



提防非接觸式流動支付服務綁定或結合惡意軟件及 NFC 功能的詐騙

近日有騙徒冒充商戶或者機構發送釣魚訊息，誘導市民將支付卡（包括信用卡、扣賬卡及提款卡）綁定至偽冒裝置，或利用惡意軟件結合手機近場通訊（NFC）功能進行未經授權的盜刷。

與蜜桃保保一起拆解騙徒手法：

手法一：釣魚短訊及假冒綁定卡

騙徒假冒商戶發送短訊，以「貨品賠償」等藉口，誘騙市民輸入銀行卡資料及自動櫃員機（ATM）密碼後，在偽冒裝置上綁定受害人的支付卡。一旦受害人批准綁定請求，騙徒即可進行盜刷。

手法二：惡意軟件及 NFC 遙距讀卡

騙徒誘騙市民下載來歷不明的應用程式並獲取手機權限後，誘導受害人將支付卡貼近手機，利用 NFC 功能遙距讀取卡內訊息並進行盜刷。

蜜桃保保防騙守則：

- 切勿回覆或批准任何非本人發起的支付卡綁定請求，包括透過手機銀行應用程式或雙向短訊發出的要求或交易，並仔細閱讀銀行訊息及通知
- 切勿從不明網站下載或安裝應用程式。本行絕不會要求客戶把支付卡貼近手機背面作認證或解鎖
- 切勿向陌生人透露銀行密碼、卡資料、或一次性驗證碼（OTP）等敏感個人資料，亦絕不點擊訊息或電郵中的可疑連結、二維碼進行交易或提交資料

如客戶收到懷疑偽冒本行發出的訊息，請即致電中銀香港客戶服務熱線 (852) 3988 2388（選取語言後，按 3、#、2）。