標準新訊

ISO 5201 金融服務—掃描條碼支付安全：有效降低行動支付風險

隨著智慧型手機普及，應用功能愈趨多元，行動支付也逐漸成為消費者慣用的付款方式，行動支付概略可區分為「二維碼(QR Code)掃描支付(常稱為掃碼支付)」(例如第三方支付、電子支付機構帳戶)與「感應支付」(例如國際三大 Pay 行動裝置錢包)等，其中掃碼支付已成為行動支付時代的主要應用模式，尤其在 2020 年新冠疫情(COVID-19)爆發後，零接觸方式可避免衍生染疫風險。依據資策會 2022 年的行動支付消費者調查結果顯示，消費者首選行動支付的偏好度於疫情期間快速成長，並預期行動支付常用度將有機會超越現金，消費者或商家樂於使用及導入此一新興支付方式，應用場域從過去的店舖、商場延伸至傳統市場、夜市、小吃攤，推升普及率及使用率，甚至有進一步取代實體錢包的趨勢。

然而，在「嗶一聲、掃一下」所帶來的便利背後，掃碼支付仍隱含著諸多的風險，可能導致使用者蒙受損失，因此，國際標準化組織(ISO)於今(113)年 4 月發布 ISO 5201「金融服務－掃描條碼支付安全(Financial services—Code-scanning payment security) 」，概述付款人於使用行動裝置操作進行掃碼支付交易時之風險評估、最低安全要求及延伸安全指南，該標準係基於 ISO 31000「風險管理－指導綱要」和 ISO/IEC 27005「資訊技術－安全技術－資訊安全風險管理」中規定的風險分析方法所建構，並針對掃碼支付設定安全分析的範圍與背景，同時定義基本架構及描述主要角色。掃碼支付基本上可區分為由收款人出示(主掃)或由付款人(被掃)出示支付碼圖片之 2 種模式，標準中分別就該 2 種模式於支付過程中可能衍生之風險進行評估與說明，並對如何採取對策以減少前述風險提出相對應的安全準則、要求與指南。

在我們日常生活中，常見的行動掃碼支付風險情形，列舉如下：

一、收款人公示之條碼被置換：付款人如未警覺而逕行掃碼，所支付金額將被移轉至收款人以外之其他帳戶而衍生交易糾紛。

二、條碼內被刻意植入惡意程式：付款人經掃碼後，包含身分證號、聯繫電話、帳戶資訊等個資，甚至行蹤動向等位置資訊均可能被竊取，進而造成嚴重損失。

三、偽造繳費通知及導向不易辨識之相似網頁：舉凡水、電、瓦斯、停車費與罰單等日常生活開支繳費通知，可能經變造後導致付款人的財物損失，另掃碼後導引至偽造之網頁，在付款人不察下，即可能洩漏個人機敏資訊。

針對前述情境，付款人為降低掃碼支付之風險，對於來源不明或用途可疑之條碼(例如：提供免費 WiFi 或換取精美小禮物)應保持警戒，經查證後再予掃碼；

對於商家公示之條碼應注意是否經過變造置換；掃碼後自動導引之網頁，應核實該網址(URL)之真假，以免蒙受損失。總之，掃碼過程中宜多一分謹慎，才能避免掉入掃碼陷阱。

除 ISO 5201 外，為因應行動金融業務的快速發展，ISO 另制定了 ISO 12812「核心銀行－行動金融服務」系列標準，該系列標準提供一個彈性的框架以適應新的行動裝置技術，包含應遵守適用的法規，例如：資料隱私、個人身分資料保護、消費者保護、反洗錢和預防金融犯罪等。該系列標準中之 ISO/TS 12812-4 則是規範個人行動支付(Mobile payments-to-persons)的案例及共通性要求，包含適用於個人行動支付的要求、運作機制的建議、不同案例的描述，並提供不同個人的行動支付之一般共通性模式、通用架構的技術實作建議、行動匯款建議等，以及具有對應交易流程的實用案例。

以我國行動支付發展情形而言，為因應支付工具多元，且諸多數據顯示消費金額逐年攀升，其中針對行動支付之 QR Code 部分，為建構更完善的使用環境，財金資訊股份有限公司在財政部的協助下，協同國內各銀行於 2017 年共同制定「QR Code 共通支付標準」，期透過既有跨行金融資訊系統及該共通標準建立共用平台，打造我國行動支付數位金流的高速公路，讓各銀行、基層金融機構、社會大眾及大小商家等，共享行動支付的便利，實踐普惠金融。此外，鑑於各式詐騙手法和駭客技術愈發精進，金融監督管理委員會於 2017 年頒布《金融機構提供 QR Code 掃描支付應用安全控管規範》，明文規定掃碼支付中被掃模式採用交易指示類 QR Code 者，因係屬使用者產生授權資訊同意扣款性質，應設定合理使用時效，且在時效內以使用一次為限，避免 QR Code 被攔截盜用，可保障交易雙方之安全性。

科技的進步為生活帶來諸多便利，但民眾仍應保

持良好的習慣及提高警覺，才能降低行動支付所帶來的風險及隱憂，可保持定期記帳及核對帳單的習慣，以避免「無感消費」可能衍生之債務償還問題。至於本文中所提及之 ISO 相關資訊可參考 ISO 官網，本局已和 ISO 簽有授權合約，民眾只需支付權利金，即可合法取得即時並已制定公布的標準資料，歡迎各界多加利用。如需查詢本局外國標準館藏狀況、價格及購買方式，請至本局「標準資料查詢系統」查詢或撥打服務專線 02-23431980 洽詢。

參考資料來源：ISO 5201、ISO 12812-1、
ISO 12812-4、中央銀行專題報告