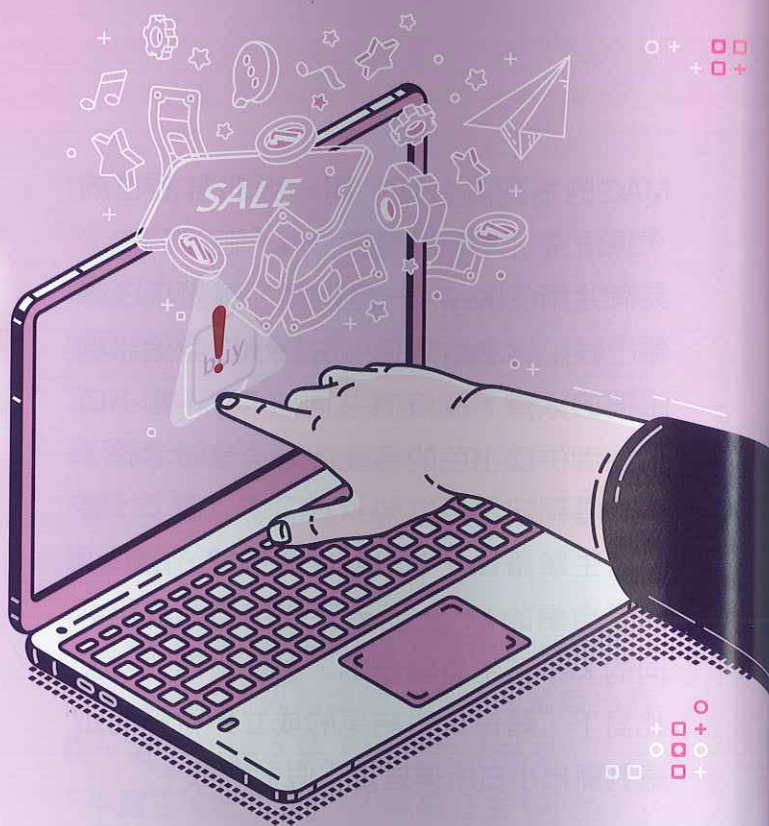


「一頁式廣告」 之潛藏風險



◆ 吳旻純

網路行銷商機無限，迎合人手一機的社會型態，成本導向的「一頁式廣告」應運而生。當沉浸在網路多元視界時，應隨時保持資安警戒意識，謹慎使用個人資料，避免落入詐騙陷阱，維護網路安全。

隨著資訊科技的日新月異，最常見的轉變是購物行為改變，在跨國境行銷之商業模式急速成長下，實體交易型態漸轉為無國界網路線上購物，不須出門即可購足所有想要的物品，加上近期震盪全球的新冠肺炎疫情，民眾因應防疫減少外出，更帶動電子商務倍速成長。電商運用各種行銷策略衝高營收，其中經濟效益高的一頁式廣告遂成為許多業者採用之行銷手法。



隨著資訊科技的日新月異與疫情的影響，民眾的消費模式已大幅轉向線上購物。

一頁式廣告內容集中聚焦、操作介面簡單友善，更重要的是透過飢餓式行銷來誘導消費者選購。（圖片來源：內政部警政署 165 全民防騙網，<https://165.npa.gov.tw/#/article/news/75>）

何謂「一頁式廣告」？

一頁式廣告 (Single-Page Website) 或稱為單頁式廣告，係指將所有商品資訊都呈現在一個頁面，圖片檔有時會內嵌動態或連結，提供買家進一步體驗及瞭解。一頁式廣告具簡單明瞭、使用者介面友善、特定主題及成本導向等特性。電銷商能吸引顧客迅速聚焦，使其在激烈競爭環境下，以最低成本獲得最大效益。

「一頁式廣告」特徵

一、簡單且內容聚焦

一頁式廣告因為版面限制，通常頁面

內容都相當簡單，商品內涵藉文字或影像意象化，以吸引買家瀏覽、點閱。

二、使用者介面友善

一頁式廣告網頁設計主要是讓使用者容易使用與集中體驗，以避免用戶於使用過程中被其他因素吸引或干擾，而中斷使用歷程，因此介面設計通常以容易使用為主。

三、飢餓式行銷

「飢餓式行銷」通指賣家營造商品「供不應求」氛圍，以此刺激消費者的購買欲，即運用人性愈得不到、愈想要的心理。例如，一頁式廣告使用的「期間限定」、「快閃」或「限時限量」等類型。

一頁式購物廣告特徵

- 特徵1：網頁上沒有公司地址、客服電話（或沒人接聽）、只留電子信箱。
- 特徵2：售價明顯低於市場行情。
- 特徵3：常以限時或倒數方式吸引民眾。
- 特徵4：免運費、號稱有7天鑑賞期及可拆箱驗貨。
- 特徵5：只能使用貨到付款或信用卡付款（使用信用卡將有被盜刷的風險）。
- 特徵6：網頁大多會有夾雜簡體字或使用大陸用語（直郵、郵費、支持換貨）。

刑事警察局
【惡意2折活動】Alpha1 Pro 遙控智能可攜化編碼機器人
【15天內免費退換，免費換新，運費全免】
【貨到付款，15天鑑賞期，無條件退換貨】

常見的一頁式詐騙廣告特徵。（圖片來源：內政部警政署165全民防騙網，<https://165.npa.gov.tw/#/article/news/85>）

「一頁式廣告」常見詐騙特徵

一、廠商聯絡資訊不明

詐騙網頁通常不會載明詳細賣方資訊，只留有通訊軟體帳號或電子信箱，有些甚至設有線上客服以取得信賴，其實是將用戶轉入另一個不明的網頁，藉機竊取個人資訊。

二、售價明顯低於市場行情

網頁通常會以超優惠價格吸引使用者，常見如「限時特價搶購」、「倒數」等用語。還有利用民眾同情心的悲情行銷手法，多出現於農產品等加工食品，誣稱因事故致農民陷入困境需要協助，實為假借援助之名，行詐騙之實。

三、網頁內容充斥簡體字或非臺灣用語

網頁文字使用簡體字或非常見語彙，如「包郵」、「直郵」、「支持換貨」及「信息」等，與臺灣「免運」及「留言」語意之用詞不同，使用者於瀏覽網頁時需特別注意。

四、網址網域不常見

網址冷僻或與知名網站網址雷同，藉以混淆使用者辨識。另外，知名入口網站如 Yahoo、Google 會使用 SSL 加密憑證，讓用戶得以傳送較私人資訊（如身分證字號、線上刷卡），即在網站和訪客共享的資訊之間增加特定編碼，網站會從 http 變成 https，以保障客戶的資料安全。因此，若一頁式廣告非使用 SSL 憑證，則該網頁之詐騙風險機率高。

五、主打免運費及便利運送付款

業者常用低價、免運及便利付款等口號吸引買家點閱，並以「貨到付款」即一手交錢、一手交貨的方式取信消費者，並看準信用卡付款易誘導消費者衝動購物心理，促使用戶因一時不查而被詐騙。

惡意「一頁式廣告」之資安危機

一天開始就與手機密不可分，打開 Yahoo 及 Google 等網站搜尋資訊、登入 FB、IG 或 YouTube 等社群媒體確認親友動態時，仔細觀察，就會發現一頁式廣告處處可見，不經意瀏覽點選，恐生資安疑慮。

一、惡意網站轉址盜取個資

詐騙的一頁式廣告資訊呈現通常不完整，藉以誘導使用者點取轉至外掛網址，而該網址實則為釣魚網頁（Phishing），當使用者鍵入個人資料後，就可能被不肖人士盜取利用，造成後續財物上損失，如常見盜刷信用卡、電話詐騙或被當人頭帳戶等情形。

二、植入勒索病毒綁架主機

一頁式廣告頁可能本身或轉址網頁都設有惡意程式，剛好用戶主機系統又有漏洞，用戶點選時，駭客藉機潛入並植入勒索病毒，綁架使用者系統，將所有檔案加密，要求支付贖金才能將檔案回復。

三、入侵通訊社群帳號，再詐騙他人

當惡意一頁式廣告竊取個資後，不肖人士可能會入侵使用者通訊及社群帳號竄改帳號密碼，假借其名義再詐騙他人。許多名人或網紅的粉專遭駭，就是被駭客看中其追蹤者多及高點閱率，此詐騙方式極易成功且有利可圖，但被駭者卻是欲哭無淚。

面對「一頁式廣告」之防護意識—資安 3P

一、個人資料重要性認知（Privacy）

當在通訊軟體或社群網頁上發現有興趣的廣告時，建議不要馬上點開，應先確



詐騙的一頁式廣告資訊呈現通常不完整，藉以誘導使用者點取轉至外掛網址，該網址實為釣魚網頁。



圖1 「一頁式廣告」之防護意識—資安 3P

認顯示資訊足堪辨識安全後再點取，並審慎填寫個人資料，以貨到付款取代線上刷卡，以降低風險。

二、定期電腦系統維護 (Protection)

電腦使用者要定期更新系統軟體，確認系統環境安全，並安裝正版軟體，避免駭客入侵竊取個資或植入勒索病毒等。

三、通訊社群帳號隱私設定 (Personalization)

在許多網頁或 APP 系統會要求使用者鍵入基本資料或者建議由社群通訊帳號直接連結，因此可以自動存取用戶其他如臉書動態、好友等情報。例如常用的 LINE 通訊軟體，如果用戶開放允許加好友，只要對方輸入手機就會自動變成好友。

使用者設定自動連動的情形下，就有可能會落入詐騙的陷阱，比如傳送詐騙購物連結或釣魚網站，如果不注意而點取，就有被盜取個資或造成財物損失之風險。因此使用者在登入、下載安裝外部、不知名的 APP 時，盡量不要自動連結社群帳號，並將通訊軟體隱私設定為不開放，以減少資安風險。

身處網路科技瞬變世代，人人均需不斷地自我調整修正，方能適應持續資訊社會化的過程。一頁式廣告呈現方式剛好符合智慧型手機頁面，正面效益是能帶動商機、活絡經濟；而負面影響則是有心人會利用一頁式廣告詐騙，造成使用者之財物損失跟資安危害。因此，人人均應切記「資安 3P」，以保障網路及個資安全。

陽光活力接地氣 廉能透明大臺中

陽光臺中 與廉同行

廣告



臺中市政府

TAICHUNG CITY GOVERNMENT

臺中市東區小型工程廉能透明機制

臺中市東區役男抽籤廉能透明機制

綠地園道

事後公開 www.east.taichung.gov.tw

富市臺中 新好生活 陽光政治 清廉城市