, and download page of the application :

➢ Application Name : COMSUITE OTP Token
➢ Version   : Android : 1.1.2 / iPhone: 1.1.1

Official App Store and Google Play download link and QR Code : (Application is free)

Android	iPhone
GET IT ON Google Play	Download on the App Store

【Caution】

✧ Download only from the official link/QR Code provided above.
   Do not download from third-party app stores or other unofficial sites.
✧ Before downloading, please confirm that the correct application is selected by
   re-checking with the name and version posted above.
✧ Once the application is installed, please continue to update to the latest version as
   soon as they become available.

2. SMS Sent by MUFG Bank for Activation of the Application

Please be reminded that MUFG Bank will never send an SMS with clickable links requesting customers to enter customers' account information and/or login information.
Customers will only receive SMS for activation or one time password from MUFG Bank. Please be very careful in handling unexpected SMS requesting for personal information or providing a link to access. Such messages are high possibility of being malicious, spoofing or SMS phishing.

3. Lost, Theft, or Change of Smartphone Device

Please be extra careful to prevent smartphones from misplacement or theft.
If the smartphone with the application installed is lost or stolen, please contact your contracting office or MUFG Bank Helpdesk immediately.

MUFG Bank Helpdesk : https://www.bk.mufg.jp/ebusiness/e/ebiz/helpdesk.html

Please consider countermeasures such as setting strong passwords on the smartphone device, etc., to minimize the damage in the event the device becomes lost or stolen. Please make sure to delete the application when deciding to change, sell, or cancel the smartphone contract.

4. General Usage Security Precautions

Whilst MUFG Bank takes all possible steps to ensure the highest security of theapplication, please find below our general recommendations to maximize security when accessing the internet from smartphone devices.

- Set Android devices so that it will NOT install "Applications from unknown sources".
- Carefully check the access permissions when installing applications on Android devices.
- Do not use free public WIFI.
- Do not use the application in public places such as cafes etc., where there are strangers. Instead, use the application where business is exercisable safely such as home or office.
- Manage passwords for the smartphone devices and for internet banking login.
- Consider using anti-virus software/application.

5. Discontinuing Usage of The Application

Please make sure to delete the applications when deciding to discontinue using.

-iPhone and App Store are trademarks of Apple Inc., registered in the U.S. and other countries.
-Android and Google Play are either registered trademarks or trademarks of Google LLC.
-Any other company and product names are either registered trademarks or trademarks of their respective companies.

END