

2023年08月29日

## 提防虛假網站

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 screenshot shows a fraudulent email from Citi. The email header features the Citi logo. The main body contains the following text:

**Citi Mobile® Token**  
看來您的帳戶尚未啟用花旗行動電子權杖 (Citi Mobile® Token)。為確保您能夠持續不斷地存取我們全面的網絡和移動服務，我們誠懇建議您儘早啟用花旗行動電子權杖 (Citi Mobile® Token)。這個步驟對於您的安全和無縫體驗至關重要。

[啟用花旗行動電子令牌 \(Citi Mobile® Token\)](#)

**Citi Mobile® Token**  
It appears that the Citi Mobile® Token has not been activated on your account. To ensure uninterrupted access to our comprehensive web and mobile services, we kindly urge you to activate the Citi Mobile® Token at your earliest convenience.

[Activate Citi Mobile® Token](#)

**Citi Mobile® Token**

- 安全：**透過您選擇的6位數解鎖密碼保護，並限制於一部移動設備。
- 即時：**無需再等待短信，即可立即進行身份驗證。
- 方便：**輕觸您的移動設備上收到的通知，然後輸入您的解鎖密碼以進行身份驗證。

Thank you for your continued trust in Citi.

Best regards,  
Your Citi Team

Download the Citi Mobile® App  
[Download on the App Store](#) [GET IT ON Google Play](#)

Add your Card

Connect with us Online



以下為該未經授權電郵格式：

[E9INFO@ONECO.NE.JP](mailto:E9INFO@ONECO.NE.JP)

[info@tsx-com.co.jp](mailto:info@tsx-com.co.jp)

[Crawford.Brown@meter-u.com](mailto:Crawford.Brown@meter-u.com)

[usan11@mail.c-5.ne.jp](mailto:usan11@mail.c-5.ne.jp)

[amadou.diawara@edhec.com](mailto:amadou.diawara@edhec.com)

以下為該未經授權之網站：

<https://eichhorn-gems.com/device/cn>

<https://eichhorn-gems.com/device/en>

<http://drlashmd.com/cn.html>

<http://drlashmd.com/en.html>

<https://asigurari-online.md/en.html>

<https://asigurari-online.md/cn.html>

<http://www.monre.gov.la/cli/cn/>

<https://pfm.kebbistate.gov.ng/token/en/username.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](http://www.citibank.com.hk) 以索取更多有關電郵或網絡保安的資訊。