兆豐國際商業銀行香港分行
MEGA INTERNATIONAL COMMERCIAL BANK
Hong Kong Branch

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

兆豐商銀香港分行的慎防詐騙忠告
Fraud prevention advices recommended by Mega Bank Hong Kong Branch

您只需實行以下數項簡單的預防措施，便可保障您免受詐騙，妥善保管您的財富。您應該經常辦理：
To protect you and your wealth from fraud, please pay attention to these few simple precautions. Here are what you should always do:

一、更新您在兆豐商銀香港分行的客戶聯絡資料
1. Update your customer contact information with Mega Bank Hong Kong Branch

請向兆豐商銀香港分行提供您最新的聯絡地址、聯絡電話號碼（含手機號碼）、傳真號碼及／或電郵地址，以便本分行可以核實任何可疑交易。基於保全理由，您必須填寫《客戶資料修改表格》（及／或由兆豐商銀香港分行不時公告之適用申請文件），並透過郵寄或親臨香港分行遞交更改申請。
Please update your latest correspondence address, contact phone number (mobile phone number inclusive), facsimile number and/or e-mail address with Mega Bank Hong Kong Branch to allow verification in the event of suspicious transactions. For security reason, you are required to update your information by submitting the original copy of Customer Information Amendment Form (and/or any applicable application document(s) announced by Mega Bank Hong Kong Branch from time to time) to us by post or visiting Hong Kong Branch in person.

請注意：兆豐商銀香港分行職員於任何情況下均不會要求您提供全球金融網用戶登入帳號及密碼，以及其他銀行帳戶密碼。
Please pay attention: Staff of Mega Bank Hong Kong Branch will never ask for your Global Electronic Banking user ID or password, or any password of other bank account under any circumstances.

二、定期更改全球金融網用戶登入密碼
2. Change your Global Electronic Banking password regularly

請謹記定時更改並小心保管您的全球金融網用戶登入密碼。您應該使用難以被猜測的密碼，並切勿以書寫方式記下密碼。
Remember to change your Global Electronic Banking password regularly and keep your password secure. Make your password hard to guess and never write it down.

三、開啟並定期更新您的裝置上已載入之網絡安全及防毒軟件程式
3. Enable and periodically update the installed internet security and anti-virus programs on your device

請啟動在您的電子裝置上已載入之網絡安全及防毒軟件程式。強烈建議您一併啟動軟件自動更新功能，以確保您的裝置已擁有最新版本的保全資料庫，以便有效防範木馬程式、釣魚程式、網絡竊聽等保全漏洞及駭客入侵。
Please enable your internet security and anti-virus programs installed in your electronic devices. It is highly recommended to enable the software's auto-update function as well to ensure the latest-version security database has been downloaded into your device, so that to effectively prevent hacker's invasion and certain security loopholes like Trojan horse, phishing and eavesdropping, etc.

兆豐國際商業銀行香港分行
MEGA INTERNATIONAL COMMERCIAL BANK
Hong Kong Branch

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

四、以其他方式核實通知您更改收款人資料的要求

4. Verify a request to change payee information for remittance by contacting the requester via a different channel

請於轉帳及／或匯款前，以電郵以外的方式，例如透過電話，向聲稱是您的商業伙伴的一方，核實對方真正身分，以防範電郵騙案。請留意以下香港警局及香港金融管理局之呼籲：

Confirm the identity of the purported business partners by means of telephone or other-than-email channel before making transfer payment and/or remittance to prevent fraud from e-mail scams. Pay attention to the appeals of Hong Kong Police and Hong Kong Monetary Authority at below sections correspondingly:

甲、香港警察呼籲：慎防電郵騙案 － 「核實電郵者身分 揭穿騙徒真面目」

A. Hong Kong Police Force Appeal: Beware of E-mail Scam – "Verify Suspicious E-mails to Uncover Online Swindlers"

「於電郵騙案中，騙徒大多會利用駭客技術入侵受害人的電郵戶口，並查看受害人與商業伙伴的電郵，再以相同或類似的電郵戶口向受害人發出電郵，聲稱付款銀行戶口已更改，並要求受害人將指定金額匯入騙徒指定的銀行戶口。警方呼籲，若您收到可疑電郵，應在付款／匯款前以電話確認對方的真正身分或該項要求的真確性，以防受騙。」

"E-mail scams have been reported where fraudsters hacked into the victim's e-mail account and extracted their business correspondence with business partners. The fraudster then sent an e-mail to the victim using the same or similar e-mail account as the victim's business partner claiming that the payment bank account had been changed in a bid to persuade the victim to deposit payment for goods into the fraudster's designated bank account. Police appeal that if you receive any suspicious e-mails, you should confirm the identity of the purported business partners or the authenticity of the requests by means of a telephone call before payment / remittance so as to avoid being deceived."

乙、香港金融管理局呼籲

B. Hong Kong Monetary Authority Appeal

「市民切勿經電郵內的超連結、網上搜尋器或可疑的突現式視窗登入網上銀行戶口，而應在瀏覽器上輸入網址或將真正的網址記錄在電腦的書簽內，藉此接駁至網上銀行戶口。此外，銀行並不會透過電子郵件要求客戶提供其戶口資料（例如網上理財登入密碼）或於網上核實其戶口資料。市民如有任何疑問，應與銀行聯絡。」

"Members of the public are reminded not to access their Internet banking accounts through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, they should access their Internet banking accounts by typing the website addresses at the address bar of the browser, or by bookmarking the genuine website and using that for access. In addition, banks are not expected to send e-mails asking their customers to provide their account information (e.g. Internet banking logon passwords) or verify their account information online. If in doubt, they should contact their banks."

兆豐國際商業銀行香港分行
MEGA INTERNATIONAL COMMERCIAL BANK
Hong Kong Branch

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

兆豐商銀香港分行給您的貼心提示
Useful tips provided by Mega Bank Hong Kong Branch

甲、使用線上銀行 －「全球金融網」
A. Accessing Online Banking – "Global Electronic Banking"

1. 兆豐商銀香港分行職員不會要求您提供全球金融網用戶登入帳號及密碼。
   Staff of Mega Bank Hong Kong Branch will never ask for your Global Electronic Banking user ID and password.
2. 您可於瀏覽器上直接輸入兆豐國際商業銀行官方網址 －「https://www.megabank.com.tw」， 以登入全球金融網服務；或把網址儲存於瀏覽器內。不要透過可疑電子郵件上的超連結或從互聯網搜索器所取得的網址登入兆豐國際商業銀行全球金融網系統。
   Safely log on to Global Electronic Banking by entering the official homepage of Mega International Commercial Bank – "https://www.megabank.com.tw" into your browser, or bookmark the authentic website address for future use. Do not use a website address or links attached in any suspicious e-mail or found through Internet search engines to log on to Mega Bank's Global Electronic Banking system.
3. 確保在不被監察的情況下輸入全球金融網密碼、任何銀行服務密碼（含個人識別碼）、登入密碼、認證碼或其他任何重要資料。
   Ensure that no one is watching you while you key in your Global Electronic Banking password, any bank services password (Personal Identification Number (PIN) inclusive), log-on password, verification password, or any other sensitive information.
4. 請勿指派多人使用同一組全球金融網帳號或密碼。
   Do not delegate multi-users to use the same set of Global Electronic Banking account or password.
5. 每次使用全球金融網後緊記登出。在登出全球金融網時，不要只關閉瀏覽器，應按照指示登出，以確保獲得妥善保障。
   Always log off your Global Electronic Banking online session. Do not just close your browser. Follow the logoff instructions to ensure your protection.
6. 小心留意「看似雷同」的虛假網頁，這些網頁專門騙取客戶的個人／秘密資料。若您懷疑網頁的真確性，應立即關閉，切勿按照網頁的任何指示行事。
   Be aware of phony "look alike" websites which are designed to trick customers and collect their personal / secret information. If you suspect a website is not what it purports to be, leave the site immediately. Do not follow any of the instructions it may present to you.
7. 切勿透過不可靠的共用電腦或電子裝置使用全球金融網服務。
   Do not use a shared computer or electronic device that cannot be trusted for accessing Global Electronic Banking services.
8. 確保個人電腦和電子裝置已裝有最新的防毒軟件，並經常更新病毒定義檔案，以預防新型電腦病毒。如得悉最新病毒定義檔案推出，請盡快下載。
   Make sure your personal computer and electronic device have the most current anti-virus software. Anti-virus software needs frequent updates to guard against new viruses. Make sure you download anti-virus updates as soon as you are notified that a download is available.
9. 建立個人／企業網絡防火牆，防止未獲授權人士進入您的電腦系統，特別是當您透過任何寬頻網絡、無線網絡、數碼用戶線路數據機或網絡路由器連線上網。
   Install a personal / corporate network firewall to help prevent unauthorized access to your computer system, especially if you connect through a broadband connection, Wi-Fi, network router, cable or DSL modem.
10. 在每次上網後，特別是在使用共用電腦時，清除瀏覽器內超高速緩衝存儲器的資料及過往資料紀錄，以確保移除您的帳戶資料。

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

Clear your browser's cache and history after each session to ensure your account information is removed, especially if you are using a shared computer.

11. 使用最新建議的瀏覽器版本，或可支援 128-bit 加密的瀏覽器。切勿啟動瀏覽器內之「自動完成」功能，以免任何帳戶號碼及私人密碼自動儲存在電腦內。
    Use the latest recommended Internet browser version, or one that supports 128-bit encryption. De-activate the "Auto Complete" function to prevent any log-on identity name, password, verification code and PIN from being stored.
12. 請確保您的操作系統及瀏覽器使用最新的修正程式。
    Always ensure your operating system and browser has the latest security patches applied.
13. 請確保上網時並無啟動作業系統內的檔案分享功能，特別是當您透過任何寬頻網絡、數碼用戶線路數據機或（無線）網絡路由器等連線上網。
    Ensure the file sharing feature is disabled in your operating system while online, particularly if you are linked to the Internet through a cable, DSL modem, or (Wi-Fi) network router, etc.
14. 注意無線網絡保全：
    Be cautious about your wireless connections security:
    - 為您的無線網絡設立個人密碼。
      Set a personal and unique password for your wireless network.
    - 不要顯示您的網絡名稱（服務設置標識符）。
      Disable broadcasting your network name (SSID-Service Set Identifier).
    - 使用加密技術保障您的無線網絡。
      Use encryption to protect your wireless network.
    - 無線上網時，使用已註冊的電腦以連接至您的無線網絡。
      Use only registered machines for your wireless network.
15. 切勿透過不知名的途徑安裝軟件或執行程式。
    Do not install software or run programs from an unknown origin.
16. 定期檢查帳戶，如有任何困難或發現任何不尋常的情況，請立即與香港分行經辦職員聯絡。
    Check your accounts on a regular basis and contact the corresponding handling staff of Hong Kong Branch immediately should you encounter any difficulties or irregularities.
17. 小心留意可疑的彈出式電腦視窗或其他來歷不明的登入網站渠道。如要瀏覽兆豐商銀官方網站，您應在瀏覽器的網址列輸入正確的網址，或為正確的網址添加書籤，以便日後登入。
    Beware suspicious pop-up windows or any other doubtful channels. You should always connect to the Mega Bank's official website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access.

乙、處理電郵

B. Handling E-mail

1. 兆豐商銀香港分行不會以電郵要求您披露帳戶密碼、全球金融網密碼、任何提款卡／借記卡／信用卡私人密碼及帳戶餘額等敏感資料。
   Mega Bank Hong Kong Branch will never send you an e-mail asking for your sensitive information including account password, Global Electronic Banking password, any PIN of ATM card / debit card / credit card or account balance, etc.
2. 小心留意欺詐性郵件。這類郵件可能會由看似可信賴的公司或朋友名義寄發，但實際上會誘騙您下載病毒程式或登入虛假網頁以套取重要資料。
   Be alert for fraudulent e-mails. These may appear to come from a trusted business or friend, but actually are designed to mislead you into accessing a fraudulent website and disclosing sensitive

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

information.

3. 小心提防任何載有連結或要求您輸入個人資料的電郵，切勿回覆該電郵、按下電郵內的連結或輸入任何敏感資料。
   Be suspicious of, and pay high attention to, any e-mail that contains an embedded hyperlink or a request to enter personal information. Do not reply, click on the hyperlinks or input any sensitive information.
4. 若您收到懷疑是假冒從兆豐商銀香港分行寄發的郵件，請立即通知本分行經辦職員，並建議依本分行職員指示處理該郵件。
   If you've received suspicious e-mails purporting to be from Mega Bank Hong Kong Branch, please notify the corresponding handling staff of Hong Kong Branch right away. It is highly recommended to follow the Branch staff's instruction to treat the suspicious e-mail.
5. 切勿開啟或預覽不明及可疑來源的電郵附件，它們可能含有病毒。
   E-mail attachments from unspecified or suspicious sources may be a virus or worm. Do not open or preview any attachment unless you are sure it is safe.
6. 切勿隨便在網絡上傳送任何重要的個人／機構或財務資料，除非是已加密的安全網頁。一般的電子郵件並無加密功能，傳送這類電郵有如寄發明信片，容易洩露資料。
   Do not send sensitive personal / organization or financial information unless it is encrypted on a secure website. Regular e-mails are not well encrypted and may leak the information easily as if it was a postcard under delivery.
7. 若您已在可疑的網站披露您的敏感資料，請即向您所在當地的警局匯報。若此網站假冒為兆豐商銀香港分行官方網站，亦請立即通知本分行。
   If you have provided sensitive information to a suspicious website, you should report to the police of the jurisdiction where you are at presence immediately. If the website is purporting to be a Mega Bank Hong Kong Branch official site, please also notify Hong Kong Branch right away.
8. 若您希望核證由兆豐商銀香港分行發出的任何電郵所附之超連結網址，或其他網頁的真確性，請查核有關超連結網址或其他網頁的保安證書，以檢視有關網頁的資料如公司名稱、網址、發行證書的機構、有效期限、加密類別等，以確定該網頁為您想瀏覽的網頁。
   If you use a link in an e-mail you have received from Mega Bank Hong Kong Branch, you may verify the authenticity of the website you are accessing by checking the website SSL certificate information, such as company name, URL, certificate issuer, validation date, and encryption types, etc, to confirm that it is the website you intend to access.
9. 若您希望核實由兆豐商銀香港分行發出的任何電郵，或確認電郵內容的真確性，請於香港分行辦公時間內致電求證真偽。
   If you intend to further acknowledge the genuineness of an e-mail or the contents thereof you have received from Mega Bank Hong Kong Branch, you may verify the authenticity by confirming with the Branch's staff by phone during Hong Kong Branch's office hours.

丙、利用行動通訊裝置

C. Using Mobile Device

1. 於流動裝置上安裝安全修保程式及最新的作業系統，不要經未確定來源下載流動裝置程式。
   Install security patches and the latest software updates in your mobile device. Do not download programs / apps from unsecured sources.
2. 確保在不被監察的情況下輸入用戶身分／登入帳號、密碼或其他任何重要資料。
   Ensure that no one is watching you while you key in your user identity / log-on name, password or any other sensitive information.
3. 每次登入後緊記登出，不要只關閉流動電話上的瀏覽器，應按照指示登出，以確保獲得妥善保障。
   Always log off your online session. Do not just close your mobile device browser. Follow the logoff

香港九龍尖沙咀廣東道 21 號海港城港威大廈
英國保誠保險大樓 22 樓 2201 室
Suite 2201, 22/F, Prudential Tower, The Gateway, Harbour City,
21 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Tel: (852) 25259687 Fax: (852) 25259014

instructions to ensure your protection.

4. 於您的行動裝置設定密碼或解鎖圖形，以防止於遺失行動裝置或行動裝置被盜時，被未獲授權人士取得並使用您的個人／機構／敏感資料。
   Set up a password or unlock sign pattern for your mobile device. This will help you prevent unauthorized use of your mobile device and access to your personal / organization / sensitive information in case it has been lost or stolen.
5. 定期清除行動裝置瀏覽器內超高速緩衝存儲器的資料及過往資料紀錄，以確保移除您的帳戶資料。
   Remove temporary files and the cache stored in the memory of your mobile device regularly since they may contain sensitive information such as your account number.
6. 刪除過期及機密的短訊信息，以及定期刪除瀏覽器瀏覽記錄。
   Delete outdated and sensitive SMS messages if they are no longer required and clear the browsing history regularly.
7. 切勿放下流動裝置不顧。
   Do not leave your mobile device unattended.
8. 避免把流動裝置借予他人，或與他人共用。
   Avoid sharing your mobile device with, or lending it to, the others.
9. 切勿把機密資料，例如密碼、個人識別碼或帳戶號碼等儲存於流動裝置內。
   Do not keep sensitive information such as your account number, PIN and password in your mobile device.