國立高雄師範大學
個人資料管理教育訓練

于燿彰 博士

2019/07/10

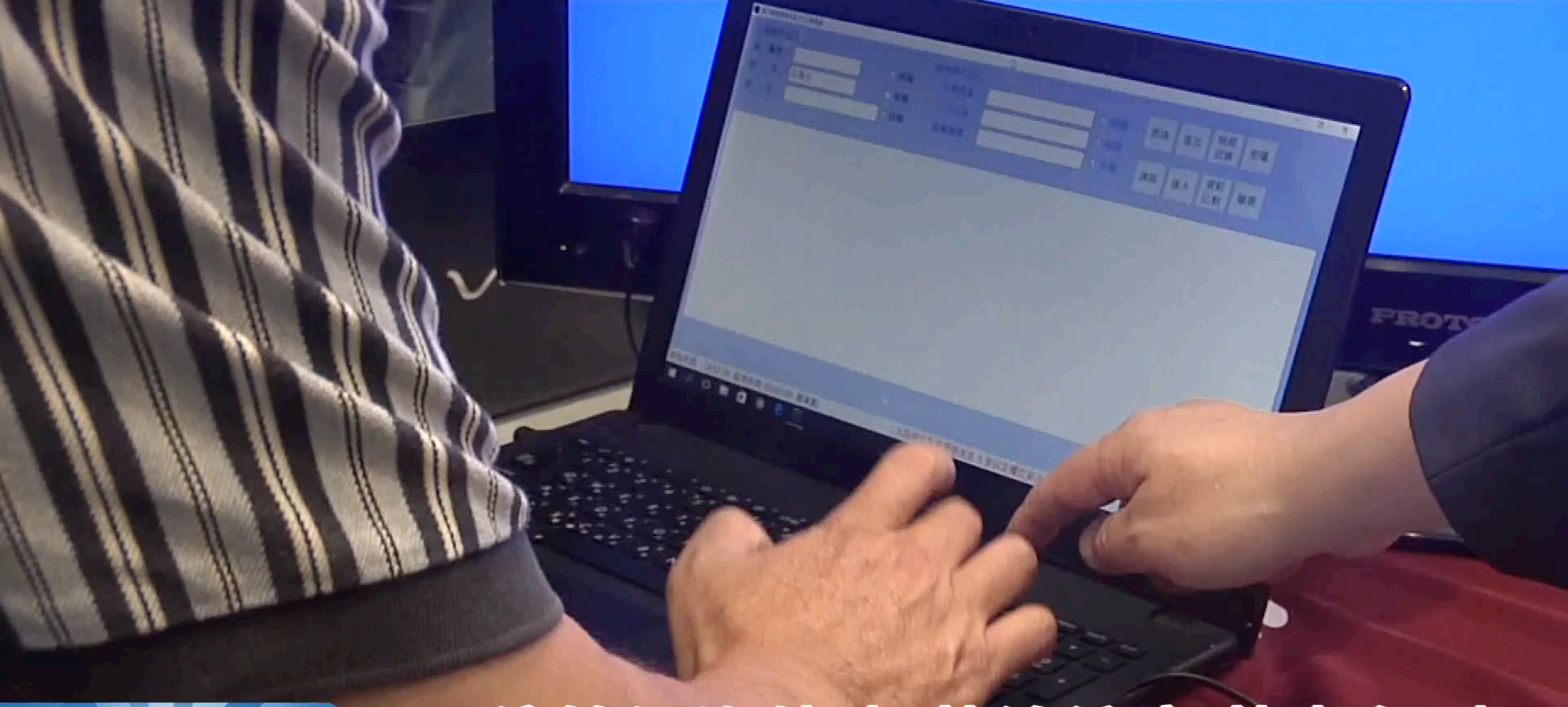
個人簡介

- 學歷:
  1. 國立成功大學 工程科學所 博士
  2. 密蘇里大學堪薩斯城分校 資訊工程所 碩士
- 經歷：
  1. 財團法人電信技術中心 資通安全組 副組長
  2. Hermes-Infortech Inc. 資深資安顧問/講師
  3. 鼎智國際技術服務有限公司 技術長/資深資安顧問
  4. 優士國際聯合顧問有限公司 技術長/資深資安顧問
- 專長:
  1. 網路通訊協定安全
  2. 資訊安全
  3. 管理系統(資訊安全、IT服務、營運持續、個人資料保護)
  4. 資安產品測試 (ISO/IEC 15408)
  5. 密碼模組測試(FIPS 140-2)
  6. 實體環境安全
  7. 密碼學
- 稽核員資格：
  1. ISO/IEC 27001稽核員
  2. ISO/IEC 7025稽核員
  3. BS10012稽核員
- 聯絡資訊:
  1. Email: avis.y@ustar-is.com
  2. Mobile: +886-928088726

大綱

- 個資洩漏案例
- 個資法簡介
- 個人資料保護管理

個資洩漏案例



1.7億筆個資外洩 蔡總統.郭董也在列

中天快點TV

台北

跨境網購留意 買3C商品恐個資外洩

娛樂要聞

- 五月天歌迷落寞 世足終戰播倔強
- 僅暖場空檔播出 電視根本沒轉播

⚠高溫黃燈 竹縣

現在溫度 宜蘭 28.5℃

IoT玩具外洩500萬筆兒童資料，香港商偉易達遭罰65萬美元

美國聯邦貿易委員會認為偉易達透過連網電子玩具及搭配App，在未經用戶同意下擅自蒐集兒童與家長資料，且未妥善保護資料，使駭客輕易竊取500萬筆資料，罰款65萬美元。

文/ 李建興 | 2018-01-11 發表

讚 4.9 萬 按讚加入iThome粉絲團 讚 183 分享 G+

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Press Releases » Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act

Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act

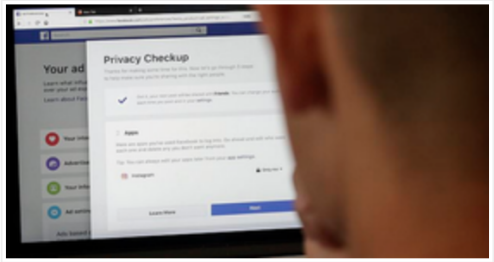
Settlement marks the agency's first children's privacy and security case involving connected toys

EVENTS CALENDAR

In English

臉書CEO祖克伯：雖然我們洩漏了8700萬筆個資，但沒有人是完美的，Facebook還是我來管最好

janus 發表於 2018年4月08日 10:00 | 收藏此文



儘管近來Facebook的爭議不斷，祖克伯可以說是四面楚歌，不過，顯然他依然覺得只有他是Facebook的救世主。他在針對媒體的劍橋分析事件中說明，根據臉書的調查，被劍橋分析收集及使用個人資料的用戶人數，達8700萬人，比原先估計的5000萬，多了3700萬人。不過，他覺得自己依然是Facebook最適合的領導人。

祖克伯還另外自爆了FB的另外一個漏洞，那就是在調查中他們發現，用戶可以透過輸入某人的Email或電話號碼，就可以取得這人在FB的公開資料，不過他表示他們已經刪除了這項功能。

《科技》公務機關個資頻外洩，政院：均啟動資安查核檢討

財經

A A A 友善列印

Facebook Google+ Twitter Weibo

20180717 20:31
豪宅市場回溫？帝寶名媛戶又喊賣 1年加價6200萬

20180717 20:17
境外電商營業人 明年起要開發票

20180717 20:09
SROI公益投資 有助企業社會資本

20180717 20:01
壽險網路投保保費上半年成長8倍 富邦奪雙冠

20180717 19:02

2017年03月31日 08:18 時報資訊 記者林資傑 / 台北報導

消基會昨（30）日召開記者會指出，公務機關近一年來已發生4起重大資安事件，外洩個資筆數高達13萬筆。行政院資通安全處對此表示，近期政府機關發生重大資安事件，均已立即啟動專案資安查核，進行事故檢討。

消基會指出，包括中華郵政「郵政商城」、勞動部「台灣就業通」、北市資訊局「薪資發放管理系統」及外交部「出國登錄系統」，近一年來接連傳出遭駭洩漏個資，分別達約1.7萬、3.4萬、7萬、1.5萬筆，呼籲應將資安問題納入檢調打擊犯罪專案計畫的執行範圍。

最新

2019.07.03 05:58

【情報員個資洩光光6】24萬公務員通通有獎　個資外洩可向銓敘部求償2億

文｜劉榮 林俊宏　攝影｜林煒凱

全文朗讀 00:00 / 02:01

銓敘部59萬筆公務員個資外洩，經過濾，其中部分資料重複，仍有高達24萬筆文官個資流出。對此，曾任台北地檢署主任檢察官、身兼律師的中華民國電腦稽核協會理事長張紹斌表示，依《個資法》規定，公務機關導致個人資料被竊取或洩漏，查明後應以適當方式通知當事人，每人每一事件賠償500元至20,000元，若被害人眾多，該事件賠償總額則以2億元為限。

8大情治系統個資爆外洩 馬政府時代疑已被中國掌控

週刊報導，國外網站揭露公務員重大資安事件後，行政院緊急調查，發現遭洩的個資還包括國安局、軍情局、調查局、警政署、檢察、海巡、政風及憲兵等8大情治系統，個資全部流出。（路透資料照）

英國航空洩50萬乘客個資，遭判史上最高罰金71億元

2019.07.09 by 楊晨欣

如何竊取個資

駭客釣魚竊個資案 木馬網站 真假只差一點

讚

2007-02-08

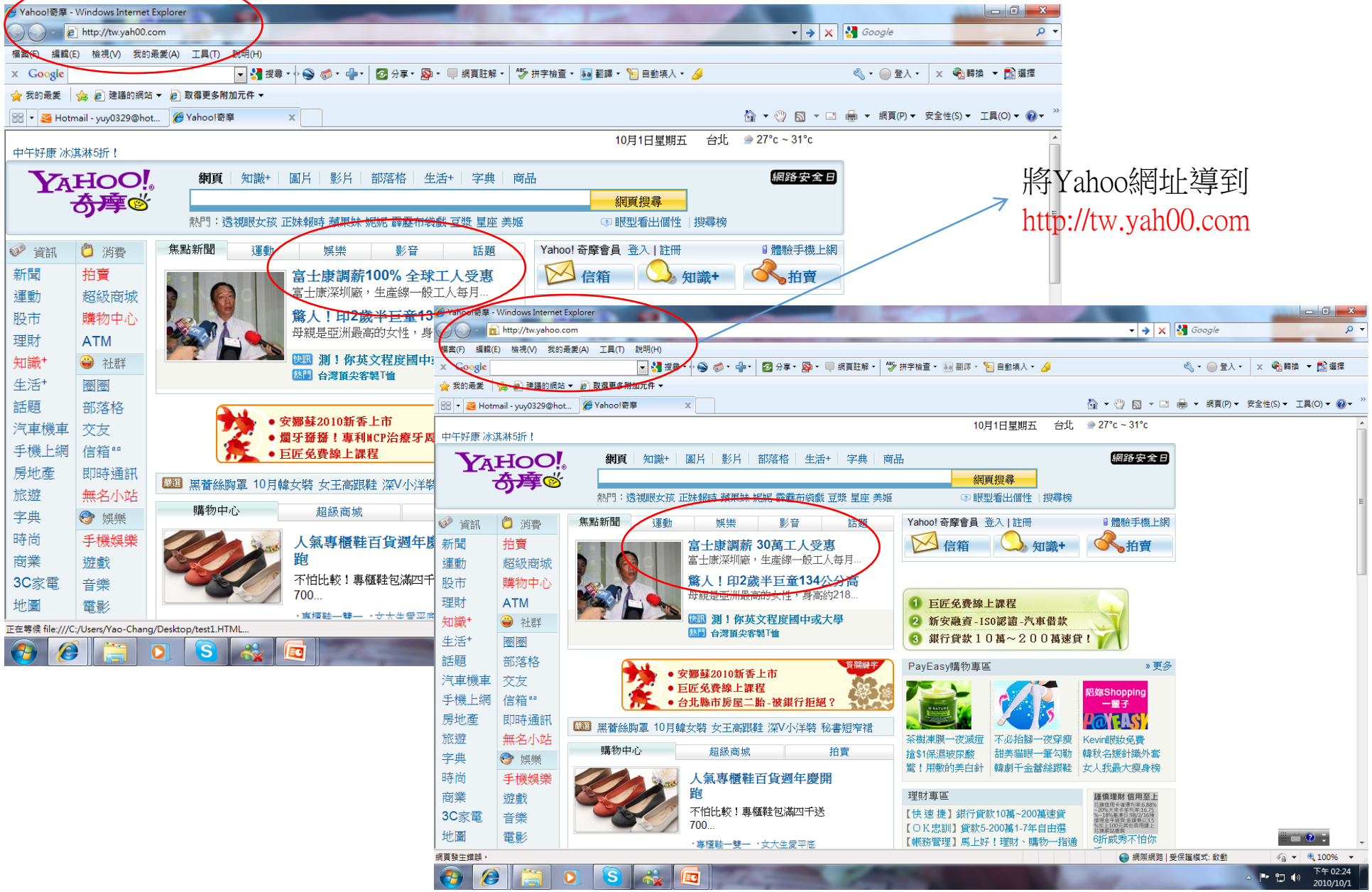
記者黃敦硯 / 特稿

刑事局追查兩岸駭客詐騙集團，發現歹徒是以變種的「網路釣魚」手法取得民眾個人資料，雖然同為架設冒牌網站，利用網友不察而誤連結，但新型的釣魚網站不像過去只竊取被害人的帳號、密碼，而會運用時下相當流行的關鍵字搜尋功能，趁機植入木馬程式，直接把整台電腦的資料偷光光。

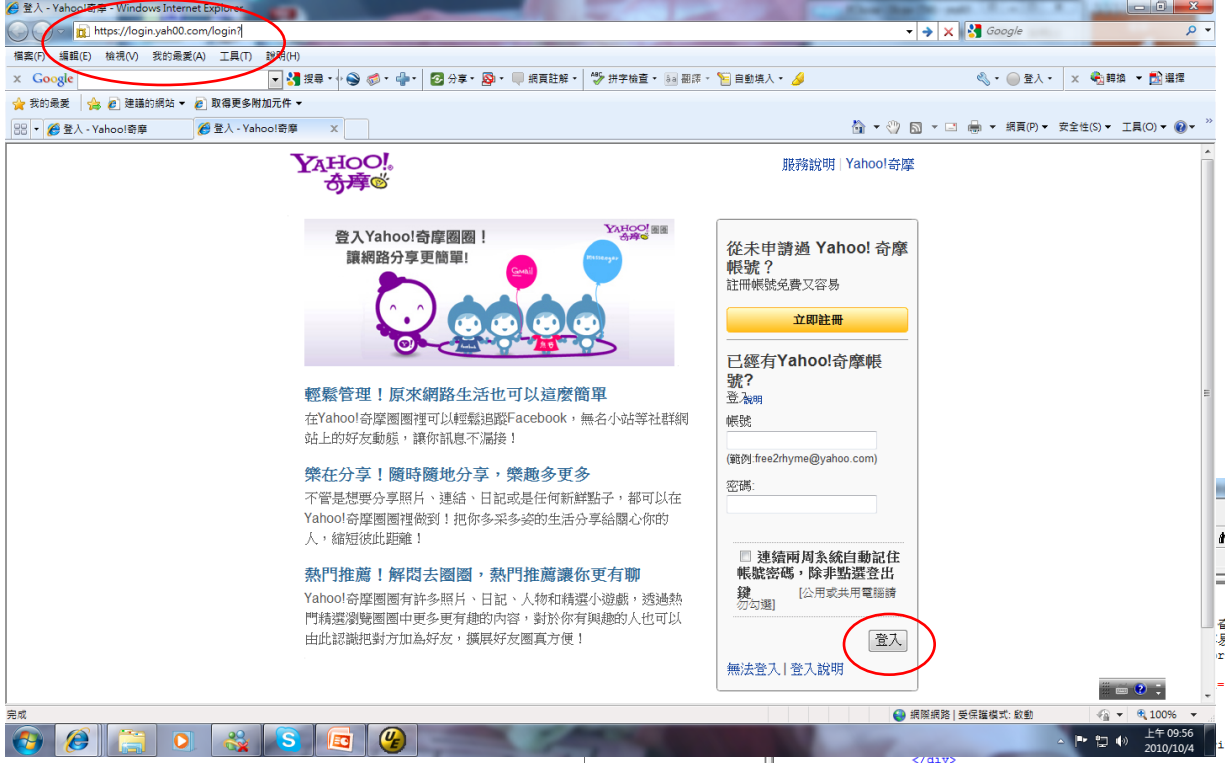
更厲害的是，當駭客將木馬植入後，會自動連回「正牌」網站，操作一切如常，民眾根本難以察覺異樣，但已暗暗執行駭客夾藏的木馬。

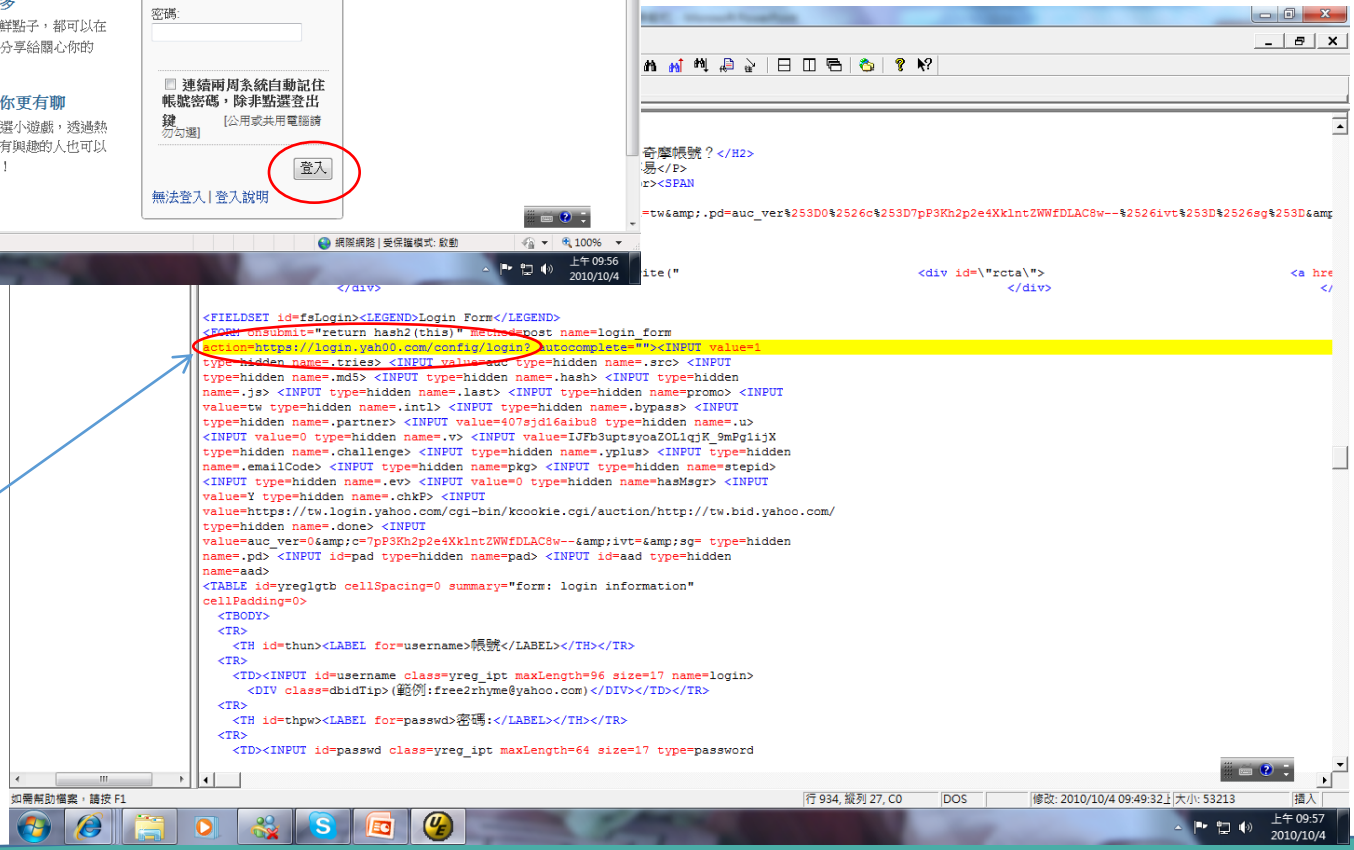
所謂的「釣魚網站」是指，駭客設計一個與正牌網站很像的網頁，讓網友一時不察而誤連結進入，並輸入自己的帳號、密碼，駭客再暗中偷走資料，可是駭客詐騙集團要的不只是帳號、密碼，而是要電腦裡全部的資料。

1、l n、h 網友難辨



將Yahoo網址導到
http://tw.yah00.com



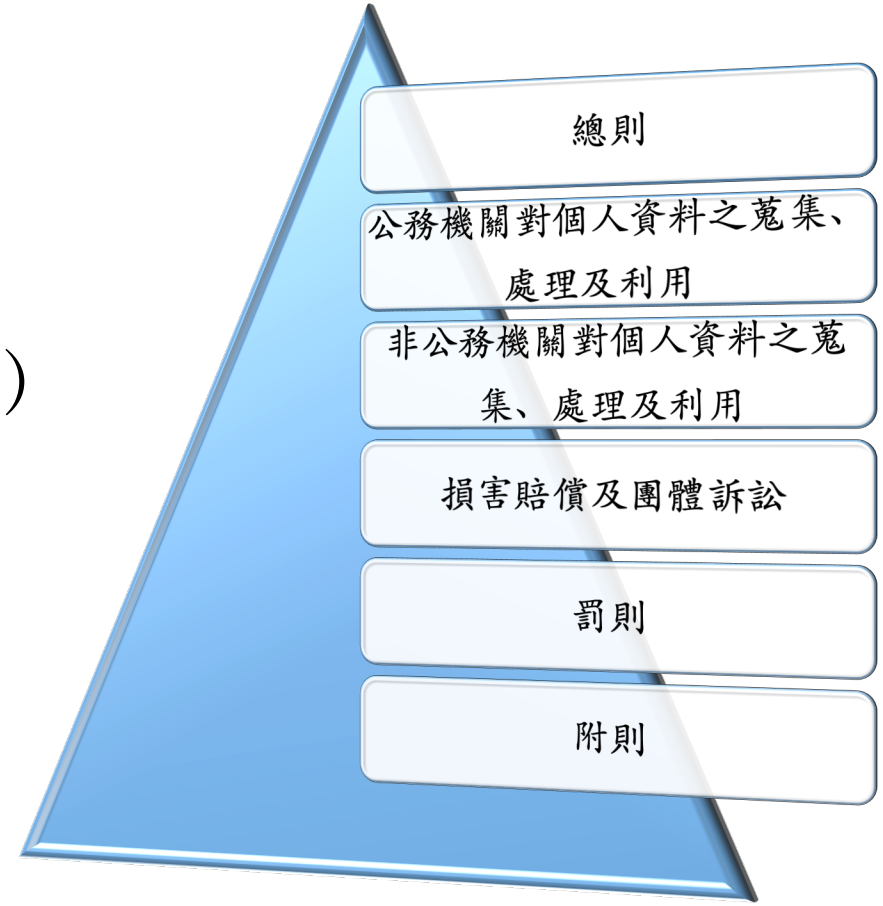


登入位址已更改成
https://login.yah00.com/login?

個資法簡介

個人資料保護法及施行細則

- 個人資料保護法（104年12月30日）
  - 六章
  - 56條
- 個人資料保護法施行細則（105年3月2日）
  - 33條



何謂個人資料

個人資料:（個資法第一章第二條）

1. 指自然人之姓名
2. 出生年月日
3. 國民身分證統一編號
4. 護 照號碼
5. 特徵
6. 指紋
7. 婚姻
8. 家庭
9. 教育
10. 職業
11. 病歷
12. 醫療
13. 基因
14. 性生活
15. 健康檢查
16. 犯罪前科
17. 聯絡方式
18. 財務情況
19. 社會活動
20. 及其他得以直接或間接方式識別該個人之資料。

個資法第一章第六條）

1. 病歷
2. 醫療
3. 基因
4. 性生活
5. 健康檢查
6. 犯罪前科

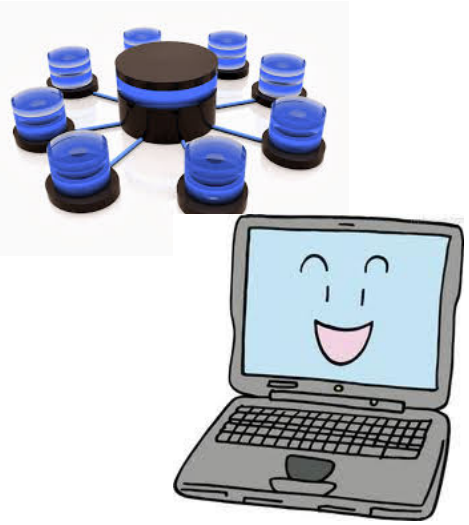
間接方式識別：（施行細則第三條）

僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能 識別該特定之個人。

類別	內容
特徵	年齡、性別、出生地、國籍、身高、體重、血型、抽煙、喝酒等。
婚姻	婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
	家庭其他成員之細節：子女、受扶養人、家庭其他成員或親屬、父母等。
家庭	是否結婚、配偶或同居人之姓名、前配偶或同居人之姓名、結婚日期、子女數等。
教育	學校紀錄：學歷、科系、畢業或肄業等。
	學生紀錄：學習過程、相關資格、考試成績或其他學習紀錄等。
職業	現行之受僱情形、離職經過、工作經驗、工作紀錄。
病歷	依醫療法(第六十七條)所定之病歷應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之病歷。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。(此部份尚未確定)
聯絡方式	傳統聯絡方式：電話、地址、電子郵件等。
	網路聯絡方式：MSN、SKYPE、Facebook、噗浪、微博、部落格、PTT 帳號等。
財務情況	帳戶之號碼與姓名、信用卡或簽帳卡之號碼、收入、所得、資產、投資、銀行、負債、支出信用評等、貸款、結匯紀錄、票據信用、津貼、福利、贈款等。
社會活動	移民情形、旅行及其他遷徙細節、休閒活動及興趣等。

個人資料檔案

- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式 檢索、整理之個人資料之集合。
  - 施行細則第5條：個人資料檔案，包括備份檔案。



蒐集

- 蒐集：指以任何方式取得個人資料。

第 8 條
公務機關或非公務機關依第十五條或第十九條規定向**當事人蒐集個人資料時，應明確告知**當事人下列事項：
一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

→ 直接取得

第 9 條
公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，**應於處理或利用前，向當事人告知**個人資料來源及前條第一項第一款至第五款所列事項。

→ 間接取得

特定目的

代號	修正特定目的項目
〇〇一	人身保險
〇〇二	人事管理(包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施)
〇四三	志工管理
〇四五	災害防救行政
〇六四	保健醫療服務
〇六九	契約、類似契約或其他法律關係事務
〇七二	政令宣導
〇七三	政府資訊公開、檔案管理及應用
〇七八	計畫、管制考核與其他研考管理
一〇七	採購與供應管理
一〇九	教育或訓練行政
一一〇	產學合作
一一三	陳情、請願、檢舉案件處理
一一六	場所進出安全管理
一一八	智慧財產權、光碟管理及其他相關行政
一二九	會計與相關服務
一三〇	會議管理
一三四	試務、銓敘、保訓行政
一三五	資(通)訊服務
一三六	資(通)訊與資料庫管理
一三七	資通安全與管理
一四五	僱用與服務管理
一四六	圖書館、出版品管理
一五七	調查、統計與研究分析
一五八	學生（員）(含畢、結業生)資料管理
一五九	學術研究
一六八	護照、簽證及文件證明處理
一七一	其他中央政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
一七六	其他自然人基於正當性目的所進行個人資料之蒐集處理及利用
一八一	其他經營合於營業登記項目或組織章程所定之業務
一八二	其他諮詢與顧問服務

資料類別

代　號　識別類：

C〇〇一　辨識個人者。
例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址及其他任何可辨識資料本人者等。

C〇〇二　辨識財務者。
例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

C〇〇三　政府資料中之辨識者。
例如：身分證統一編號、統一證號、證照號碼、護照號碼等。

代　號　特徵類：

C〇一一　個人描述。
例如：年齡、性別、出生年月日、出生地、國籍、聲音等。

C〇一二　身體描述。
例如：身高、體重、血型等。

C〇一三　習慣。
例如：抽煙、喝酒等。

C〇一四　個性。
例如：個性等之評述意見。

代　號　家庭情形：

C〇二一　家庭情形。
例如：結婚有無、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。

C〇二二　婚姻之歷史。
例如：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。

C〇二三　家庭其他成員之細節。
例如：子女、受扶養人、家庭其他成員或親屬、父母、同居人及旅居國外及大陸人民親屬等。

C〇二四　其他社會關係。
例如：朋友、同事及其他除家庭以外之關係等。

資料類別

代　號 社會情況：
C〇三一 住家及設施。 例如：住所地址、設備之種類、所有或承租、住用之期間、租金或稅率及其他花費在房屋上之支出、房屋之種類、價值及所有人之姓名等。
C〇三五 休閒活動及興趣。 例如：嗜好、運動及其他興趣等。
C〇三八 職業。 例如：學校校長、民意代表或其他各種職業等。
C〇三九 執照或其他許可。 例如：駕駛執照、行車執照、自衛槍枝使用執照、釣魚執照等。
代　號 教育、考選、技術或其他專業：
C〇五一 學校紀錄。 例如：大學、專科或其他學校等。
C〇五二 資格或技術。 例如：學歷資格、專業技術、特別執照 (如飛機駕駛執照等)、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等。
C〇五七 學生(員)、應考人紀錄。 例如：學習過程、相關資格、考試訓練考核及成績、評分評語或其他學習或考試紀錄等。
代　號 受僱情形：
C〇六一 現行之受僱情形。 例如：僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等。
C〇六三 離職經過。 例如：離職之日期、離職之原因、離職之通知及條件等。
C〇六四 工作經驗。 例如：以前之僱主、以前之工作、失業之期間及軍中服役情形等。
C〇六五 工作、差勤紀錄。 例如：上、下班時間及事假、病假、休假、娩假各項請假紀錄在職紀錄或未上班之理由、考績紀錄、獎懲紀錄、褫奪公權資料等。

資料類別

C〇六六 健康與安全紀錄。 例如：職業疾病、安全、意外紀錄、急救資格、旅外急難救助資訊等。
C〇六八 薪資與預扣款。 例如：薪水、工資、佣金、紅利、費用、零用金、福利、借款、繳稅情形、年金之扣繳、工會之會費、工作之基本工資或工資付款之方式、加薪之日期等。
C〇七二 受訓紀錄。 例如：工作必須之訓練與已接受之訓練，已具有之資格或技術等。
代　號 財務細節：
C〇八一 收入、所得、資產與投資。 例如：總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等。
C〇八四 貸款。 例如：貸款類別、貸款契約金額、貸款餘額、初貸日、到期日、應付利息、付款紀錄、擔保之細節等。
代　號 商業資訊：
C一〇三 與營業有關之執照。 例如：執照之有無、市場交易者之執照、貨車駕駛之執照等。
代　號 健康與其他：
C一一一 健康紀錄。 例如：醫療報告、治療與診斷紀錄、檢驗結果、身心障礙種類、等級、有效期間、身心障礙手冊證號及聯絡人等。
C一一七 政治意見。 例如：政治上見解、選舉政見等。
C一一八 政治團體之成員。 例如：政黨黨員或擔任之工作等。
C一一九 對利益團體之支持。 例如：係利益團體或其他組織之會員、支持者等。
C一二〇 宗教信仰。
C一二一 其他信仰。

處理

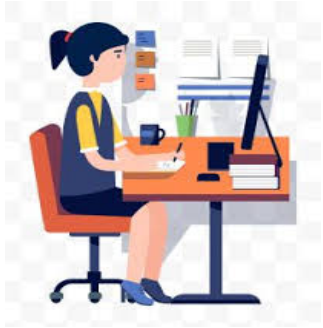
- 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、 編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
  - 新增文件、建檔案、輸入系統
  - 編輯檔案、刪除檔案、儲存檔案、複製檔案
  - 檢索查詢、更正錯誤、製作連結
  - 內部傳送至別部門/單位

利用

- 利用：指將蒐集之個人資料為處理以外之使用。
  - 對當事人使用其個資：如使用通訊錄打電話或寄信、E-mail。
  - 揭露第三方：如提供檢調單位調查、提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位。

個資當事人的權利

- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
  - 查詢或請求閱覽。
  - 請求製給複製本。
  - 請求補充或更正。
  - 請求停止蒐集、處理或利用。
  - 請求刪除。



職員

個人資料

人事室

資料建檔

人事薪資系統

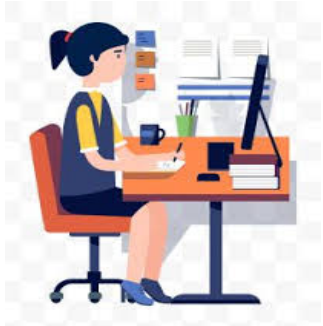
出納

查詢人事薪資資料

印領清冊

會辦核銷

主計室



職員

個人資料
（蒐集）

人事室

資料建檔
處理（輸入）

人事薪資系統

查詢人事薪資資料
處理（檢索）

處理（儲存、
刪除）

出納

印領清冊
處理（輸出）

會辦核銷
處理（內部傳送）

處理（儲存、
刪除）

問答 1

- 私立學校於實施教育之範圍內，為個人資料保護法所稱公務機關或非公務機關？

個資法問與答

【個資法即時通】私立學校於實施教育之範圍內，為個人資料保護法所稱公務機關或非公務機關？

張貼日期：2013/07/24

答：個資法所定之公務機關，係指依法行使公權力之中央或地方機關或行政法人。因此，公立學校如係各級政府依法令設置實施教育之機構，而具有機關之地位，應屬個資法之公務機關。至於私立學校，雖然由法律在特定範圍內授與行使公權力，惟私立學校在適用個資法時，為避免其割裂適用個資法，並使其有一致性規範，私立學校應屬個資法所稱之非公務機關。

(摘自「法務部102年6月24日法律字第10200571790號書函」-本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢)

問答2

- 學生校服如繡上姓名、學號是否違反個資法？

個資法問與答

【個資法即時通】學生校服如繡上姓名、學號是否違反個資法？

張貼日期：2015/03/31

一、按個資法係為規範個人資料之蒐集、處理及利用而設（個資法第1條規定參照）。旨揭疑義係學校要求學生於制服繡上姓名、學號，尚未涉及學校蒐集、處理及利用個人資料，故無個資法之適用，合先陳明。

二、次按教育部訂定之「學校訂定教師輔導與管教學生辦法注意事項」第21點第4項規定：「除前項情形外，有關學生服裝儀容之規定，應以舉辦校內公聽會、說明會或進行全校性問卷調查等方式，廣納學生及家長意見，循民主參與程序訂定，以創造開明、信任之校園文化。」是旨揭疑義係屬學校之教育管理規定是否合法妥適，宜由教育部本諸職權釐清。（摘自「法務部104年1月19日法律字第10403500300號函」-本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢）

問答 3

- 悠遊卡股份有限公司所發行結合各大專院校學生證功能之記名式悠遊卡，就蒐集學生個人資料之方式應如何適用個資法？

個資法問與答

【個資法即時通】悠遊卡股份有限公司所發行結合各大專院校學生證功能之記名式悠遊卡，就蒐集學生個人資料之方式應如何適用個資法？

張貼日期：2013/06/10

答：悠遊卡股份有限公司(下稱悠遊卡公司)所發行結合各大專院校學生證功能之記名式悠遊卡（下稱校園卡），悠遊卡公司與學校間訂有校園卡之採購契約，該契約之主體為悠遊卡公司與學校，惟該採購契約僅為提供悠遊卡公司與學生間成立契約關係之平台，學生後續使用校園卡乘坐大眾運輸交通工具或為其他消費行為，甚或票卡遺失時辦理申請掛失及返還餘額等事項，均係直接向悠遊卡公司為之，故有關悠遊卡公司若係依個資法第 19 條第1項第2 款規定而取得學生之個人資料，應係基於與學生間之電子票證定型化契約，而與學校間之採購契約無涉。另學校基於教育行政或學生資料管理之特定目的，蒐集、處理或利用學生之個人資料，包含核發學生證，惟就學生證結合記名式悠遊卡之功能，由學校將學生之個人資料提供予悠遊卡公司，為特定目的外之利用，應區分公立學校或私立學校而分別依個資法第16條但書、第20條第1項但書規定為之。

個資法16條

- 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法 定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者 ，得為特定目的外之利用：
  - 一、法律明文規定。
  - 二、為維護國家安全或增進公共利益所必要。
  - 三、為免除當事人之生命、身體、自由或財產上之危險。
  - 四、為防止他人權益之重大危害。
  - 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當 事人。
  - 六、有利於當事人權益。
  - 七、經當事人同意。

個資法20條

- 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集 之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利 用：
  - 一、法律明文規定。
  - 二、為增進公共利益所必要。
  - 三、為免除當事人之生命、身體、自由或財產上之危險。
  - 四、為防止他人權益之重大危害。
  - 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當 事人。
  - 六、經當事人同意。
  - 七、有利於當事人權益。

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。
非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

個人資料保護管理

個資安全維護

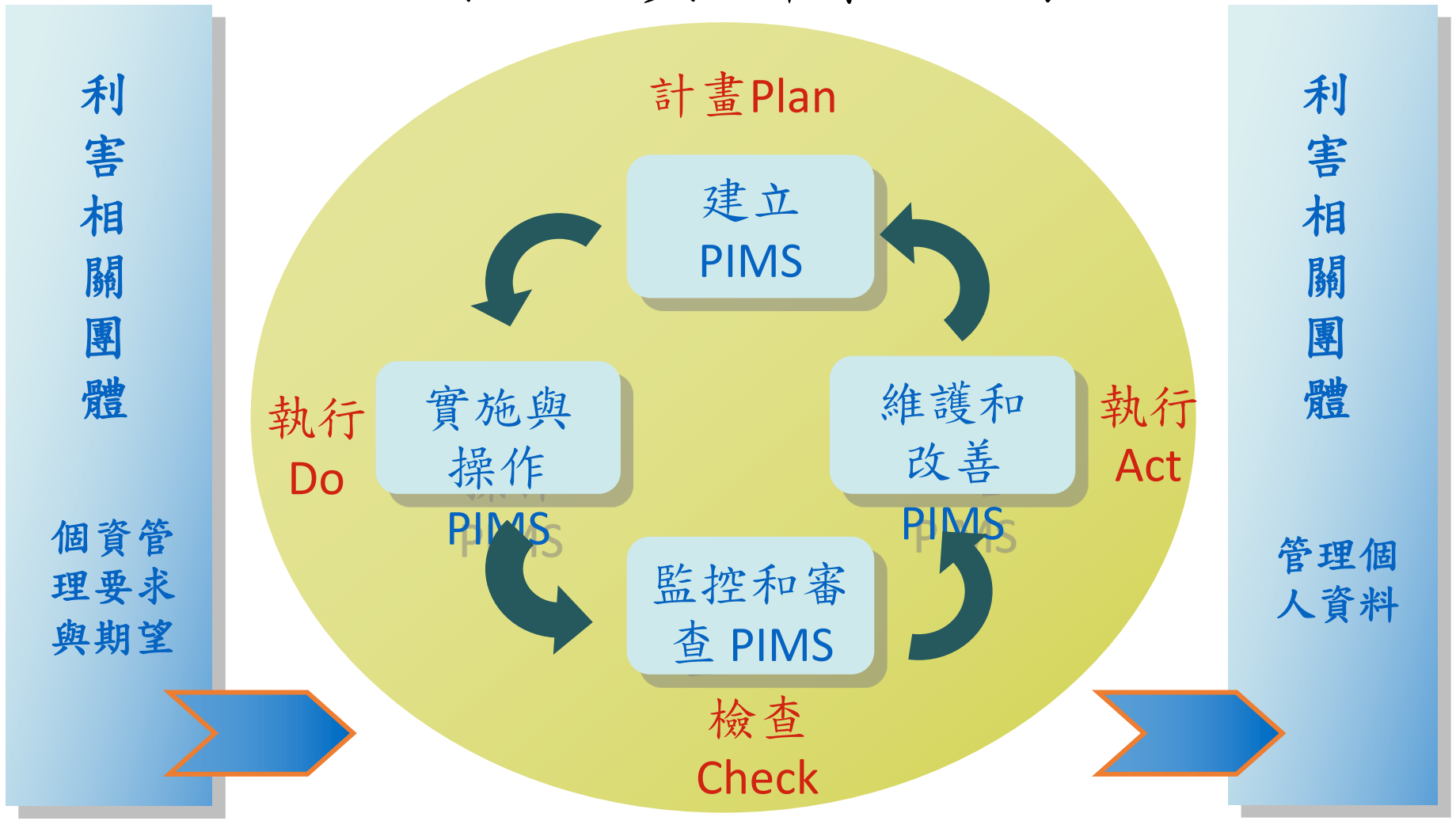
- 個資法
  - 第六條第一項但書第二款及第五款所稱適當安全維護措施
  - 第十八條 所稱安全維護事項
  - 第十九條第一項第二款及第二十七條第一項所稱適當 之安全措施

- 施行細則
  - 一、配置管理之人員及相當資源。
  - 二、界定個人資料之範圍。
  - 三、個人資料之風險評估及管理機制。
  - 四、事故之預防、通報及應變機制。
  - 五、個人資料蒐集、處理及利用之內部管理程序。
  - 六、資料安全管理及人員管理。
  - 七、認知宣導及教育訓練。
  - 八、設備安全管理。
  - 九、資料安全稽核機制。
  - 十、使用紀錄、軌跡資料及證據保存。
  - 十一、個人資料安全維護之整體持續改善。

BS10012: 2017 個人資料管理系統

- 合法、公平且透明的處裡
- 僅基於特定合法目的取得
- 適當、相關及限於資料侷限原則
- 正確並即時更新，盡可能沒有任何延遲的刪除或更正
- 資料的儲存不得超過許可的必要
- 使用技術及組織方法以適當確保個人個人資料的安全、正確及機敏

BS10012: 2017 個人資料管理系統 PDCA



Annex SL (架構改變)

- BS 10012: 2017 年版個人資訊管理系統標準已參照 ISO 組織 Annex SL 對撰寫標準本文 PDCA 架構來撰寫，當組織擁有重疊的管理系統時，例如:品質管理(ISO 9001)、環境管理(ISO 14001)、資產管理(ISO 55001)、資訊安全管理(ISO 27001)，或營運持續管理(ISO 22301)等，可以透過此一共同架構適當整合。

BS10012:2017

條款四、組織全景	P
條款五、領導與承諾	P
條款六、規劃	P
條款七、資源	P
條款八、運作	D
條款九、成效評估	C
條款十、持續改善	A

BS10012:2009

條款三、規劃PIMS	P
條款四、實作與運作PIMS	D
條款五、監督與審查PIMS	C
條款六、改善PIMS	A

Plan （規劃）	條款 4 Context of the organization 組織全景	條款 4.1 Understanding the organization and its context 瞭解組織及其全景，需要鑑別與個人資訊管理有關之內部外部 議題
		條款 4.2Understanding the needs and expectations of interested parties 瞭解關注方的需要及期望，需要辨識關注 方以及其對組織個人資訊管理系統的期望內容。
		條款4.3 Determining the scope of the personal management system 確認個人資料管理系統範圍
	條款 5 Leadership 領導作為	條款 5.1Leadership and commitment 領導及承諾
		條款 5.2 Policy 政策:對於政策必要時提供予關注方，以及 政策內容對於內部外部議題、關注方要求的增加。

條款6 規劃

- 條款 6.1.2 Data inventory and data flow 資料盤點與資料 流向:由於 GDPR 將資料控制者、資料處理者、協同資料控 制者、第三方，以及委外廠商等均有不同的法律責任與規範，
  - 目的
  - 類別
  - 說明個人資料的流向 外
  - 資料控制者
  - 資料處理者
  - 協同資料控制者
  - 第 三方
  - 以及委外廠商等角色
  - 以及所使用的關鍵系統、存放位 置，及個人資料保留時間表等資訊。

條款6 規劃

- 條款 6.1.3 Legal basis 法源依據
  - 需確認蒐集、處理、利用個人資料與特種個人 資料的法源依據
    - 個人資料保護法第 15 條、第 16 條、第 19 條，及第 20 條第 1 項要求銜接。
- 條款 6.1.4 Privacy impact assessment(PIA)隱私衝擊分析 及條款 6.1.5 Privacy risk treatment 隱私風險處置
  - 建立隱私衝擊分析方法論 以符合 GDPR 第 35 條個人資料衝擊分析要求 。

GDPR Article 35: Data protection impact assessment
第三十五條　資料保護影響評估

條款6 規劃

- 條款6.1.6 Priorconsultationandauthorization事前諮詢與授權
  - 符合 GDPR 第 36 條第 3 項要求，要求組織建立該機制
- 條款 6.1.7 Privacy by design and by default 從設計著手保 護隱私
  - 符合 GDPR 第25 條要求，組織於設計重大變更時須適當的以組織化與技術 程序實現從設計著手保護隱私控制要求，並留存相關紀錄。
- 條款 6.2 PIMS objectives and planning to achieve them 個人資訊管理系統目標與達成之規劃
  - 組織除應文件化個人資訊管 理系統目標外，目標應盡可能可被量測，並規劃量測的頻率、 時間、評估量測的方法、執行量測的人員，以及所需的資源等。

條款七支援

- 條款7.1 資源
- 條款7.2 能力
- 條款7.4 認知
- 條款7.5文件化資訊

Do 實施

條款八 運作

- 條款 8.2.1 Key appointments 重要人員之指派
  - 條款 8.2.1.2 Data protection officer(DPO)資料保護官:
  - 符合 GDPR 第 37 條至第 39 條要求，規範組織應選定資料保護官，並明訂資料保護官 的責任與工作。
- 條款 8.2.6 Fair, lawful and transparent processing 公平、合法 與透明化的處理:
  - 條款 8.2.6.1 Collection and processing of personal information 個人資料蒐集與處理
    - 將對資料主體直接或間接蒐集個人資料所為之告知 要求，從原有的 privacy notice 隱私權公告或 online privacy statement 線上隱私權聲明，統一改為 privacy right information 隱私權資訊;隱私權資訊告知的內容具體化『讓 處理過程公平與透明的任何其他資訊』，例如:保存期限的準 則、資料主體向主管機關申訴的權利，且對於有關資訊可能用 於任何自動化決策和/或剖析時，包括所涉及的邏輯和對資料 主體的影響等。

條款八 運作

- 條款 8.2.6.2 Records of privacy information(such as notices and statements)隱私權資訊告知或聲明的紀錄
  - 保留告知的隱私權資訊內容 或隱私權資訊版本等資訊，作為未來解決告知爭議的參考。
- 條款 8.2.6.3 Timing of privacy information 隱私權資訊的時 機及條款 8.2.6.5 Collection from third parties 自第三方蒐集
  - 符合 GDPR 第 14 條 要求，於間接蒐集時告知資料主體隱私權資訊的期限為一個月內。

條款八 運作

- 條款 8.2.7.3 Processing children's information 處理兒童的資訊:
  - 符合 GDPR 第 8 條要求，將組織於處理兒童個人資料時，需額外考量其父母或 監護人的同意要求，除非為提供專業諮詢與預防性服務的情況 例外。
- 條款 8.2.7.5 Open data 開放資料
  - 開放資料的運用上，要求組織應建立去識別化機制，使資料無從識別其資料主體，除非有公開個人資料的基礎或法律要求。
- 條款 8.2.10.1Retention schedules 保留時程
  - 符合 GDPR 第 5 條第 1 項第 e 款要求，組織如 因公共利益、學術研究等目的，需將個人資料轉為給長時間保存， 則應採取適當的技術上和組織上措施，維護自然人的權利和自由。

條款八 運作

- 條款8.2.11.3 Storage and handling 儲存與處理
  - 雲端儲存空間及個人自備裝置(BYOD)等議題納入控管要求。
- 條款8.2.11.5Access controls存取控制
  - 使用者存取 個人資料監督機制，納入組織應實施的控管要求範圍。
- 條款8.2.11.7Managing security breaches管理安全事件
  - 符合 GDPR 第 33 條要求， 於發生安全事件時，組織應於 72 小時內通報主管機關，並依 照 GDPR 第 34 條要求，於發生安全事件時，組織應沒有延遲 下通知資料主體;同時，標準並明訂通報主管機關及通知資料 主體的內容。

條款八 運作

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。
公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

- 條款8.2.11.8Transfer of personal information outside the border 個人資料移轉到國境外地區
  - 以傳輸之所在地國家是否已有適當安全評估、國家(主管機關)是否已對所在地國現行法律法規健全情形予以評估、合約保護，以及專責人員適當評估等作為控制要求的考量。
- 條款8.2.12.1Responding to rights 回應其權利
  - 符合 GDPR 第 12 條要求，當資料主體提出權利行使時，需於一個月內回應，必要時得以延長一個月，此條款要求類似我國個人資料保護法第13條要求。

條款八 運作

- 條款8.2.12.2Access to information 個人資料使用權
  - 資料主體對其使用權行使查詢 內容種類明文列出，包含:處理目的、類別、資訊揭露的接收 者，尤其接收者為第三國或國際組織(利用的對象)、個人資 料被儲存的期間或準則、有權要求更正或刪除個人資料，限制 處理關於該自然人的個人資料、存在向主管機關提出申訴的權 利、間接蒐集時個人資料的來源、在自動化決策含剖析，和涉 及邏輯上有意義的資訊，該處理對自然人的意義和後果，以及 將個人資料轉移到第三國或國際組織時的防護措施等資訊。

條款八 運作

- 資料主體依據條款 8.2.12.4 Erasure 刪 除 權 、 8.2.12.5 Restriction of processing 限制處理權、8.2.12.6 Data portability 個人資料可攜權、8.2.12.7 Objection 反對權， 以及 8.2.12.8 Automated decision-making, including profiling 自動化決策，包括剖析等權利時，適用的前提與要 求，以符合 GDPR 第 17 條、第 18 條、第 20 條至第 22 條要 求。

Check 檢查

條款九成效評估

- 條款 9.1 Monitoring, measurement, analysis and evaluation 監督、量測、分析及評估
  - 要求組織除應文件化個人資訊管理系統績效量測紀錄外，並規劃量測的頻率、時間、評估量測的方法、執行量測的人員，以及所需的資源等。
- 條款 9.3 Management review 管理審查
  - 要求組織於管理審查時需額外討論內部外部議題的變動，以及對個人資訊管理系統績效之回饋與趨勢分析。

Act 行動

條款十持續改善

- 仍保留 10.2 Preventive actions 預防措施，作為處理潛在不 符合事項的因應措施。

Q/A