恒生銀行
HANG SENG BANK

# Online Banking Security

To provide you with better online protection, we are constantly reviewing our efforts and upgrading our systems. However, security is a joint effort, so please view the sections below for handy hints on what measures you can take.

## When you Logon to Business e-Banking

Always access our Business e-Banking by keying in the website address (www.hangseng.com) at the address bar of the browser. Never gain access via hyperlinks embedded in emails, unknown sources such as pop-up windows or search results from internet search engines.

Avoid opening additional internet browsers sessions when your internet banking session is open.

If you encounter slow response or unusual screen pop-up, log out from Business e-Banking immediately and scan your computer with the most updated anti-virus software.

Always check the last logon date and time after logging in your Business e-Banking.

Avoid conducting banking transactions or check account balances from a public terminal.

Always log off properly and close the browser after you have finished using e-Banking Services. Never leave your e-Banking session unattended while using Hang Seng e-Banking Services.

If any unauthorized logon activity, suspicious logon behavior or website is found, please contact the Bank immediately at (852) 2198 8000.

## Install Firewall and Anti-Virus Protection

Ensure your computer or mobile device has updated firewall and anti-virus software installed. The software should be updated regularly to protect you against new hacking attempts. Make sure the software is the latest version, otherwise you may encounter system error when using our online banking services.

Never open email attachments or URLs unless you know they are from a safe and reputable source.

To protect your computer against viruses and online threats, an end-point security solution – Webroot SecureAnywhere will be available for free download after logon.

恒生銀行
HANG SENG BANK

## Safeguard Your Passwords

Change your password on a regular basis, at least every 60 days.

Keep your password confidential. Do not write down or reveal your password to anyone. Our Bank staff will never ask for your password.

Avoid using your birthday, name. ID card number, telephone number or other similar numbers as your password.

## Making Online Payment

Always notify the Bank to update the contact information if there is any change in mobile phone number. Please ensure you will be able to receive the notifications that is sent to your mobile device via your selected delivery channel.

Review the payment details sent to your mobile devices(including SMS and WeChat) and contact our Bank immediately for any suspicion.

Review transaction records or statements regularly. Report to the bank if suspicious transaction is found.

Set up dual authorisation control will provide extra protection for your online transactions.

If you suspect any security breach or unusual account activities, please contact our Customer Service Representatives on (852) 2198 8000 (24 hours) as soon as reasonably practicable and change your password as soon as possible.

Warning: you may be held liable for all losses if you have acted fraudulently or with gross negligence, or failed to follow the safeguards set out above.

We maintain strict security standards and procedures to prevent unauthorized access to information about you. Outside of the normal Internet Banking log-in process, **Hang Seng Bank will never contact you and ask that you validate personal information such as customer ID, password, or account numbers**. If you receive such a request, please notify us immediately at (852) 2198 8000.

恒生銀行
HANG SENG BANK

# 網上銀行保安提示

為使客戶於使用網上銀行服務時得到更佳保障，我們不斷致力檢討各項保安措施並安排系統升級。然而，單靠我們的努力並不足夠，您作為網絡使用者亦有責任保障自己的戶口安全。請查看下列各項，取閱您可以採取的各項保障網上活動的措施。

## 登入商業e-Banking

為確保您能進入真正的恒生商業 e-Banking 網址，請您於瀏覽視窗網址位置鍵入網址 www.hangseng.com。切勿透過電郵內的超連結或來歷不明的途徑（例如：彈出視窗或互聯網搜尋結果）登入商業 e-Banking。

於使用 e-Banking 服務時，切勿同時開啟其他瀏覽器及瀏覽其他網站。

如果有不尋常的視窗彈出或電腦操作異常緩慢，您應該徹底登出恒生商業 e-Banking 賬戶，並利用最新電腦病毒定義檔的電腦防毒軟件為電腦進行電腦病毒掃描。

於登入恒生商業 e-Banking 後，請留意上一次登入日期及時間有沒有異樣。

不應使用在公眾地方提供的上網服務進入恒生 e-Banking 服務進行交易或查詢戶口結餘。

請緊記當您完成所有 e-Banking 服務後，必須登出賬戶以及關閉瀏覽器。於使用 e-Banking 服務時，切勿讓網頁長時間閒置。

如發現任何不尋常的登入情況或可疑網頁，請盡快致電(852)2198 8000 通知本行。

## 設置防火牆及安裝防毒軟件

應為電腦或區域網絡安裝防火牆和防毒軟件，並替您的瀏覽器下載最新的安全套件更新及增修版程式。這些程式可堵塞一些已發現的保安漏洞，確保您獲得最新保安技術的保障。確保軟件已更新至最新版本，否則有可能導致網上銀行系統錯誤。

切勿打開任何帶有附件的不名來歷電郵，以保障電腦免受病毒侵襲。

為致力保障您的電腦的防禦措施 ，您可於登入恒生商業 e-Banking 後免費下載 Webroot SecureAnywhere 防毒軟件增強電腦設備保安。

小心保管您的密碼

每隔一段時間透過恒生 e-Banking 服務更改密碼，例如最少每 60 天更改一次。

不要向任何人士披露密碼。不要寫下或記錄密碼而不加掩藏。(恒生銀行的任何人員，都不會要求您說出密碼。)

不要以您的出生日期、姓名、香港身份證號碼、電話號碼或類似數字作為密碼。

網上轉賬或付款時

如流動電話號碼有所更改，客戶須儘快通知本行以作出更新。請確定您的流動裝置能透過你所選擇的發送渠道收取訊息。

留意有關網上理財轉賬的手機提示 (包括短訊及微訊)，並核對轉賬資料。如有任何懷疑，請即通知本行。

經常查閱交易/轉賬紀錄，如發現任何不尋常的交易，請盡快通知本行。

設定雙重授權可為您的網上交易提供額外保障。

如果閣下對網上保安或戶口活動有懷疑，請在合理切實及可行範圍內盡快致電(852) 2198 8000(24小時)與本行客戶服務員聯絡及應盡快更改密碼。

注意：倘若閣下作出欺詐行為或因為嚴重疏忽或未能遵守上述之保障措施而招致任何損失，閣下將要承擔所有損失。

本行一貫採取嚴格的保安標準及程序，以防止未獲授權人士取得有關閣下的資料。恒生銀行絕對不會在正常的網上銀行登入程序以外，接觸閣下及要求閣下確認個人資料，例如客戶名稱、密碼或戶口號碼。倘閣下接獲此等要求，請立即致電(852) 2198 8000通知本行。