安全須知

Security Notice

妥善保管個人密碼及個人資料
Please do keep your Personal Identification Number and Personal Data properly.

客戶有責任採取合理措施，確保您所使用的密碼安全且保密。在設定密碼時，敬請您特別注意下列各點：
Customers have responsibility to adopt reasonable measures to ensure that the Personal Identification Number you use is secured and confidential. When setting up a Personal Identification Number, please pay special attention to the following points:-

■ 當收妥密碼函件後，應盡快透過網上銀行更改密碼，然後將密碼函件銷毀。

When receiving the “Notification of your Personal Identification Number”, you should access the TSB online service and change your Personal Identification Number, and then destroy the “Notification of your Personal Identification Number”.

■ 請勿於不同的網路銀行使用同一組密碼。
Please do not use the same Personal Identification Number for different internet banking service platforms.

■ 請勿使用懶人密碼。
Please do not use a weak Personal Identification Number.

切勿選用容易被猜中的密碼，例如連續或相同的數字或英文字如 12345678、11111111、ABCDEFGH。
Do not use Personal Identification Number that is easily to be figured out. For example, using consecutive or same numbers or characters such as 12345678, 11111111, ABCDEFGH.

■ 請勿使用與您個人資料相關的密碼。
Please do not use a Personal Identification Number which is related to your personal data.

例如您的名字、出生日期、電話號碼等。
For example, your name, birth date, contact phone number and etc.

■ 請勿寫下密碼。
Please do not write down your Personal Identification Number.

我們的建議是使用者代號或密碼應牢記腦中，無論任何時刻，您都不應用筆寫下或用其他方式記下密碼。但如果您需要記下密碼，請確保用來寫下／記下密碼的方法不會讓他人輕易取得或推斷到密碼。
We suggest you to remember your User ID or Personal Identification Number in your brain. No matter when, you should not handwrite your Personal Identification Number down or remember your Personal Identification Number in other ways. But if you need to remember the Personal Identification Number, please make sure that the way how you write down or memorize your Personal Identification Number won’t be obtained or figured out by others easily.

■ 請定期變更密碼。
Please change the Personal Identification Number periodically.

請經常不定時變更密碼，且避免重複使用已用過之密碼。
Please change the Personal Identification Number from time to time and please avoid using the Personal Identification Number which you’ve used before.

■ 請務必將一般網站的密碼，與網路交易的密碼特別區分。
Please do classify the Personal Identification Number for the use of general websites and for the use of online trading.

一般網站的密碼可能為明碼，較容易被人猜中或盜用，需特別注意。
The Personal Identification Number for the use of general websites may be unhidden and may be easily to be figured out of stolen. Please pay special attention to it.

■ 請勿向任何人透露密碼，包括銀行職員及警方。
Please do not reveal your Personal Identification Number to anyone including bank staffs and the police.

■ 切勿在公共場所（如網咖或圖書館）使用網路銀行服務，因為這些地方的電腦極有可能安裝了駭客程式，因而使您的密碼外洩。

Please do not use the online banking service in public (ex. internet cafes or libraries), since the computers in these places may be installed with hacker programs which may cause to leak Personal Identification Number.

您可藉由瀏覽器網址列的鎖頭標誌
You may click on the lock icon on the address bar of the browser

查閱網路銀行交易網站的數碼證書有關資料，來辨識是否為正確網站。
to check the relevant information of the digital certificate of the online banking transaction website to identify whether it is the correct website.

關於防範偽造網站
Regarding preventing fake websites:

請注意本行網路銀行之網址為 https://www.taishinbank.com.tw/nb/TIBSGWeb，務必確認您是連上本行的正式網站。
Please note that the website address of our bank’s online banking service is https://www.taishinbank.com.tw/nb/TIBSGWeb. Please make sure that you are connecting the official website of our bank.

■ 每次進入系統應在瀏覽器上輸入網址或將真正的網站記錄在瀏覽器的「我的最愛」中，藉由此兩種管道連結到本行網路銀行的入口。
Every time your login our bank’s online banking service website, you should enter the website address on the browser or add the real website address into your “Favorites” and to login to our bank’s internet banking via these two channels.

■ 除非您已完全確定登入本公司網站，否則不應提供任何有關您的交易帳戶的資料。
Unless you’ve completely login to our bank’s internet banking website, or you should not provide any of data of your transaction account.

■ 您應對其他網上詐騙活動經常保持高度警覺，以免受騙，招致無謂損失。
You should usually keep high alert to other online fraud cases so as to avoid being cheated and cause any unnecessary loss.

電腦的保安措施
Security measures of the computer.

您應確保您的個人電腦是安全的，並採用適當措施保護電腦，您可採用的措施如下：
You should make sure that your personal computer is secured and adopt proper measures to protect your personal computer. Measures you may adopt are as below:-

■ 請定期執行使用者電腦之安全套件更新及增修版程式。一些常用的電腦軟體時常都會發現安全漏洞，一旦發現這種情況，軟體出版商便會推出「增修版程式」供用戶使用來防堵這些漏洞，如用戶電腦未安裝增修版程式，病毒和駭客便可利用此安全漏洞進入這些電腦，盜取資料。
Please run the update and revision program of security software of the user's computer regularly. Some commonly used computer software often finds security loopholes. Once such a situation is discovered, the software publisher will launch an "enhanced version" for users to use to prevent these loopholes. For example, if the user's computer does not install an enhanced version, viruses and Hackers can use this security loophole to enter these computers and steal data.

■ 請為您的電腦安裝病毒偵測軟體，並定期更新版本、安裝最新的病毒定義檔，以有效保障電腦免受病毒侵襲。
Please install anti-virus software in your computer, update the version regularly and install the latest virus definition files, so as to protect your computer from being attacked by viruses effectively.

■ 請注意，病毒、特洛伊軟件及駭客程式可透過電子郵件傳播，蠕蟲病毒更可將病毒複製及發送至電郵地址簿上各收件人。因此，閣下不應開啟並即時刪除來歷不明的電子郵件，亦不要透過電子郵件提供的超連結登入電子交易服務。如需開啟電子郵件內的附件，亦應先進行病毒掃描。另外，騙徒亦會藉電郵進行不法活動。
Please note that viruses, Trojans, and hacker programs can be spread via e-mail, and worm viruses can also replicate and send the virus to each recipient in the e-mail address book. Therefore, you should not open and should immediately delete emails from unknown sources, and do not log in to online trading services through hyperlinks provided by emails. If you want to open the attachment in the email, you should also execute a virus scan first. In addition, fraudsters also use emails to conduct illegal activities.

■ 請安裝個人防火牆，防火牆是一種小程式，可助保護您的電腦系統不會在連接網際網路時受到入侵，或所載內容被人擅自盜用。安裝了防火牆，即可阻止資料在未經您授權下上傳或自您的電腦下載。
Please install a personal firewall. A firewall is a small program that can help protect your computer system from being invaded when connected to the Internet or the content contained in it is stolen without authorization. A firewall is installed to prevent data from being uploaded or downloaded from your computer without your authorization.

行動裝置的保安措施
Security measures of mobile devices

您應確保您的行動裝置是安全的，並採用適當措施保護行動裝置，您可採用的措施如下：
You should make sure that your mobile devices are secured and adopt proper measure to protect your mobile devices. Measure you may adopt are as below:-

■ 設定行動裝置時：
When setting up mobile devices:-
如沒有必要使用基於位置為本的應用程式，應關掉行動裝置內的定位服務設定。
不應破解行動裝置以解除其使用或存取限制。
Android 使用者請提防 Certifi-Gate 及 Stagefright 漏洞。
If it is not necessary to use location-based apps, please turn off the location service setting in your mobile devices.
The mobile devices should not be hacked to remove its use or access restrictions.
For Android users, please prevent the loopholes of Certifi-Gate and Stagefright.

■ 使用行動裝置時：
When using mobile devices:-
應盡可能使用嚴謹的認證方式，例如雙重認證，保護用於處理敏感資料的網上帳戶。想了解更多有關帳戶保安的提示，你可以瀏覽處理帳戶及密碼指引。
Please use rigorous authentication methods as much as possible, such as two-factor authentication, to protect online accounts used to process sensitive data. For more tips on account security, you can browse the guidelines for handling accounts and Personal Identification Numbers.

應小心看守你的行動裝置，一時疏忽都有被竊的可能。

Please aware your mobile devices, any neglect may lead to be stolen.

不應在行動裝置上處理敏感資料，除非使用具有加密功能的或安全的端到端連接。

Sensitive data should not be processed on mobile devices unless an encrypted or secure end-to-end connection is used.

不應下載或接受不明或不可靠的程式或內容。

You should not download or accept unknown or unreliable programs or content.

連接公共的 Wi－Fi 熱點時要謹慎。應避免存取敏感資料，除非採取了足夠的保安措施。

Please be cautious when connecting to public Wi-Fi hotspots. Avoid access to sensitive information unless adequate security measures are taken.

■ 備份行動裝置內的資料時：

When backing up data in mobile devices:-

將資料同步至雲端服務前應評估保安風險，並採取適當的保安措施，例如避免將敏感資料自動備份或同步至雲端平台上。

應在許可的情況下，開啟備份/同步軟件之加密選項。

應確保儲存在桌面電腦或抽取式媒體上的備份都經過加密。

Before synchronizing data to cloud services, you should assess the security risks and take appropriate security measures, such as avoiding automatic backup or synchronization of sensitive data to the cloud platform.

Enable the encryption option of the backup/synchronization software can only be done under permission.

Make sure that all backups stored on a desktop computer or removable media are encrypted.

■ 棄置行動裝置時：

When disposing of the mobile devices:-

應確保行動裝置內的數據和設定在棄置前已被完全地刪除。

Make sure that the data and settings in the mobile devices have been completely deleted before disposal.

■ 任何時候：

In anytime,

應把行動裝置放置在安全的地方，尤其是在不使用時。

應時刻留意與行動裝置有關的保安漏洞，並安裝最新的修補程式。

不應在行動裝置上安裝非法或未經授權的軟件。

不應接受不明或不可靠的無線連接要求。
the mobile device should be placed in a safe place, especially when not in use.
Always pay attention to security vulnerabilities related to mobile devices and install the latest patches.
Illegal or unauthorized software should not be installed on mobile devices.

■ 用流動應用程式的注意事項：
Notes on using mobile apps:-
只安裝來自官方或可靠來源的流動應用程式。
應安裝流動保安程式(如防禦惡意軟件)，以保護裝置和資料的安全。
應閱讀其他用户的評語，了解應用程式的使用條款及私隱政策等等。
在安裝或使用流動應用程式時，應徹底審視應用程式的所有權限要求，特別是一些涉及特權的存取。
在許可的情況下，應啟用由流動應用程式所提供保安功能(如密碼保護，安全連接等)。
經常更新系統及流動應用程式至最新版本。
不要下載來歷不明的文件，或打開或點擊可疑或不可靠的連結。
在使用即時通訊應用程式(例如 Whatsapp、LINE、WeChat 等)時，如收到任何詐騙消息後，不應再次轉寄，以免此類詐騙消息進一步散播。　　定期檢查已安裝的流動應用程式，並移除一些不再需要的應用程式。
不可移除裝置上設定的使用和存取限制(例如 jailbreak)。
關掉行動裝置內的無線服務例如 Wi-Fi、藍芽(Bluetooth)、近場通訊(NFC)等的自動連線功能。
Only install mobile apps from official or reliable sources.
A mobile security program (such as anti-malware) should be installed to protect the security of the device and data.
You should read other users’ comments, understand the app’s terms of use and privacy policy, etc.
When installing or using a mobile app, you should thoroughly review all the permission requirements of the app, especially those that involve privileged access.
If permitted, the security features provided by the mobile application (such as password protection, secure connection, etc.) should be enabled.
Frequently update the system and mobile applications to the latest version.
Do not download files from unknown sources, or open or click on suspicious or unreliable links.
When using instant messaging applications (such as Whatsapp, LINE, WeChat, etc.), if you receive any fraudulent messages, you should not forward them again to avoid further dissemination of such fraudulent messages. Check the installed mobile apps

regularly and remove some apps that are no longer needed.
The usage and access restrictions set on the device cannot be removed (e.g. jailbreak).
Turn off the automatic connection function of wireless services such as Wi-Fi, Bluetooth, and Near Field Communication (NFC) in the mobile device.

其他安全注意事項
Other safety precautions:-

■ 本行不會以電子郵件或電話要求客戶提供私人帳號或密碼，亦不會發送嵌入超連結(包括以 QR 碼形式顯示)、交易網站或網路銀行行動 APP 的電子郵件給您。此外，請勿以電子郵件內的超連結網址進入本行網站。若發現可疑的電子郵件，請立即向本行查詢，切勿逕行連結來路不明之網站及鍵入帳號與密碼，或是透過網際網路搜尋引擎或可疑彈出視窗上顯示的超連結存取銀行網站。
The Bank will not ask customers to provide their personal account numbers or passwords via email or phone calls, nor will it send you emails with embedded hyperlinks (including display in the form of QR codes), transaction websites or online banking mobile apps. In addition, please do not use the hyperlink URL in the email to enter our website. If you find a suspicious email, please check with the bank immediately. Do not directly link to an unknown website, type in your account number and password, or access the bank's website through an Internet search engine or a hyperlink displayed on a suspicious pop-up window.

■ 建議您應嚴格限制任何未經授權的人使用您的電腦，且應避免在使用網路銀行服務中途離開電腦。使用完畢應立即登出網路銀行服務系統。
It is recommended that you strictly restrict any unauthorized person from using your computer, and avoid leaving your computer in the middle of using online banking services. You should log out of the online banking service system immediately after using it.

■ 應時常檢查帳戶餘額及對帳單，或系統操作記錄，以發現是否有異常交易。如發現任何錯漏、未經授權的交易、可疑的登入紀錄、異常的網銀畫面或彈出畫面等情況，請立即通知本行。
Check account balances and statements, or system operation records from time to time, to find out if there are any abnormal transactions. If you find any errors or omissions, unauthorized transactions, suspicious login records, abnormal online banking screens or pop-up screens, please notify the Bank immediately.

如有任何懷疑，請立即通知下列機構
If you have any doubts, please notify the following organizations immediately.

■ 台新銀行新加坡分行　電話：65-6224-0888
Taishin International Bank, Singapore branch　Tel: 65-6224-0888

■ 新加坡金融管理局　電話：65-6225-5577
Monetary Authority of Singapore　Tel: 65-6225-5577

■ 新加坡警方　999
Singapore Police　Tel: 999

欲了解常見的網路銀行詐騙案例或客戶使用網路銀行之相關權益，可連結至以下機構查詢，以確保自身權益。
To learn about common online banking fraud cases or the related rights and interests of customers using online banking, you can link to the following institutions to inquire to ensure your rights and interests.

■ 新加坡金融管理局（ https://www.mas.gov.sg/ ）
Monetary Authority of Singapore（ https://www.mas.gov.sg/ ）