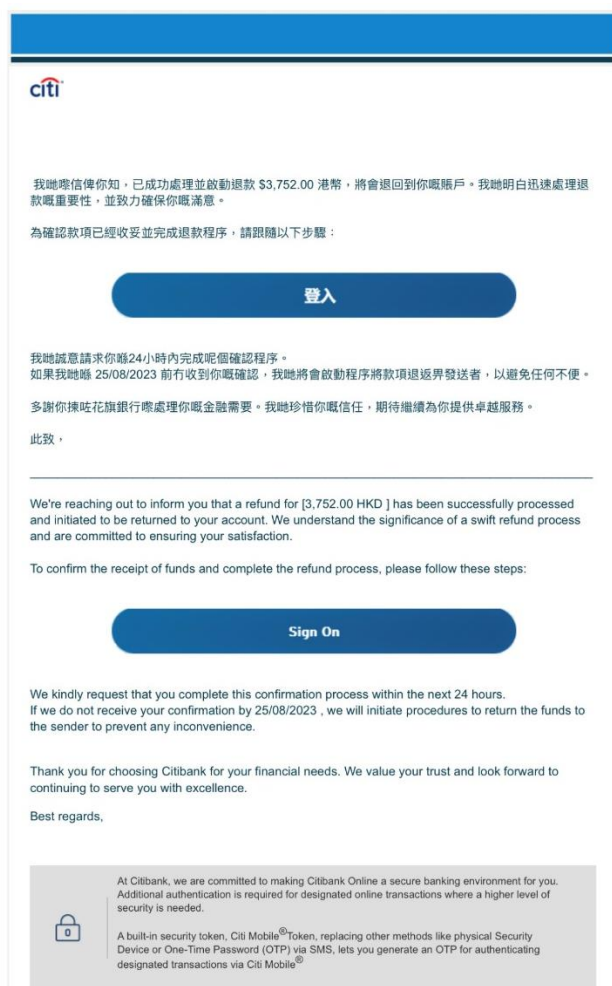


2023 年 08 月 23 日

提防虛假電郵

花旗銀行發現偽冒由本行發出之電郵，內附連結令客戶點擊至未經授權之網站，該網站要求客戶輸入銀行資料。

以下是虛假電郵之內容：



The image shows a screenshot of a fraudulent email from Citi. The email is in Chinese and English. It starts with the Citi logo and a message in Chinese: "我哋嚟信俾你知，已成功處理並啟動退款 \$3,752.00 港幣，將會退回到你嘅賬戶。我哋明白迅速處理退款嘅重要性，並致力確保你嘅滿意。" (We are writing to inform you that we have successfully processed and initiated a refund of \$3,752.00 HKD, which will be returned to your account. We understand the importance of a swift refund process and are committed to ensuring your satisfaction.)

Below this is a blue button with the Chinese characters "登入" (Log In). The text continues: "為確認款項已經收妥並完成退款程序，請跟隨以下步驟：" (To confirm the receipt of funds and complete the refund process, please follow these steps:)

Another blue button with the English text "Sign On" is shown. The email then says: "我哋誠意請求你唔24小時內完成呢個確認程序。如果我們唔曉 25/08/2023 前冇收到你嘅確認，我哋將會啟動程序將款項退返原發送者，以避免任何不便。" (We kindly request that you complete this confirmation process within the next 24 hours. If we do not receive your confirmation by 25/08/2023, we will initiate procedures to return the funds to the sender to prevent any inconvenience.)

The English version of the email is also visible: "We're reaching out to inform you that a refund for [3,752.00 HKD] has been successfully processed and initiated to be returned to your account. We understand the significance of a swift refund process and are committed to ensuring your satisfaction. To confirm the receipt of funds and complete the refund process, please follow these steps:"

At the bottom, there is a grey box with a lock icon and text: "At Citibank, we are committed to making Citibank Online a secure banking environment for you. Additional authentication is required for designated online transactions where a higher level of security is needed. A built-in security token, Citi Mobile® Token, replacing other methods like physical Security Device or One-Time Password (OTP) via SMS, lets you generate an OTP for authenticating designated transactions via Citi Mobile®"



以下為該未經授權電郵格式：

bsolak@oakmillbakery.com

csuarez@capitalprts.com

henrique.brito@partneer.pt

nchavarria@cfia.or.cr

danielle.swaw-kennedy@grapecreekisd.net

citibank@capitalparts.com

以下為該未經授權之網站：

<http://ig-papers.com/onmore>

<http://niaah.org/fly1>

<http://niaah.org/fly2>

上述未經授權之網站將用戶轉至以下冒充花旗銀行之網站以獲取個人資料

<https://kultura.mr.gov.ua/citi/login.php>

<https://kultura.mr.gov.ua/citi/CN/login.php>

花旗銀行重申沒有發出該電郵或與該虛假電郵有任何關係，並提醒公眾留意任何載有連結或要求輸入個人資料的電郵或短訊。客戶應在任何情況下切勿向可疑發件人提供任何個人或銀行賬戶資料。如果客戶擔心他們可能已經向此未經授權的電郵披露其個人資料，請立即致電花旗銀行電話理財服務 (852) 2860 0333 查詢及聯絡香港警察。請瀏覽花旗銀行網頁 www.citibank.com.hk 以索取更多有關電郵或網絡保安的資訊。