賬戶盜用

賬戶盜用

甚麼是賬戶盜用？

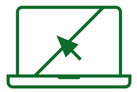
此類詐騙一般由於騙徒誘導您洩露個人資料，從而取得您的銀行賬戶存取權限。他們會重設密碼及安全驗證資料，使您無法登入賬戶，並可能更改賬戶所連結的電話號碼、地址及電郵地址，令其可如同合法客戶般操作賬戶。

遙距賬戶盜用

此類詐騙是指騙徒控制您的裝置某網站，並在您毫不知情或未經授權的情況下，從您的銀行賬戶進行付款。騙徒通常會先發送連結、要求您瀏覽或下載特定軟件，以取得您的裝置的遠端存取權限。透過閱讀本指南，您將了解騙徒常用的手法，並掌握防範措施，保護自己及業務免受侵害。

電話號碼詐騙

這是指騙徒透過更改來電顯示號碼，偽裝成您的銀行的官方電話號碼。該號碼可能與真實號碼完全相同，或僅相差一個數字。騙徒亦可能使用隱藏號碼來致電。



惡意程式與網絡釣魚

騙徒會利用惡意軟件及連結竊取個人資料。

這些資料可能被用作誘導您誤信某通電話屬真實來電，或用以入侵您的銀行賬戶。

授權代碼

請注意：包括銀行在內的任何機構，絕不會指示您如何使用實體或數碼保安裝置（即「保安編碼」），亦不會要求您提供網上理財授權代碼。

.

賬戶盜用

建議貼士

- ✓ 切勿透露您的網上理財使用者名稱、密碼、授權代碼或任何一次性密碼 (OTP)。
- ✓ 請記住，來電號碼有可能被偽造，切勿單憑來電顯示判斷對方身份。
- ✓ 如接獲不明來歷的電話，請掛線並改用經獨立渠道核實的電話號碼（例如對方官方網站所列的號碼）回撥查詢。建議使用另一部電話，或先聯絡熟悉的聯絡人，以確保通話線路安全無虞。
- ✓ 對可疑電郵及短訊務必提高警覺，尤其是含有連結或要求提供資料的訊息。所有要求提供資料的訊息，應直接向相關公司核實，並參照上述聯絡方式。
- ✓ 切勿因不明來歷的電話而點擊任何連結、瀏覽網站或下載軟件。
- ✓ 您的保安編碼裝置屬個人專用。如有人來電要求您使用該裝置，請立即終止通話並聯絡您的銀行。
- ✓ 恒生絕不會要求您參與任何正在進行的調查、指導您如何回答問題，或要求您將資金轉至所謂「安全賬戶」。
- ✓ 請確保公司已設立既定程序，讓員工通報可疑情況，並確保全體員工均了解「遙距賬戶盜用」詐騙的風險。
- ✓ 加強員工教育——確保所有人員均認識「遙距賬戶盜用」詐騙手法，並已建立相應的通報及處理流程。
- ✓ 在付款流程中建立嚴謹的盡職審查文化，例如採用雙重審批機制，以加強風險防控。