



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 **ifastgp.com.hk**。
- 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。奕豐投資平台服務（香港）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，奕豐投資平台服務（香港）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 **ifastgp.com.hk** 和 **ifastnetwork.com**。切勿通過其他網站或媒體的連結登入奕豐投資平台服務（香港）。
- 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，檢查是否顯示為奕豐投資平台服務（香港）。
- 請時刻警惕虛假網站和主題是來自奕豐投資平台服務（香港）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 **37664334**。