申萬宏源香港 SHENWAN HONGYUAN

DOC/317/05-19

Shenwan Hongyuan Securities (H.K.) Limited 申萬宏源證券(香港)有限公司
Shenwan Hongyuan Futures (H.K.) Limited 申萬宏源期貨(香港)有限公司
(Collectively known as "Shenwan Hongyuan") (統稱「申萬宏源」)

Placing Order through Instant Messaging Applications Service
使用即時通訊應用程式以發出交易指示服務

Risk Disclosure Statement and General Advice to Customers
風險披露與致客戶的一般建議

Risks of using instant messaging ("IM") applications for order placing 使用即時通訊應用程式發出交易指示的風險

1. Network broken down 網絡中斷
Network can be broken down for either users or at both ends which may cause communication completely stopped.
網絡中斷可能在任何一方用家或同時在兩端發生而引致對話完全中斷。

2. IM service provider suffers from system breaking down 即時通訊服務供應商系統停止操作
The system of the IM service provider may break down and messages are delayed in delivery or disappear from the system.
即時通訊服務供應商系統停頓導致各方已發出訊息延誤或在系統內消失。

3. **The system of IM service provider malfunctions 即時通訊服務供應商系統不正常操作**
The system of the IM service provider may malfunction, causing communication break downs, message delivery delayed, message wrongly delivered or sent messages disappear within the system.
即時通訊服務供應商系統不正常操作或會令對話中斷、訊息延誤、訊息誤傳或已發訊息在系統內消失。

4. **Phishing scams 網絡釣魚詐騙**
Messages containing phishing content or link might be sent to you seemingly from someone you know or a trustful enterprise to trick careless recipients overlooking the authenticity of the contents and fall into phishing scams or fraud.
騙徒可能會偽裝成閣下認識的人或可靠的企業，透過即時通訊把帶有釣魚訊息或連結動的訊息傳送給閣下，誤導大意的收件人因不注意內容真偽而墮入釣魚陷阱或訊息詐騙圈套內。

5. Computer virus spreading 散播電腦病毒
Computer virus is the program (malware) designed to carry out destructive activities to victims. Often malware is hidden in the messages with malicious attachments. If you open the message or attachment, the application or the system might be compromised.
電腦病毒是那些設計出來對受害者執行有害活動的惡意程式，通常會隱藏於帶有惡意附件的訊息內，若閣下打開訊息或附件，程式或系統便可能受到損害。

6. **Public network risk 公共網絡風險**
Mobile IM access and communication via the public network might lead to message contents intercepted and eavesdropped and thus sensitive information leaking.
在公眾網絡下使用流動即時通訊交談，可能引致訊息內容被攔截及竊聽，因而把敏感資料外洩。

7. **Account theft 賬號遭盜用**
Popular mobile IM applications often allow you to use your IM account on the computer by accessing the web based version for the sake of convenience. However, if your account is not managed properly or your password is successfully cracked by attackers, it might be misappropriated.
受歡迎的流動即時通訊程式一般為提供方便會允許閣下在電腦上透過網頁版本的登入而使用同一即時通訊賬號；可是，如果閣下未能妥善管理賬號或閣下的密碼被攻擊者成功破解，閣下的即時通訊賬號或會遭盜用。

8. Application bug 軟件漏洞
If you do not apply the bug fix patch by updating the mobile IM application regularly, malicious users might be able to conduct attacks through the software vulnerabilities. It might cause the application or system crash, or leakage of sensitive data and account information.
如果閣下沒有持續更新應用程式去修補程式漏洞，惡意使用者便可透過程式漏洞進行攻擊，導致程式或系統受到破壞，敏感資料及賬號也有機會因此而遭盜取。

The above list of risk of using IM services is by no means an exhausted list and can only indicate various risks that may associate with such services.
以上列單並非使用即時通訊服務的風險的完備清單，只是表明可能與此服務相關連的各種不同風險。

General Advice for using IM Applications 使用即時通訊程式的提示：

Do's 要做的事

1. Enable firewall protection 使用防火牆保護

Personal firewall should always be enabled.
個人防火牆裝置必須經常開啟。

2. Anti-virus app installation and update 裝置抗病毒程式並保持更新

Install anti-virus app to protect your device from virus and ensure the anti-virus app is update.
安裝防毒程式以保護閣下的裝置並確保防毒程式得到持續更新。

3. Know the security features of mobile IM applications 了解流動即時通訊程式的保安功能

Various security enhancements, such as message encryption, message self-destruct, two-factor authentication login, privacy settings feature in different mobile IM services. You are advised to understand such security features and apply them wisely to protect yourself.
不同流動即時通訊服務都會提供各款保安功能，例如訊息加密、自我刪除訊息、雙重認證登入、私隱設定等。建議閣下清楚了解相關保安功能，並明智地應用它們來保障閣下。

4. Encrypt your messages 加密你的訊息

Always enable message encryption of your IM software.
開啟即時通訊程式軟件上的訊息加密功能。

5. Conduct regular checkup on the security or privacy settings 定期檢查保安和私隱設定

Regularly review the security and privacy settings of your IM applications.
定期檢查即時通訊程式服務的保安及私隱設定。

6. Disable automatic friend search or invitation acceptance function 關閉自動朋友搜尋及應邀加入功能

When you disable automatic friend search or invitation acceptance function, naturally you reduce the chance for scammers to conduct phishing scams and fraudulent messages on you and hence minimise the risk of information leakage and falling into the trap.
當閣下關閉自動朋友搜尋及應邀加入功能後，自然降低成為網絡騙徒向閣下施以釣魚陷阱及訊息詐騙的機會，以減低資料外洩及誤墮陷阱的風險。

7. Disable sharing of resources function 關掉資源分享功能

Only enable resource sharing function when you need to and remember to disable it after process completion.
只在需要時才開啟資源分享功能，當閣下使用完畢切記把功能關掉。

8. Disable remote control of microphones and video cameras 關掉遠端控制和使用麥克風和攝錄機功能

When you use IM applications, disable remote activation and control of microphones and video cameras if they are not needed.
使用即時通訊服務時，如果不使用遠端控制和使用麥克風和攝錄機功能，應把功能關掉。

9. Verify the recipient list 核實收件人名單

Always verify the recipient list carefully before sending out messages.
在發出訊息前，須小心核實收件人名單。

10. Scan any files before opening them 開啟任何檔案前先掃描這些檔案

Scan any files receiving from IM with updated anti-virus app before opening these files.
要開啟從即時通訊傳送過來的檔案，先使用已更新的防毒程式掃描以確定檔案不含病毒方可開啟這些檔案。

11. Update all apps with latest patches 使用修補程式更新所有程式

Make a habit to update all apps especially the IM apps in your devices and other system components with their latest patches.
養成習慣定期下載最新修補程式去更新手機內所有程式，尤其是即時通訊程式和其它的系統程式組件。

12. Enable all notification alerts 啟動所有通知訊息提示

Enable all notification alerts when receiving incoming calls, messages and files to ensure you are kept informed if there are any secret background executions
在接收通話、訊息和檔案時，閣下應啟動全部通知訊息提示，以便閣下可察覺是否有其它工作秘密地在背景執行。

13. Download apps only from the official channels 只在官方渠道下載程式

Download apps only from official app markets endorsed by OS or device vendors.
只在系統或裝置供應商認許的官方程式網站內下載程式。

14. Refuse granting excessive information access rights to apps 拒絕批准程式過度存取資料權限的要求

Restrict the requests from any downloaded apps for accessing your data only on need to process basis and refuse their excessive access right requests.
限制任何已下載的應用程式訪問閣下資料的請求(僅限於實際處理所需)，並且拒絕所有過度的存取權限請求。

15. Activate device screen lock 啟動屏幕鎖

Preventing the unauthorised use of IM by keeping the device screen lock activated.
保持屏幕鎖啟動以防止未授權使用閣下的即時通訊。

16. Log in the IM service (web version) without having your password stored in the computer. 登入網上版即時通訊服務時勿使用記住賬戶密碼功能

Always opt out from the setting of "Remember my password" when you log in the IM service (web version).
當登入即時通訊服務(網上版) 時，永遠拒絕網頁上的"記住帳戶密碼"功能。

17. Log out the IM service (web version) properly 正確登出網上版即時通訊程式

It is a must to log out properly after using the IM service (web version) to prevent unauthorised use of IM.
必須正確登出即時通訊程式(網上版) 以防止未授權使用閣下的即時通訊。

Don'ts 不要做的事

1. Never send personal or sensitive data 永不發送私密或敏感資料

Millions of possibilities of leaking data such as data being intercepted during transmission by the unauthorised third party or the transmission not being encrypted, so stop sending personal or sensitive data via IM.
數不清的原因可導致資料外洩，例如資料傳送中途被未經授權第三方攔截或傳送過程未加密資料，因此不應使用即時通訊發送私密或敏感資料。

2. Ignore whatever requests coming from strangers 漠視陌生發件人各類請求

Never respond to the messages sent by strangers; simply ignore their request coolly especially anything related to password or authentication codes until you can get in touch with staff of the relevant organisation via official channel.
從不回應任何來自陌生發件人的訊息；除非閣下透過官方聯系方式接觸到有關機構職員，否則冷待那些與密碼或確認相關的要求。

3. Be aware of messages containing unknown links or attachments 小心來歷不明訊息內的連結或附件

Don't click open the link nor the attachment contained in the message casually. There might be malwares waiting to infect careless IM users falling into traps.
切勿隨便點擊打開即時通訊傳遞過來的來歷不明訊息內的連結或附件。惡意軟件永遠在等待大意的即時通訊用家墮入圈套。

4. Disable automatic acceptance of file transfers in IM services 關掉即時通訊上的檔案傳送自動接受功能

Never turn on the automatic acceptance of file transfers in IM services as it often places your device to extra high risk of receiving virus-infected files unknowingly.
切勿啟動即時通訊上的檔案傳送自動接受功能，不然閣下會不自覺地把閣下的裝置置於接收含病毒檔案的高危處境。

5. Don’t reveal unnecessarily extra personal information 毋需披露過多個人資料

When setting up your profile in your IM account, refrain yourself from revealing personal information unnecessarily.
當閣下制作即時通訊賬戶的個人簡介，避免披露太多個人資料。

6. Don't disclose contact lists used for batch submissions 不要透露用於同時發送給多位收件人的聯絡名單

Don’t disclose casually your contact lists via IM.
切勿隨便使用即時通訊透露同時發送給多位收件人的聯絡名單。

7. Don't use rooted devices 決不使用權限解鎖設備

Rooted devices may earn you super administrative privileges but also expose your device OS to an easier route for being attacked.
權限解鎖設備毋疑會提升閣下至超級管理權限，但同時也會讓閣下的設備操作系統更易遭入侵。