山證國際
SHANXI SECURITIES INTERNATIONAL

親愛的客戶：

擺脫網絡安全壞習慣

網絡犯罪愈來愈頻繁，應常常保持警惕，盡量避免以下一些網絡安全壞習慣。

1. 沒有定期更新
電腦及設備上的操作系統、瀏覽器和其他軟件中的漏洞是網絡犯罪可以進行攻擊的主要方式之一，停用自動更新功能會暴露設備於不安全環境。

2. 不安全的密碼
對多個帳戶使用相同的密碼和易於猜測的憑證，為黑客提供了極大的便利。

3. 使用公共 Wi-Fi
黑客可以利用相同的網絡了解您的互聯網使用情況、登錄您的帳戶並竊取您的身份。為了安全起見，請儘量避開這些公共熱點，若您使用時，也避免在連接時登錄任何重要帳戶。

4. 隨意點擊來路不明之連結
網絡釣魚是目前最大的網絡威脅之一，仔細核對發送電子郵件的個人或公司以確保其合法，不要隨意點擊不明的連結。

5. 未在所有設備上使用資訊安全產品
在網絡威脅多變的時代，應該確認所有的電腦設備及流動裝置都有安裝專業且具知名度的資訊安全產品。

6. 點擊不安全的網站
http:// 是網頁伺服器與您的電腦瀏覽器以一般（非安全）模式在進行互動交談，內容有可能遭攔截。而 https:// 多了一個字母 S 代表「 安全（secure）」，基本上意謂著，您的電腦與伺服器間的資料傳遞是以加密的方式進行互動交談。

7. 工作電子郵件用於個人日常
試想使用工作的電子郵件和密碼在購物網站和其他網站上註冊，您會習慣性收到大量促銷郵件，減低了對釣魚郵件的警覺性。另外，如果這些網站遭到破壞、攻擊，黑客就有可能劫持您的公司帳戶。

8. 通過電話提供詳細訊息
語音網絡釣魚（也稱為 vishing）是一種越來越流行的從受害者那裡獲取個人和財務資訊的方式，詐騙者經常偽裝他們的真實號碼以增加攻擊的合法性，所以請儘量避免透過電話發送任何敏感或重要訊息。

9. 沒有定期備份
勒索軟件每年給企業造成數億美元的損失，試想如果突然無法開啟您的電腦，當中所有的資料都可能永遠丟失，其中包括家庭照片和重要的工作文件等等。根據 3-2-1 最佳備份原則（至少備份三份、使用兩種不同形式、其中一份備份要存放異地），定期備份可在最壞的情況發生時，讓您高枕無憂。

山證國際
SHANXI SECURITIES INTERNATIONAL

我司會不時更新關於網絡安全的提示，請您關注我司以下網站：
http://www.ssif.com.hk/main_hk/customerCenter/cybersecurity/index.shtml

如有垂詢，請聯絡您的客戶經理或致電客戶服務熱綫 +852 2501 1001（香港及海外）或 +86 4008411618（中國內地）。

山證國際證券有限公司
山證國際期貨有限公司 謹啓
2022 年 5 月 4 日