PayPal

防範詐騙付款的
5 項措施

管理風險

詐騙付款與詐騙交易活動會對你的網路業務與銷售帶來影響。運用對的工具並落實正確流程，就能將風險降到最低，並保障業務及顧客安全 — 減少交易退款費用與財務損失。

詐欺犯如何下手

一般而言，網路詐欺犯最常利用兩種方式竊取金錢：

冒用帳戶：

這是常見的詐騙手法，詐欺犯透過電子郵件，騙取顧客在零售網站上的用戶名稱與密碼。接著登入帳戶、變更密碼、並進行未授權購買。

盜用身份：

即便商家已採取防範措施，詐欺犯還是想方設法駭進商家資料庫竊取個人資料。駭客常向其他詐欺犯兜售信用卡卡號，詐欺犯再於零售網站開設新帳戶，並以遭盜用的卡片進行購買，而被害人毫不知情。

防範詐騙付款的五項措施

監控所有交易，每日對帳

沒有人比你更了解自己的業務，例如有哪幾位大手筆的顧客、或顧客的消費習慣等。掌控自己的帳戶並確認有無異常，包括帳單地址、收件地址、及顧客實際所在位置之間是否有出入。

考慮設定交易上限

設定同一帳戶每日交易次數或是交易金額的上限。如不幸遇到詐騙，有助於將風險降至最低。

要求使用信用卡安全碼 (CVV)

支付卡行業(PCI)規範明訂不得將顧客的信用卡卡號、持卡人姓名與 CVV 一同儲存。此規範能有效預防網路詐騙，因為詐欺犯根本無法取得 CVV，除非他們同時能竊得實體信用卡。多數支付處理商皆提供附有 CVV 認證工具的結帳頁面範本，請善加利用。

嚴格的密碼條件

駭客會運用精密程式來計算各種密碼排列組合。目前已知的最佳密碼強度條件，必須至少 8 個字元的字母與數字混合，並包含至少一個大寫字母與一個特殊字元。

使用最新版本的平台與軟體

確認自己使用最新版本的作業系統 (OS)。作業系統供應商會持續進行軟體安全更新，以保障你不受安全漏洞所苦，也免於最新病毒及惡意程式的侵害。

關於防毒軟體的重要須知

建議安裝*商用*等級掃毒軟體並定期更新，以清除惡意軟體與間諜軟體。免費的個人版軟體防護力往往不足。如果你的網站是透過管理平台架設，平台的自動安全更新有助即時修補安全漏洞。

本文內容僅供參考。進行任何商務決策前，應另行徵詢專業而獨立的會計、財務和法律意見。