香港仔 LION ROCK DAILY www.lionrockdaily.com 2022.8.3 | WED

■店員應把讀卡機拿到顧客面前作轉賬。 網上圖片

防信用卡盜刷 專家教路自保

信用卡是不少人日常的支付方式，既方便又快捷。不過，信息安全專家及密碼學家龐博文指，信用卡上充滿個人的敏感資訊，若不小心保管，可能會被不法之徒有機可乘。有不少市民就遇到信用卡被盜刷而追討無門的事件，招致金錢損失。到底一般市民的信用卡為何會被盜刷，以及應如何預防此事發生？

習慣性行為 助受害人申訴

被盜刷信用卡後，到底有什麼解決辦法？其實銀行是可查找這些被盜刷的賬目的證據和紀錄。現在所有發卡和收單銀行都支援一種名為「3D SEC」的安全機制，在這個機制下所有的信用卡轉賬紀錄，都會分析時間、地點等，作為持卡者的「習慣性行為」。銀行是可根據這些「習慣性行為」的紀錄，透過分析來判斷轉賬是否已被盜取？還是屬持卡者的慣常行為。因此，當發生盜刷時，記得要向銀行進行維權申訴。

龐博文小檔案

一個擁有接近半甲子（30年）經驗，由Apple IIe年代存活至今的前線信息安全專家及密碼學家。擅長有組織性網絡對抗、黑客術及電腦鑑證調查技能。其口頭禪為：「你今日畀人Hacked咗未呢？」

一般來說，每張信用卡都印有一些重要的敏感資訊，是絕對不可洩漏，其中包括：信用卡正面的信用卡編號（Credit Card Number）、到期日期（Expiration Date）、持有者名稱（Holder Name）及卡背面的安全編碼（CVV）。龐博文指，根據信用卡安全指引，所有商戶都不可儲存這些資訊，尤其是信用卡編號和安全編碼，更加是重中之重。龐博文解釋，當收到信用卡的收據存根時，只會顯示「前六後四」的數字（中間的數字都會被遮蓋）。此外，當使用信用卡進行網購，除了要輸入以上的資訊，還需另外輸入一個由手機短訊傳來的一次性密碼，作第二次認證才可成功轉賬。

信用卡不能離開視線範圍

既然整個交易流程都非常嚴謹，為什麼依然有人會被不法之徒盜刷信用卡呢？

龐博文表示，受害者應該是在兩種情況下被盜取了信用卡敏感資訊，「第一種是在現實世界消費時，例如在餐廳或酒店，顧客直接把信用卡交給店員，並離開自己的視線範圍進行轉賬。這情況非常危險，因現時的信用卡都已支援非接觸式轉賬。信用卡上面不是有一個晶片嗎？它的用途就是如此。正確做法應該是店員把信用卡讀卡機拿到顧客面前，在其視線範圍內作非接觸式轉賬。」信用卡離開持卡人的視線範圍，就有機會被人用手機拍下信用卡正反兩面的敏感資訊。

龐博文又指，「第二種情況就是透過電郵或紙本文件，把信用卡敏感資料交予店舖。這情況其實不時發生，如一些酒店透過電郵要求顧客在訂房時，把這些敏感資訊寫在電郵當中。」

開通SMS一次性密碼更安全

即使不法之徒拿到敏感資料，銀行不是還需要一次性密碼嗎？為何依然會被盜刷？龐博文解釋，賊人有可能知道此信用卡持有人的電話號碼。其中一種情況是透過電郵或紙本文件預訂服務時，信用卡持有人把電話號碼留下以作聯絡用途。在這種情況下，賊人只需透過一個短訊哄騙持卡人點擊手機上的不明來歷短訊，然後發動MMI快捷指令例如「*21」或「*64」，這樣就會把一次性密碼直接飛線到插入的手機上。

龐博文說更嚴重的是，有很多持卡人根本沒有啟動接收SMS一次性密碼；或不是所有網購網站都啟動支援一次性密碼機制，換句話說，部分網購網站只需輸入敏感資料就已可進行轉賬。

如要預防或避免這些情況，龐博文建議：「第一，持卡人應親身拿信用卡到收銀處結賬，而非轉交他人代辦；第二，千萬不要透過電郵、紙本或電話訊息，把信用卡敏感資料發放或告訴店員，因為他們根本沒需要知道這些資訊。」龐博文又指，商戶應設置一個合乎信用卡安全指引的網上收款程序，並不可能在電話或電郵向顧客查詢或紀錄這些敏感資料。此外，持卡人亦應向發卡銀行啟動SMS一次性密碼認證功能，及盡量使用預付卡或已限制轉賬數目的虛擬信用卡。