



善用保安措施，保障您的密碼

我們建議用戶採取以下措施：

- 不要將您的密碼告知任何人。iFAST 的職員在任何情況下都不會要求您提供密碼。
- 請勿以個人資料（例如電話號碼或出生日期）作為在 FSM 專用的密碼。
- 請勿採用連續的數字（如 123456）作為密碼，或在密碼中重複（兩次以上）使用同一數字（如 121145）。
- 不要在其他網路服務中使用相同的密碼，因為這可能帶來保安漏洞。
- 不要將您的密碼寫下來或蓄存在您的電腦，應把密碼緊記在心中。
- 定期更改您的密碼。如欲更改密碼，請點擊「認購/贖回」>「更新帳戶」。
- 每次登出後，請清理您的快取記憶和瀏覽記錄。
- 請緊記在使用後登出網頁。
- 若瀏覽器詢問您是否儲存登入名稱/密碼，請點擊「不」。
- 不要在公眾或他人的電腦上（例如朋友辦公室的電腦，或者網吧裏的電腦）輸入您的密碼。
- 安裝防毒軟件，並經常下載更新檔。
- 如果您使用無線上網，請確保資料傳輸過程是安全的。
- 定期登錄您的帳戶和查閱交易歷史，並檢查您的資產狀況。

安全顧問：網路釣魚詐騙

「網路釣魚」（Phishing）是一種常見的網路詐騙手法。騙徒冒充合法的企業，發送虛假郵件來騙取受害人的敏感個人資料，再利用這些資料來竊取用戶的財產或進行其他詐騙行為。

以下是騙徒常用的「網路釣魚」伎倆，但他們的手法層出不窮：

- 以偽造的電郵地址、公司標誌及圖片，讓您認為這些電郵及網站是來自 iFAST。
- 偽造仿似屬於我們的域名(domain names)。
- 通過虛假網站的超連結或在電郵中植入表格，誘使用戶洩漏個人資料。

我們提醒用戶：

- 主動聯絡我們時，才須提供個人資料讓我們核實身份。我們不會利用郵件或電話，主動要求客戶提供資料。
- 在任何情況下，iFAST 的職員都不會要求顧客說出帳戶密碼。
- 若要登入我們的網站，必須輸入我們的域名 www.ifastfinancial.com.hk。切勿通過其他網站或媒體的連結登入 iFAST。

- 登入後，請確保連接是以 SSL 加密。您可以檢查網址是否標示為 https://，或者在狀態列上是否顯示了一個上鎖圖案，來確認網頁已經加密。請經常在伺服器數碼證書上，檢查是否顯示為 iFAST。
- 請時刻警惕虛假網站和主題是來自 iFAST 的可疑電郵。如果您懷疑自己遇到「網路釣魚」，請立即聯絡我們。

安全顧問：間諜程式

間諜程式是一種電腦軟件，它可以在用戶不知道或不同意的情况下，收集用戶資料。這些程式監控用戶的互聯網瀏覽情況，從中竊取他們的隱私資料，並將這些資料發送給其他人。

間諜程式件通常會捆綁並隱藏於免費或共用軟件中，您可以輕易地從互聯網下載這些免費或共用軟件。有時候它們會聲稱可以加快連線速度或有其他好處。安裝某些間諜程式後，它們會改變用戶的網路連接方式，令用戶通過間諜程式的伺服器，間接連接到互聯網。

如果您的電腦出現以下情況，可能已遭間諜程式入侵：

- 經常跳出令人討厭的廣告。
- 在沒有事先通知的情況下，瀏覽器的設定被更改。
- 有一個第三者的工具欄出現在瀏覽器上，而且難於關閉。
- 當您瀏覽網頁時，瀏覽器經常出錯。
- 系統運算速度變慢，電腦反應時間較正常長。

我們建議用戶採取以下措施：

- 不要從不明網站下載及安裝任何軟件。
- 不要點擊那些以免費贈品吸引您的網上橫額或彈出式廣告。
- 安裝並定期更新您的反間諜軟件。經常掃描您的電腦，搜尋、隔離及刪除系統中的間諜程式。
- 安裝防毒軟件，並經常更新病毒定義檔案。
- 定期更新您的電腦作業系統和瀏覽器，確保系統是新版本。
- 定期更改您的投資帳戶密碼。

iFAST 極為重視網路安全。我們會阻止用戶經間接伺服器連接到 iFAST，作為防護措施之一。如果您被拒絕瀏覽我們的網站，您可能是在有意無意間使用了間接伺服器連接軟件或遭間諜程式入侵。在這種情況下，我們強烈建議您諮詢專業資訊科技顧問，或卸載有關軟件。

雙重認證(2FA)

什麼是 2FA 雙重認證？

2FA 指的是 Two Factor Authentication，即雙重認證

為什麼要進行 2FA 雙重認證才能登入奕豐平臺？

奕豐致力於不斷為網上客戶提供最高的安全性保障，遂啟用動雙重認證（2FA）功能，作為額外的身份驗證措施。

有了雙重認證功能，即使您的帳戶名稱及密碼被盜取，“侵入者”仍需經過雙重認證才能登入您的奕豐帳戶，讓通過網路釣魚或間諜軟體收集客戶資料的駭客較難侵入您的帳戶。