數位發展部
針對堵詐、阻詐成效（第一季）
書面報告

數位發展部

中華民國113年4月

壹、案由

根據警政署資料，今年1到5月詐騙案件相較去年同期激增21%，來到1萬3,363件，然而仔細翻查了數位部的預算以及打詐綱領等相關資料後發現，數位部毫無存在感，只不斷強調技術支援的角色，完全不符合人民對數位部成立的期待，據網路民調統計，民眾對數位部不滿意度達81%，是各部會間最高。以新制定的打詐綱領1.5版為例，統計各部會在綱領中被提及的次數，可以大致代表其工作負擔以及政策細緻程度，內政部出現了127次、法務部99次、金管會25次、NCC16次，數位部居然只有10次，甚至連外交部負責在外館網站轉貼防詐訊息出現次數都高過數位部，唯一讓人有印象的僅為建置政府短碼簡訊公用平臺，故要求數位部每一季應提供針對堵詐、阻詐作為以及相關具體成效之書面報告，並公告於官網供民眾查閱。

貳、說明如下：

依行政院「新世代打擊詐欺策略行動綱領1.5版」跨部會分工事項，數位發展部（以下簡稱數位部）主辦「加強電商業者資安維護」、「防制第三方支付詐騙」及「防制遊戲點數成為詐騙工具」等策略，相關措施及執行成效說明如下：

一、 強化「電商」資安與個資保護措施

（一）推動作法：

1. 強化電商資安防護能力：

利用企業資安評級工具安排資安顧問一對一輔導公協會會員進行評級工作，從111年至113年

3月底累計已協助88家公協會會員進行資安評級及紅隊演練，由資安業者模擬進攻業者服務平台，驗證其既有資安解決方案的有效性。

2. 推動電商業者導入隱碼技術：

隱碼技術將訂單收貨人電話號碼轉換為代碼，宅配單同步進行隱碼處理，物流士只透過平台撥打總機+撥接代碼與訂單收貨人聯繫，避免民眾電話外洩。目前已有5家主要業者已導入物流隱碼服務，2家業者積極導入進行系統與場域測試驗證，另有多家電商業者表達引入意見洽談中。

圖1　隱碼技術實例

3. 積極辦理個資外洩案件：

自111年8月27日起至113年3月底，本部接獲內政部警政署165通報疑似個資外洩的業者及由業者自行通報共57家，已結案54家(含曾依個資法裁處2家），經業者補充資料後給予觀察期2家，尚請業者補充資料1家。

4. 辦理行政檢查作業：

自111年8月27日起至113年3月底，針對重大個

資外洩或高風險、保有大量個資業者加強行政檢查，共計針對24家業者辦理29次行政檢查。

（二）重點成效：

依警政署通報民眾報案解除分期付款詐騙案件，自112年7月起數位部接獲通報電商業者案件已逐步下降。此外，自112年10月迄今數位部所轄大型電商平台已未列為警政署165全民防騙網公告之高風險賣場。

圖2　165全民防騙網公告圖

二、強化第三方支付管理措施

（一）推動作法：

1. 在「法遵面」部分：

已訂定「第三方支付服務業防制洗錢指引手冊」及其範本，協助業者進行法遵作業以及落實 KYC；並同時於112年8月底啟動洗錢防制查核作業，第三方支付業者如未落實法遵、不願配合改善或規避查核者，將依洗錢防制法相關規定進行裁罰。截至113年3月底止已主動辦理25家洗錢防制查核作業(包括法務部調查局通報疑似違反相關規定業者)，檢視業者於防制洗錢及打擊資恐作業有無落實。

2. 在「業務經營面」部分：

訂定「第三方支付服務業能量登錄制度」，要求申請業者提出洗錢防制及法遵聲明書始能登錄；未完成登錄者將請金管會要求銀行基於其未完成法遵以及確認客戶身分(KYC)等重要考量，不提供虛擬帳戶服務，僅提供低風險之信託或履約保證金專戶等業務服務。

3. 在「行政協助面」部分：

透過能量登錄制度掌握實質經營第三方支付服務業者名單，並提供通過登錄業者介接內政部戶役政系統及臺灣集中保管結算所實質受益人資料庫，未來亦協助開發掃描外部網站的系統工具，協助業者完成法遵規定，透過合法第三方支付業者的公示制度，減少詐騙案件之發生。

（二）重點成效：

本部綜合財政部、集保中心、銀行公會及與第三方支付服務業有業務聯繫關係之相關機關及公協會資料，國內目前實際經營第三方支付服務業之公司行號家數尚不足100家，截至113年3月底止，數位部數產署目前已受理84家業者申請能量登錄制度，包括國內主要第三方支付業者，並已召開14場審查會議，且將陸續於官網公告通過業者名單，業者目前審查進度為40家通過、28家審查後尚待補件、9家不通過、6家尚在資格審查中。

三、精進遊戲點數防治

（一）推動作法：

1. 針對遊戲點數阻詐提出四大措施防制：

遊戲點數被當成詐騙犯罪工具點數卡業者端積極溝通業者導入一次性驗證碼(OTP)，目前主要業者

皆已導入不定期OTP措施；遊戲端督促業者針對遊戲帳號進行儲值監控及遊戲行為監控，包括透過系統監控異常儲值情形、設置黑名單；超商端四大超商皆依營業額規模自律限制，單店單日最高3萬元限額、於販售機台設置購買遊戲點數警語；客服端督促業者增加客服處理人力，建立即時溝通平台。

2. 重點業者召開例行會議檢視其阻詐成效：

針對遊戲點數詐騙案件量較高之業者列為重點業者召開例行會議檢視其阻詐成效，促使業者推出「遊戲延遲入點」並搭配「點數防詐鎖卡平台」服務。

（二）重點成效：

據統計，整體遊戲點數詐騙案件數已自112年單月最高1,600件，下降至113年3月約百餘件。

四、建置「111政府專屬短碼簡訊平臺」

（一）推動作法：

1. 政府專用短網址服務：

數位部統籌建置「111政府專屬短碼簡訊平臺」，提供政府機關統一以111短碼發送政府簡訊，讓民眾透過識別簡訊來源為111電話號碼，即可確認簡訊安全無虞。

2. 簡化政府採購111簡訊之行政程序：

各機關透過共同供應契約自行下單採購發送111訊，簡化政府機關採購111簡訊之行政程序，擴111簡訊應用範疇。

（二）重點成效：

112年9月27日完成111簡訊平台建置，截至今(113)年3月底止，已有勞工局、執行署、台水、台電、豐原醫院等91個單位之民生業務，共發送逾745萬則簡

訊，簡訊類型包括水電繳費通知、補稅通知、罰款繳納、國民年金權益通知、門診異動等；並且已有136個單位，透過共同供應契約採購逾2,870萬則簡訊。

五、 本部與 TWNIC 合作利用 AI 對詐騙網頁進行封網

（一）封阻措施：財團法人台灣網路資訊中心(TWNIC)為協助網際網路接取服務提供者（IASP)，已規劃 DNS RPZ (Response Policy Zone, RPZ)自律機制限制接取惡意或不當的網域名稱，並以法律明確授權，且經法院判決、裁定或行政機關處分，始得啟動。

（二）緊急聲請範圍：TWNIC 近期並擴大處理範圍，針對檢警調認定涉及網路詐騙之網域名稱，緊急向 TWNIC 提出聲請，亦可啟動 DNS RPZ 執行網域名稱限制接取。

（三）TWNIC 為協助電信事業及 IASP 有效執行網路治理相關政策，規劃 DNS RPZ 自律機制，依法院判決或法律授權之行政處分要求各 IASP 業者封阻網域名稱。另檢警調等機關認定選舉期間執法機構緊急申請、重大金融犯罪、假冒中央二級機關網站或詐騙網站等重大案件緊急申請，亦可要求 RPZ 攔阻。自112年到113年3月 RPZ 攔阻網域累計42,593件。