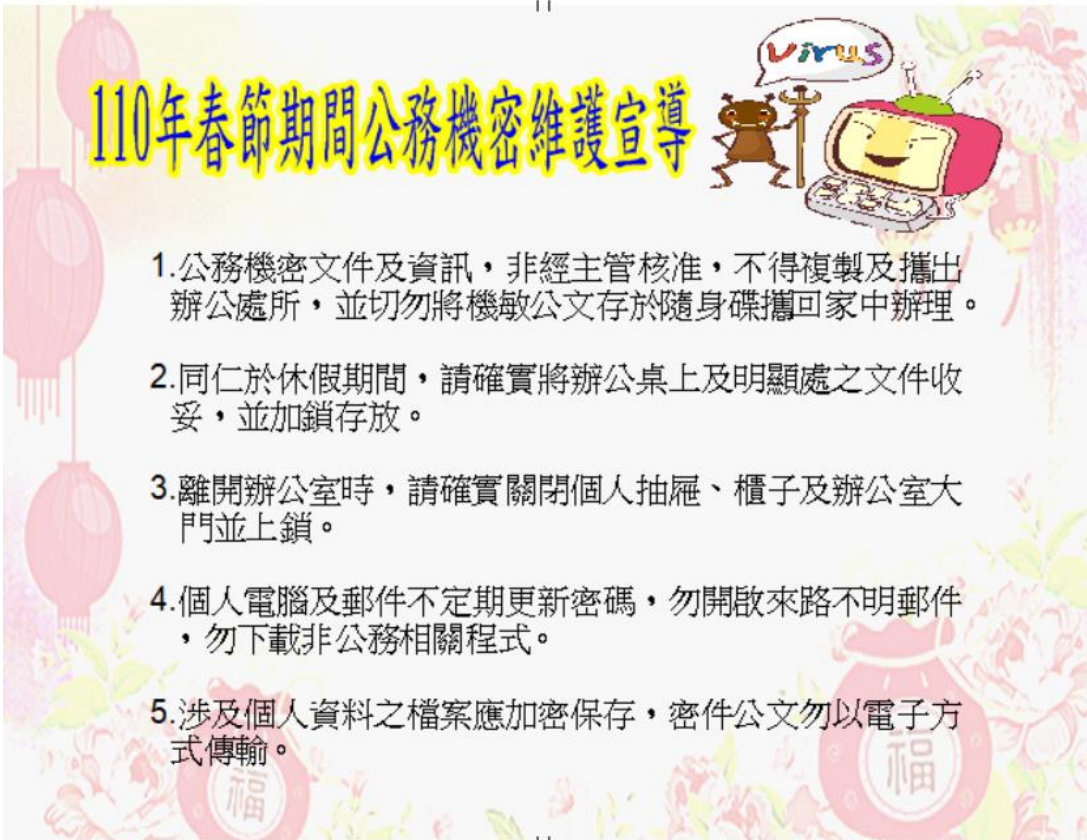


# 公務機密

## 資訊安全維護



### 110年春節期間公務機密維護宣導

1. 公務機密文件及資訊，非經主管核准，不得複製及攜出辦公處所，並切勿將機敏公文存於隨身碟攜回家中辦理。
2. 同仁於休假期間，請確實將辦公桌上及明顯處之文件收妥，並加鎖存放。
3. 離開辦公室時，請確實關閉個人抽屜、櫃子及辦公室大門並上鎖。
4. 個人電腦及郵件不定期更新密碼，勿開啟來路不明郵件，勿下載非公務相關程式。
5. 涉及個人資料之檔案應加密保存，密件公文勿以電子方式傳輸。

### 資安時事案例

哪些手機通ESS資安認證呢？

防止駭客入侵 專家教你自保4招

### 個人資料保護法

基隆正義哥翻帳單「寄垃圾給原主」  
違反個資？律師給答案

### 生活中的資安

由「刷臉」進校園事件，談  
生物特徵的個資保護

### 數位學習

104年資安動畫金像獎  
資安福音



## 哪些手機通ESS資安認證呢？

小丰子3C俱樂部 2021年1月14日

日前發生台灣大哥大貼牌的Amazing A32出廠前就被植入木馬程式有資安疑慮，引起喧然大波。為亡羊補牢，NCC除要求台灣大哥大需妥處A32 資安問題外，也新增規定「行動業者自有品牌手機在中國製造者，須符合資安標準才可販售」及「中國品牌手機、行動業者自有品牌中製手機將納入年度抽測標的」。消基會則呼籲政附應加速資安認證，加強資安管理的強度，確保5G時代消費者電信消費的品質保障。

目前有哪些手機通過智慧型手機系統內建軟體資通安全檢測技(ESS標章)呢？以下作一說明：為保障消費者使用智慧型手機資通安全，政府在 106年3月3日公告「智慧型手機系統內建軟體(Embedded Software on Smartphone Systems, ESS)資通安全檢測技術規範」，將手機內建軟體資通安全檢測認證(ESS標章)分成初級、中級及高級三種資安等級。

NCC也曾於108年下半年針對電信事業108年第1季銷售量較高之10款不同品牌智慧型手機進行抽測，經完成初測、複測及改善後，有9款手機通過測試，有一款手機兩次複檢都未通過。因智慧型手機資安檢測並非強制性規定，108年抽測後也就不了了之。由於智慧型手機安全檢測分屬NCC與經濟部所管轄，過去也未曾發生手機出廠前就被置入木馬程式的案例，所以智慧型手機資通安全檢測大都被政府與業者所輕忽。A32的案例，暴露政府與電信業者對於手機資安防護措施要求嚴重不足。

隨著智慧型手機與行動網路普及，網路上到處有危害資費的連結及APP，購買後的資安風險其實是遠大於購買前。要保護個人使用手機的資料與隱私安全，NCC提醒大家要有以下良好使用手機習慣的口訣：

### 一、三不：

1. 不強行取得根管理者 (root) 權限或越獄 (JB)
2. 不瀏覽可疑網站
3. 不連接可疑Wi-Fi接取點。

### 二、五要：

1. 要定期更新密碼
2. 要更新軟體程式及備份資料
3. 要關閉未使用的Wi-Fi/藍牙/NFC等介面
4. 連接的Wi-Fi接取點要開啟加密防護
5. 手機廢置前要刪除機敏資料。

## 防止駭客入侵 專家教你自保4招



財訊 作者: 林宏達

台灣的駭客大會是台灣每年一度的資安大會，許多特殊議程討論敏感攻擊案例，不對媒體公開。

採訪當中，我們遇到資安專家都會問，「你如何保護自己的資訊安全？」以下是資安專家的4個自保方法。

- 1、如何管密碼。創造幾個複雜的密碼片段，加在一起使用，例如，你有4段不同的密碼，上甲網站時，你用的是A密碼加B密碼，上乙網站時，則用B密碼加C密碼，這樣遠比萬用密碼安全，也簡化記密碼的負擔。
- 2、把公司和私人郵件信箱分開。很多人為了方便，把公用郵件和私人郵件都寄到同一個信箱，這會讓駭客容易一手掌握你所有資訊，把不同用途的信箱分開，不但便於管理，也能降低資安風險。
- 3、更新軟體。手機和電腦系統廠商都定期會提供軟體更新檔，許多是修補已被駭客發現的漏洞，更新能降低被攻擊的風險。
- 4、使用手機要小心。如果是安卓系統的手機，安裝App，會被要求跟功能毫不相關的權限，如手電筒程式要求存取通訊錄的權限，就要小心是不是間諜軟體，不要給App和用途無關的權限。也有駭客會製作假App，安裝程式前一定要看清楚。

## 基隆正義哥翻帳單

「寄垃圾給原主」 違反個資？

## 律師給答案



ETtoday新聞雲 2021年01月07日 12:43 記者劉昌松／台北報導

基隆正義哥受不了民眾亂丟垃圾，翻出垃圾中的帳單寄回「物主」，引起刺探蒐集個資的疑慮，但律師李尚宇認為，民眾隨處丟棄垃圾，應可預期會被人撿走，正義哥翻垃圾目的並非獲取不法利益或損害他人利益，且沒有「開拆信封」的行為，應無觸法問題。

李尚宇指出，《個人資料保護法》立法目的是「規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用」，罰則明訂「意圖為自己或第三人不法之利益或損害他人之利益」，而任意蒐集、處理及利用他人個資，可處5年以下徒刑，得併科1百萬元以下罰金。

依照新聞報導，亂丟垃圾的民眾應該知道，該處地點並非合法垃圾集中處所，可以預期垃圾會被人翻動或撿走，如果有覺得重要的東西，也應該會先自行銷毀、嘎碎等處理，而基隆正義哥因看不下環境髒亂，想把垃圾寄回讓民眾感受雜亂，目的並非獲取利益或損害他人利益，應不至於觸犯《個資法》。

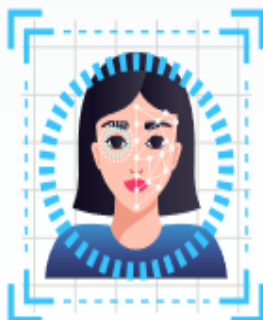
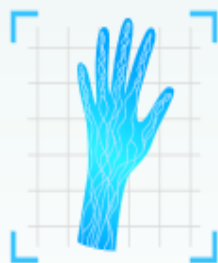
李尚宇表示，翻查帳單的行為，另外還有可能觸犯《刑法》妨害秘密罪，但與這起個案最接近的犯罪態樣，是可處拘役或9千元以下罰金的「無故開拆或隱匿他人之封緘信函、文書或圖畫」，而報導中的正義哥似乎也沒有「開拆信封」行為，也無違法問題。



# 由「刷臉」進校園事件， 談生物特徵的個資保護

◆ 大學講師 — 魯明德

報載近期某市議員接獲民眾陳情，指出某女中宿舍購置人臉辨識系統，有侵犯隱私權的疑慮。此新聞讓人聯想到，是否可妥善運用資訊科技來深化門禁管理，卻又不會侵害到隱私權的兩全其美做法。



生理特徵包含指紋、掌紋、掌型、虹膜、面容、聲紋及 DNA 等，行為特徵則有走路姿勢、心跳及簽名筆跡等。

生物特徵是某個人特有的生理 (Physical) 或行為 (Behavioral) 特徵。生理特徵包含指紋、掌紋、掌型、虹膜、面容、聲紋及 DNA 等，行為特徵則有走路姿勢、心跳及簽名筆跡等。由於生物特徵通常具有獨特、不易改變的特性，因此被廣泛用於個人辨識系統，如門禁管理、上下班打卡等……。

根據報紙報導，新北市某國中小在 108 年就推行刷臉入校，以臉部辨識的方式辨識學生進入校園，學生們直呼「好潮」、「上學更新鮮」；然中部某女中在

109 年 9 月購置人臉辨識系統後，卻引發家長對隱私權的擔憂。

在資訊界工作的小潘看到這些新聞後，思考著個人隱私跟資訊科技有沒有可能取得平衡？於是在每月一次的師生會上，就立刻提出他的疑問。司馬特老師聽完了這個大哉問之後，喝了口咖啡，緩緩回應小潘：這個問題可分成二個層面來看，一個是生物特徵、一個是個人資料。

在《個人生物特徵識別資料蒐集管理及運用辦法》第 2 條中，定義生物特徵識



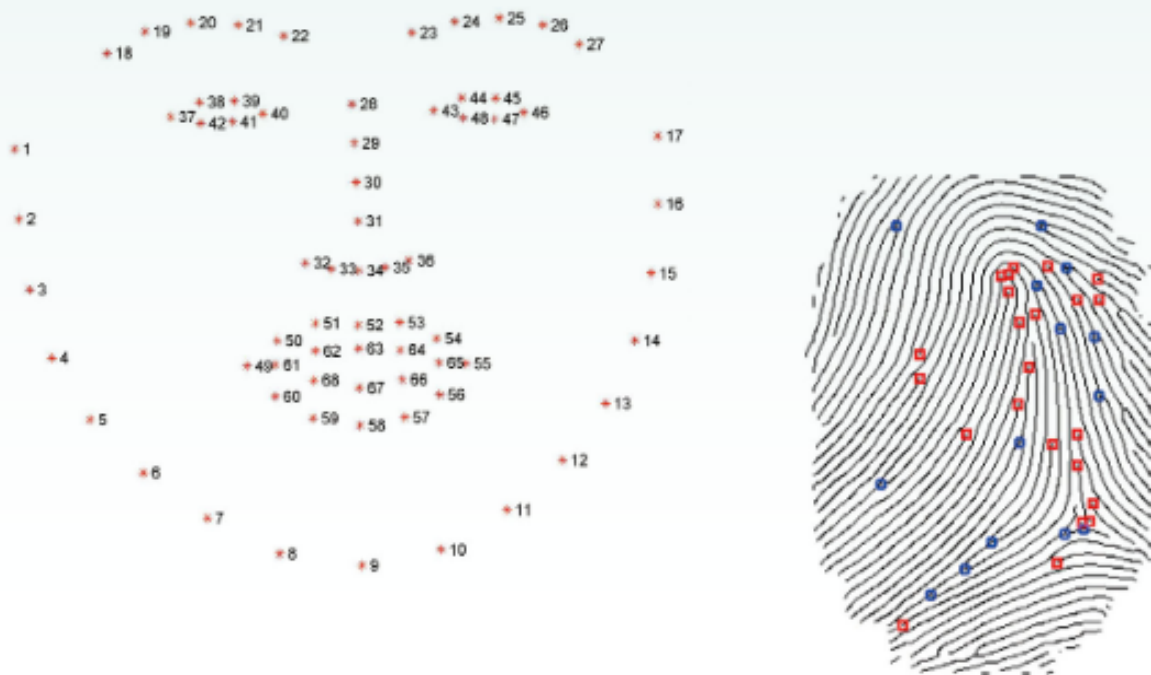
隨著科技的快速發展，近年來有越來越多校園引入人臉辨識技術，圖為弘光科技大學圖書館建置的人臉辨識系統。（圖片來源：弘光科技大學，<http://pr.hk.edu.tw/app/news.php?Sn=347>）

別資料是「指具個人專屬性而足以辨識個別身分之指紋及臉部特徵資料」。而在《個人資料保護法》第2條中，定義個人資料是「指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」。

由這個定義可以看出來生物特徵主要指的是指紋及臉部特徵，而個人資料則是

除了正面表列的項目外，還包含其他得以直接或間接方式識別該個人之資料，廣義來看，臉部特徵未在條文中列出，但仍然屬於可以識別出個人的資料。

小潘聽到這裡，馬上想到一個問題：有沒有方法不要識別出個人，又能有效的做門禁管理？司馬特老師想了想，喝口咖啡接著說，當我們存放在資料庫裡的資料不是人臉照片或指紋，再加上把資料去識別化（De-identification）後，就可以做到門禁管理又不會侵害隱私了。



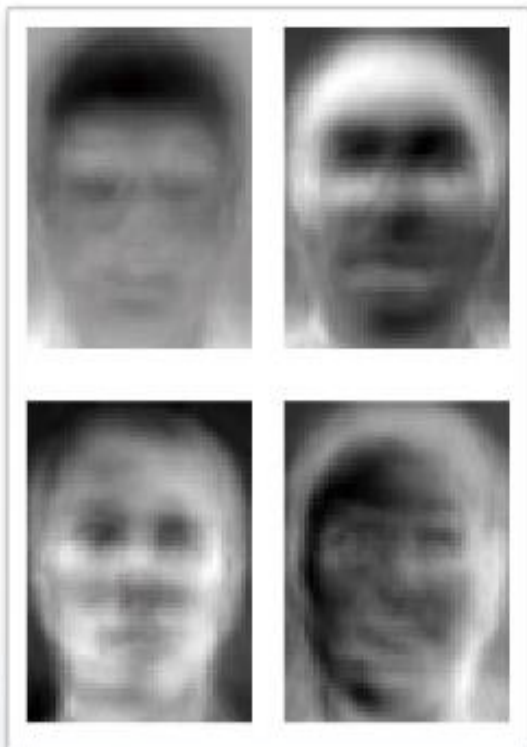
人臉與指紋的特徵圖。(Photo Credit: iBUG, Department of Computing, Imperial College London, <https://ibug.doc.ic.ac.uk/resources/300-W>; Hariyanto, S. A. Sudiro, S. Lukman, <https://uksim.info/aims2015/CD/data/8675a037.pdf>)

小潘聽得一頭霧水，資料庫裡不放人臉照片，要怎麼比對呢？司馬特老師拿出2張圖來說明，每個人的臉部或指紋上的特徵都不一樣，我們可以取得的是這些特徵點的座標及其特徵值（eigenvalue），這是一個多維的資料，再把每個人的這些位置座標與特徵值以演算法做成各自的特徵向量（eigenvector），存放到資料庫，作為日後門禁管理比對的基準。

舉例來說，在進行門禁管理時，若有一天有個小強要進門，人臉辨識系統便會根

據小強的這些特徵，分別讀取它的特徵值，做成特徵向量值後，再與資料庫裡的特徵向量做比對；若在資料庫中找到有相同的特徵向量，就表示小強是合法的使用者，可以開門放行；如果資料庫裡沒有相同的特徵向量，則表示小強不是合法的使用者，不會開門讓他進來。又因為門禁的資料庫裡只有特徵向量，並沒有小強的名字，即使看到特徵向量，也沒有辦法辨識出哪一個是小強，因此，就沒有洩漏行蹤的隱私權問題，也沒有個人資料外洩的問題。





人臉辨識系統會根據面部的特徵分別讀取它的特徵值，做成特徵向量值。(Photo Credit: AT&T Laboratories Cambridge, <https://commons.wikimedia.org/wiki/File:Eigenfaces.png>)

小潘接著問：那二個特徵向量要如何做比對？司馬特老師喝了口咖啡，繼續說下去，不論是存在於資料庫中的特徵向量，還是要做比對的特徵向量，都存在於多維度的特徵空間 (eigenspace)，只要把它們做餘弦 (cosine) 運算，如果  $\cos \theta$  運算的值為 1，則二個向量就可以視為是相同的向量。

小潘聽完司馬特老師的解說點頭如搗蒜，但是，反應快速的小潘立刻又想到另外一個問題，如果資料庫中只有特徵向量，有一天萬一機房發生問題，要找出誰曾經進去過，豈不是就找不到人了？

司馬特老師非常高興小潘能夠舉一反三，喝口咖啡接著說下去：這就是公司管理的問題囉，在建置員工的臉部或指紋特徵時，一定會有員工的姓名做對照，不然怎麼知道這個特徵向量是誰的，但是，放到門禁管理系統的特徵向量則是經過去識別化的，也就是只有把特徵向量放過去，這樣一旦有一天有異常資料要比對時，自然可以回到內部找出該特徵向量是屬於誰的。

小潘聽完老師一席話恍然大悟，原來資訊科技不只是電腦軟硬體，我們小時候念了半天不知其所以然的向量、三角函數，也有這種用途啊！華燈初上，這次的師生會就在焦糖瑪琪朵的香味中進入尾聲，小潘帶著滿意的答案吹著口哨離開。