臺東林區管理處政風室
112年5月號

公務機密

# 資訊安全維護

公務家辦

## 公務資料遭竊

＃使用家用電腦存放公務資料
＃密碼強度不夠
＃防護措施不足


### 資安時事案例

詐騙猖獗！刑事局破獲國內首件假基地台發送釣魚簡訊

普發6000元險被盜領 警逮2嫌查出多人個資

### 個人資料保護法

執行臨檢、路檢勤務時得否抄錄民眾身分證資料？

### 資訊安全防護

常見5大資訊安全威脅與對應資安防護措施

### 數位學習

105年資安動畫金像獎
David's Secret


## 詐騙猖獗！

# 刑事局破獲國內首件假基地台發送釣魚簡訊

周刊王CTWANT |中國時報林郁平
2023年4月7日

[周刊王CTWANT] 詐騙集團發送釣魚簡訊不是新鮮事，但刑事局首度查獲歹徒為躲避查緝，竟從大陸引進假基地台設備並安裝在車內，由31歲郭姓男子開車在北市鬧區四處發送釣魚簡訊。郭嫌到案後，警方清查至少有30多名被害人，詐騙逾300萬元，檢方複訊後聲押郭嫌獲准。

刑事局電信偵查大隊分析165反詐騙諮詢專線資料庫，發現去年9月至11月共接獲30多件假冒遠通電收ETC、玉山銀行釣魚簡訊的詐騙案。歹徒發送「eTag帳單自動扣款失敗」等簡訊內容，誘騙民眾點擊連結並輸入個資、信用卡號等資訊，詐團成員再以手機綁定行動支付方式，冒名在賣場、境外網站盜刷購買高價3C產品，總財損達300多萬元。

警方發現，被害人手機在接收釣魚簡訊時竟無通信紀錄，研判歹徒是利用在大陸已問世多年的假基地台發送。專案小組與電信業者合作掌握偵測技術，在台北捷運中山站前，查獲郭嫌開車發送釣魚簡訊，查扣假基地台設備及天線，為國內首件犯罪手法。

郭嫌去年8月底自大陸返台，坦承大陸詐團指示將假基地台設備裝在租賃車上，因假基地台的電波訊號比電信業者強，所以他開車到中山、信義區等捷運站出口或人潮聚集處，強制發送釣魚簡訊至民眾手機，每天最多發送2000則，可獲2000元酬勞。全案訊後依詐欺罪嫌移送雲檢偵辦。


# 普發6000元險被盜領 警逮2嫌查出多人個資

民視新聞網 2023年4月17日
民視新聞／陳崇翰 基隆報導

上週基隆一名顏姓男子，到ATM要領取全民普發6千元現金，卻被告知已經被登記在其他銀行帳戶。警方調閱登錄入帳IP位置，也查出手機門號所有者，成立專案小組，在彰化逮到王姓男子和姚姓女子。原來顏姓男子曾透過網路借錢，導致個資外洩，目前得知共有5人受害，所幸款項都沒入帳。

檢警一左一右，將王姓男子帶上車，並查扣犯案用手機等證物。原來他涉嫌，台灣首宗竊取他人個資，企圖詐領普發現金。
基隆一名顏姓男子，上周一到新北汐止超商，透過ATM提領失敗，撥打1988客服專線，卻被告知款項登記在不明銀行帳戶。

經警方調查，原來他去年初，曾透過網路借錢，當時將身分證、健保卡，拍給王姓男子。推測就此，個資遭到外洩，因為之後還遭人冒名註冊線上遊戲帳號。今年1月，顏姓男子才前往戶政事務所，變更身分證字號。

被害人顏先生說，「因為我之前身分證字號，有被人家冒名去登記註冊遊戲，怕我自己就不能領了。」

員警根據登錄的IP記錄追查，發現金融帳號的開戶人，就是這名30歲的王姓男子，而手機號碼，則是一名40歲的姚姓女子，他們盜用個資，企圖詐領普發現金。警方在嫌犯手機裡，發現共有5名受害人的登錄資料，所幸檢核機制卡關，款項都沒入帳。
基隆市警察局第三分局副分局長李惠煌表示，「本局刑警大隊持拘搜票，在彰化逮捕犯嫌2名，並在身上查扣手機當中，有發現多人的個資。」

警訊後，2名犯嫌依詐欺、洗錢防制法及個人資料保護法等罪嫌，移送地檢署偵辦。由於姚姓女子說詞反覆，案情交代不清，法院裁定收押，而王姓男子則諭令10萬元交保。後續也將擴大追查，是否還有更多類似個案。

# 執行臨檢、路檢勤務時得否抄錄民眾身分證資料？

- **內政部警政署 93 年 01 月 12 日警署行字第 0930002479 號函**
  - 警察職權行使法第 2 條第 2 項明定，警察為達成其法定任務，於執行職務時，得依法採取查證身分、蒐集資料等措施；又，依據電腦處理個人資料保護法第 3 條第 9 款及第 7 條規定，得為個人資料之蒐集。是以，警察執行臨檢、路檢勤務時抄錄民眾身分證資料，其基於「**犯罪預防**」、「**刑事偵查**」所為必要之個人資料蒐集，自無逾越該法授權之虞。

資料來源:花蓮縣警察局

# 常見 5大資訊安全威脅與對應資安防護措施

我們還可以將資訊安全細分成如下資訊安全種類，進一步採取合適的應對措施。

## 1.網路安全

是指針對連接網路裝置、網路中傳輸的資訊、利用網路運作的軟體及透過的服務，這些項目的安全都包含在網路安全範圍內，有心人士會透過對網路的侵害，來達到竊取敏感資訊，癱瘓裝置、軟體或服務等，進而製造出個人的身份被盜用與詐騙，甚至是企業的重要資料被竊取或無法正常營運等問題。

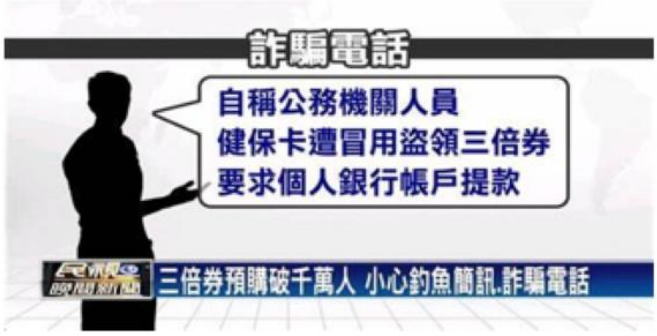
## 2.系統安全

電腦系統或者網站系統的安全，會隨著技術的日新月異，隱藏於其中的缺陷也隨之浮現或被發掘，這些缺陷我們通常稱之為漏洞，而漏洞的存在將使得系統和資料的保密性、完整性、可用性、授權機制都面臨有心人士的威脅。針對系統安全，通常會透過對漏洞進行管理作為應對措施。漏洞管理的第一步就是定期進行資安檢測，如系統弱點掃描，並以風險為依據排定補救措施優先順序。此外最好隨時檢測資訊環境中是否存在異常的網路行為，以提前發現漏洞。

## 3.應用程式安全

上述說明中有提到軟體安全中包含了應用程式安全，而應用程式玲瑯滿目，更與生活也息息相關，從文書作業、訊息的傳遞到商業的交易都有應用程式的存在。我們需要了解如何避免有心人士從應用程式的運作中，找出潛藏的漏洞，進而用以侵害個人隱私，財產甚至是人身安全。因此使用者必須留意且重視正在使用的應用程式之來源、發佈應用程式的單位或組織是否主動地檢視程式的安全性，並在整個應用程式生命週期內保護程式避免威脅迫害。降低網路犯罪者找出並利用應用程式中的漏洞來竊取資料、智慧財產以及機密資訊等行為。

資料來源:數位通國際網路有限公司




## 4.資料加密及身份認證授權

在資料安全上除了確保資料的保存外，也要考慮到資料被竊取的可能性，目前有許多的機制及技術能對資料進行加密，讓非經授權的有心人士無法識別及解讀，萬一發生被竊取時，可以藉此增加對資料的保護能力，降低損害。近期頻傳的勒索病毒也是對資料保護的嚴重考驗，過去單純保護資料不被竊取的方式，已經無法滿足這種惡意行為，必須採取新的資安思維及防護技術來保障資料。現今的生活中，已不再需要到特定地點辦理，使用網路就可以執行，大大地增加便利性，但隨之而來的問題是如何確保身份認證的授權身份、資料的管理及使用。近年來國際間提出許多相應的規範與認證，政府單位、金融機構服務及企業網站，可以參考或遵循國際標準或國家規範，來保護及使用民眾的資料。

## 5.雲端安全(雲端運算安全)

所謂的「雲端運算」與傳統電腦系統及架構不同之處，雲端運算是一定要透過網際網路來使用可共享的軟、硬體資源之運算技術。由於雲端運算是依靠著網路來實現，並且能將架構中的軟、硬體及應用程式，以共享的方式提供給不同用戶使用，因此在討論雲端運算安全時，必須將網路安全、系統安全、應用程式安全及資料加密安全及身份認證授權等條件一起考量，所以一個可靠且值得信賴的雲端運算環境必須同時具備多個面向的安全能力。