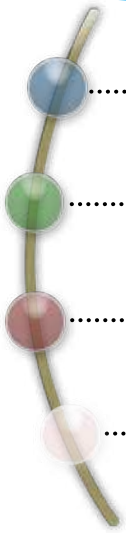
# 中興大學

## 電子郵件社交工程防護宣導教育訓練課程

Davies Wang
2014.5

## 課程大綱



- 2014資安管理新挑戰
- 常見的網路犯罪活動
- 安全防護實務
- 問題與討論

# 2014資安管理新挑戰

# 2014年資安管理新挑戰

| 來源 | 過去情形 | 現階段挑戰 |
|---|---|---|
| 惡意駭客 | 資訊系統破壞或入侵知識僅由少數駭客掌握，相關技術具有進入門檻 | 攻擊工具垂手可得，人人都可是駭客，24小時進行主動、無時差攻擊 |
| 民眾 | 僅注重服務的效率與品質 | 開始具備個人資料保護與資訊安全意識，並重視個人資料安全 |
| 媒體 | 未關注個資保護議題 | 媒體爆料文化盛行，監督企業或政府機關的資訊保護作為 |
| 法律規範 | 電腦處理個人資料保護法(84年公布) | 「個資法」2012.10 上路 |

## 可能面臨的資訊安全事件

* 內部人員不當存網路
* 電腦病毒
* 攜帶型電腦偷竊
* 內部人員未經授權存取資
* 被阻斷提供服務
* 入侵
* 資訊竊取
* 破壞資料及網路
* 通訊詐欺
* 財物詐欺
* 無線竊聽
* 有線竊聽

## 常見的網路犯罪活動

# 電腦犯罪

| 惡意碼<br>( malicious code ) | 簡述特徵 |
|---|---|
| 特洛伊木馬<br>( Trojan Horses ) | 常會以很有用的程式碼如電腦遊戲、計算器、文書處理器等，加上一有破壞性的程式片段，然後以頗具吸引力的檔名，放在公共軟體區，當不知情的人使用之後，便會把電腦中的資料刪除掉造成損害。 |
| 蠕蟲<br>(Worms) | 是一種可以透過電腦網路四處傳播，更可在不同的機器上執行的程式，一般它利用網路之郵遞服務，遠端執行或遠端登陸的能力做為傳播之基本工具。 |
| 後門<br>(Back doors) | 所謂後門程式，即程式設計師，爲節省系統發展時間或做快速除錯工作，常寫一段程式，可以跳過安全作業驗證之作業。當系統發展完畢後，因未將系統之程式片段刪除，使的以後有人可以使用此段程式，入侵電腦系統，妨礙電腦作業之安全。 |
| 邏輯炸彈<br>(Logic Bombs) | 邏輯炸彈是指系統發展人員，故意在所發展之系統中，暗藏一小段程式碼，此程式碼會尋找時機發作，破壞檔案、更改資料內容，使系統當機或其他的破壞性工作。 |
| 電腦病毒(Viruses) | 電腦病毒是一種程式，由有心人發展出來的。他的行為就如同細菌般，會不斷的複製自己，並且依附在其他正常程式之間隨著擴散出去。 |



# 犯罪趨勢

■電腦[網路]犯罪分類法

| 電腦犯罪類型 | 犯罪方法 |
|---|---|
| 非法使用型 | Unauthorized use of computer-related assets , resources, user right , privilege or priority. |
| 詐欺型 | Introduction of fraudulent records or data , software or hardware into a computer system. |
| 破壞型 | Manipulation, modification, alteration or destruction of information or file, software or hardware. |
| 竊取型 | Theft, by electronic means , person or otherwise, of money, financial instruments, property, services, data, software or hardware. |

盜用LINE拐代墊詐財

主管帳號遭駭 發訊30同事2受害

林金聖、林志青・報導 LINE淪為詐騙工具！北市1名男子接獲主管LINE的請託訊息，幫忙代墊3500元收下網購的衣服，他代墊收貨之後，詢問主管才知被騙，他昨查詢發現同單位近30名同事都收過此訊息，包括他共2人受害，近日將報案。

刑事局指出，LINE在台用戶數逾1600萬，詐騙集團疑利用木馬程式等病毒，入侵電腦竊取LINE網路版的帳號密碼，再假冒親友身分行騙，據165反詐騙專線統計，近半月來共3件LINE詐騙諮詢案，其中1人被騙，尚不包含蔡男及其同事的詐騙案，提醒民眾收到代付貨款簡訊，應打電話求證。

◀被害民眾收到主管遭盜用的帳號傳訊，誆稱「先幫我墊付」。



## LINE詐騙訊息 你不能相信的10句話-1

- 這是你那晚沒來的照片，我被整慘了…
- 這是上次聚會照片，你好好笑喔！
- 我在墾丁拍的照片，你覺得哪張最好看。
- 這是我畢業旅行的照片，都在相簿。
- 這是那天我們遊玩的照片，都在相簿。
- 我們中秋烤肉的照片，好好玩喔。
- 看著這些照片，好懷念以前的日子喔。
- 我是你之前的朋友，想知道我是誰，請看網址。
- 好久不見，還記得我嗎？

# LINE詐騙訊息 你不能相信的10句話-2

* 受害者超過六成是大學以上學歷；其中一成是碩士，比國、中小學歷的受害者加起來還高。辦案人員說，學歷高者使用智慧型手機比率很高，「依賴網路越重，越容易被騙！」除了軍公教人員被騙，從事資訊科技人員也有四十多人上當，可見這種利用「人性」的騙術很高招。
* 警方說，目前能植入木馬程式的都是Android作業系統；電信小額付款雖定有上限，但沒限定一天使用幾次，有被害人一天損失三萬元，提醒民眾注意。

# 安卓用戶千萬別點 「您的快遞簽收通知單」是病毒！

* 重要資訊！最近手機詐騙盛行，許多人因為誤點連結損失大把鈔票。一名使用安卓(Android)系統手機的雲友向《ETtoday東森新聞雲》反映，最近收到一則詐騙訊息，上面寫著「**您的快遞簽收通知單，收件電子憑證 http://goo.gl/OOOO**」，如果亂點，訊息就會引導使用者下載並安裝病毒程式，請大家謹慎以對！


參考來源：網路新聞

# 無線網路安全

## Wi-Fi未加密遭偷用盜刷

### 鄰居犯案 女遭連累喊「倒楣」

**地方中心・報導** 「人在家中坐，禍從天上來！」新竹一名林姓女子接到警方傳喚，指其涉及網路盜刷信用卡案件，並查扣林女住處的網路設備，最後才發現因女子住處的無線網路（Wi-Fi）未鎖密碼，遭人盜用。林女在真相大白後大呼：「我真的有夠倒楣！」

新竹警方昨根據歹徒盜刷信用卡所購買的網費電話卡資料，拘提一名37歲門姓男子到案，門男坦承盜用鄰居林姓女子Wi-Fi，登錄網站後，持竊來的他人信用卡資料購買遊戲儲值點數和網費電話卡。警方已調查清查門男所涉盜刷案件數。

刑事局科技犯罪防制中心主任施所培提醒，有使用網路購物的民眾，電腦最好要定時進行掃毒，也不要下載不明檔案或點選不明網址，以避免被植入木馬程式盜取資料；另外家中Wi-Fi的權限也應加設密碼。

**防信用卡遭盜刷注意事項**

- 信用卡刷卡結帳時，應不離視線
- 保存簽單仔細與帳單核對日期、明細表，發現問題及時向銀行反映
- 刷卡完畢檢查卡片及卡號、簽名
- 刷卡後放皮夾，避免放口袋而遺落
- 疑卡不見，請銀行先凍結刷卡，若在限定時間內找回，再啟電解除

資料來源：本報資料室

資料來源：網路新聞

---

電子報 【駭客遙控電腦 偷拍正妹洗澡】

各位姐姐妹妹注意，最近偷拍猖獗，要小心自己成為不雅照的影中人！根據英國《每日郵報》報導，英國有利用遙控管理工具（remote administration tool，簡稱RAT）的「鼠輩駭客」，他們入侵受害者筆電，然後擅自打開電腦內置鏡頭，監察你的一舉一動甚至錄影，讓你的隱私全無。

http://www.chinatimes.com/realtimenews/%E9%A7%AD%E5%AE%A2%E9%81%99%E6%8E%A7%E9%9B%BB%E8%85%A6-%E5%81%B7%E6%8B%8D%E6%AD%A3%E5%A6%B9%E6%B4%97%E6%BE%A1-20130621002476-260401

資料來源：網路新聞

# 網路訟棍PO文「釣魚」連告50人 鄉民付兩萬和解才脫身

社會中心／綜合報導
上網打嘴砲也能賺大錢？台大批踢踢實業坊近日出現一批「網路訟棍」，專門在公開討論區出言挑釁「引戰」，若網友「上勾」回罵即會挨告，目前已知有50多位鄉民為此搭入官司，有人支付了兩萬多元和解金才脫身，「不過是推文『56不能亡』也挨告……」，但法律規定就是如此，網友也只能斟酌用字，三思而後PO文自保。
「請各位小心特定ID的釣魚文！」時任台大批踢踢(PTT)八卦板板主的「四叉貓」XXXXGAY(我老公是張孝全！)上月26日發文公告，呼籲網友推文時千萬要小心，不要掉入「訟棍陷阱」之中，「我本月也被告了，昨天早上去警察局做了筆錄」，引發眾人熱烈討論。
網友細心找出挨告的文章，發現有人似以多重帳號，在PTT多個板面發表偏激的「戰文」，只要下面推文出現稍微過當言論，發文者就馬上興奮地說：「我已備份囉，大家法院見！」有網友不過說了句「你算哪根蔥？」「臭客」也被告公然侮辱，十分無言。
據稱，提告人為了增加網友的困擾，還會憑IP位址選他地報案，讓住在高雄的人要跑到台北做筆錄、台北人要跑到高雄來回奔波，有人不堪其擾，選擇隱忍和解，為了幾個字就賠了2萬多元，「提告如此容易，告訴人至少幺到一次你大老遠做筆錄的機會，這難道不是法律的瑕疵嗎?」

專業律師表示：
不管是不是因為對方挑釁，只要出言在網路上公開罵人，公然侮辱罪就會成立，但成案不代表告得成，過去法院就曾判過如「天龍人」、「瘋子」、「他媽的」，屬意見評論或俚語，不構成公然侮辱判被告無罪。


資料來源：Ettoday

# 組織型駭客攻擊手法-APT

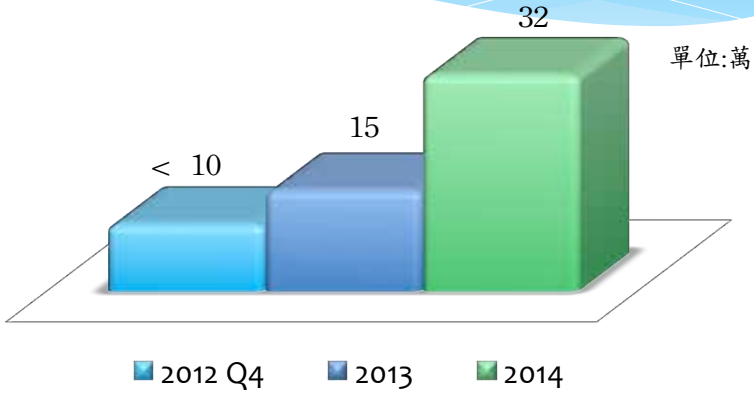
* 進階持續性威脅Advanced Persistent Threats
  * Advanced：採用進階而高深的攻擊手法
  * Persistent：持續有計畫地攻擊特定目標
* 特徵
  * 特定目標
  * 低調、隱匿、手法多變、客製化
* 目的
  * 竊取資訊
  * 政治因素
  * 金錢利益

# 小心！史上最狠毒勒索軟體肆虐臺灣


* 勒索軟體CryptoLocker大舉入侵臺灣，公司與個人陸續傳出災情，該軟體會將受害者電腦加密，導致檔案無法使用，更限期3天支付9,000元贖金，否則將毀損解密金鑰。近日，有一支名為CryptoLocker的勒索軟體（Ransomware）現蹤臺灣，企業陸續傳出受害災情，該軟體透過釣魚郵件入侵，會將受害者電腦的檔案全數加密，導致檔案無法存取，而且駭客採用高超的加密技術，讓受害者無法自行復原，並限期3天支付9,000元贖金，否則將毀損解密金鑰，受害者苦不堪言。

資料來源：ITHOME

# 勒索軟體倍數成長




資料來源:資安工具廠商

**Spear Phishing**

Send an email to a person of interest

**Watering Hole Attack**

Infect a website and lie in wait for them

* Targeted Attacks predominantly start as spear phishing attacks
* In 2012~2013, Watering Hole Attacks emerged
  * Popularized by the Elderwood Gang

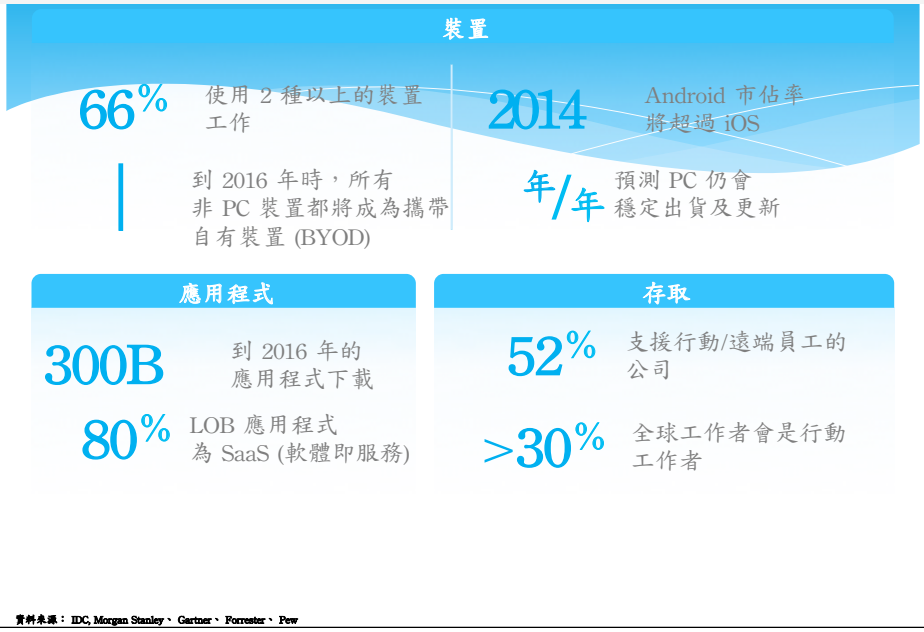
# 水坑式(Watering Hole)攻擊

* 攻擊者分析攻擊目標經常瀏覽之網站
* 攻擊者分析網站弱點，將惡意程式放置其中
* 最終某些攻擊目標的使用者因為瀏覽該網站而遭到入侵

# BYOD的趨勢與風險

* 自帶設備上班 (Bring Your Own Device, BYOD)
  * Forrester：76%組織允許自帶設備，有一半受訪企業都承認，曾經因為自帶設備而遺失資料
* 自帶設備的風險
  * 封閉的iOS並不代表安全
  * 超過80%的Android設備使用的是舊版本OS。意味著它上面的漏洞可能不會被修復，新的安全功能也可能無法使用
  * 惡意程式的泛濫
    * 偽裝的熱門遊戲
    * 偽冒知名開發商

# 技術變更的步伐和發展速度日新月異




資料來源：IDC, Morgan Stanley、Gartner、Forrester、Pew

# 惡意APP


惡意 APP 化身防毒 APP，一下載安裝後，手機就無法運作，得付129美金贖金，才能恢復正常。

# 惡意APP已突破百萬

# 行動裝置惡意程式分類

* 短信木馬
* 廣告模組
* 獲取智慧手機root許可權的漏洞利用程式
* 惡意扣費
* 遠程控制
* 隱私竊取
* 惡意傳播
* 電話費暴增


病毒可以透過系統漏洞去取得ROOT權限並執行任意的程序而後利用以下三類行為獲取利益(續前頁)

✧ 竊取手機訊息
✧ 發送付費簡訊
✧ 竊取帳號密碼

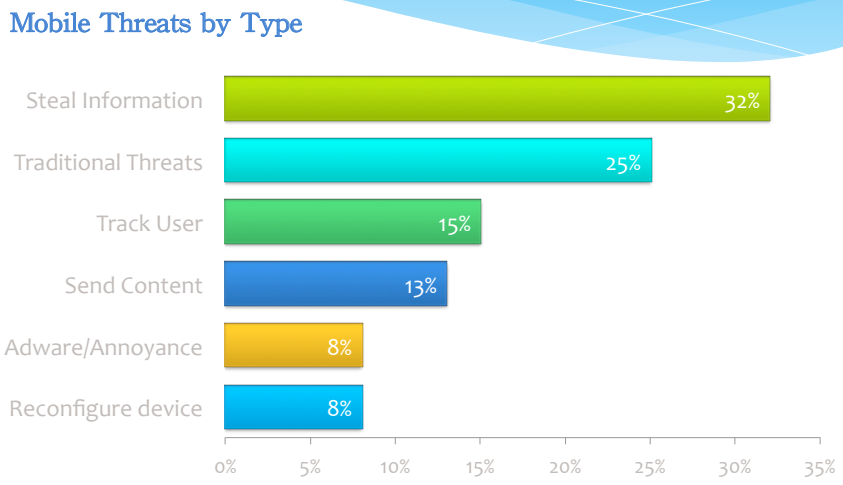
# Vulnerabilities & Mobile Malware

| Platform | Vulnerabilities |
|---|---|
| Apple iOS | 387 |
| Android | 13 |
| Blackberry | 13 |
| Windows Mobile | 2 |

| Device Type | # of Threats |
|---|---|
| Apple iOS Malware | 1 |
| Android Malware | 103 |
| Symbian Malware | 3 |
| Windows Malware | 1 |

* Today there is no significant link between mobile OS vulnerabilities and exploitation by malware
* In the future that may change

# What Does Mobile Malware Do?



# 容易暴露隱私的地雷

資安工具廠商，針對台灣人使用率最高的社群平台臉書（Facebook）做的調查，容易暴露隱私的地雷包括，

1. 臉書設定大「公開」。儘管有高達77% 的使用者擔心自己的資料（如個資、照片等）會被公開，但也有37% 的使用者設定隱私權為「公開」。

2. 是高達61%的臉書使用者不會主動定期檢查隱私權設定，甚至有1/4的使用者不知道可以調整隱私權設定。

3. 為「用生日做懶人密碼」，趨勢科技調查出有58%使用者會在臉書公布自己的生日在臉書上，也有40%的使用者使用自己的生日當作密碼，易被有心人士盜用。

4.是「使用臉書不設防」。目前臉書台灣活躍使用者超過1400萬人，但31%的臉書使用者曾被盜用過臉書帳密，還有66%曾莫名加入網路社團或詐騙社團，顯示臉書平台已成為駭客及詐騙集團的目標平台之一，但有防護的人並不多。

5.個風險是30%臉書使用者會「接受」自己好友的朋友加入至好友名單中，但這有來自廣告社群或是詐騙社群的邀請，在按下接受鈕前要三思。

6.遺失手機，造成裝置中個人隱私資料如私密照片等曝光外洩。

資料來源：趨勢科技

# 2014年十大安全威脅預測

* 進階持續性威脅攻擊(APT, Advance Persistent Threat)。
* 行動裝置的資料保護。
* 來自內部的威脅。
* 透過瀏覽器的攻擊持續增加。
* 社群網站引起的安全及隱私問題。
* 檔案安全日趨重要。
* 資料安全走入雲端。
* 駭客越來越猖獗。
* 資安變成商業營運必備要素。
* 資料安全與隱私條例在全球有逐漸被聚合的趨勢。

參考來源：資安人網站

# 安全防護實務

# 釣魚網站防護


資料來源：趨勢科技

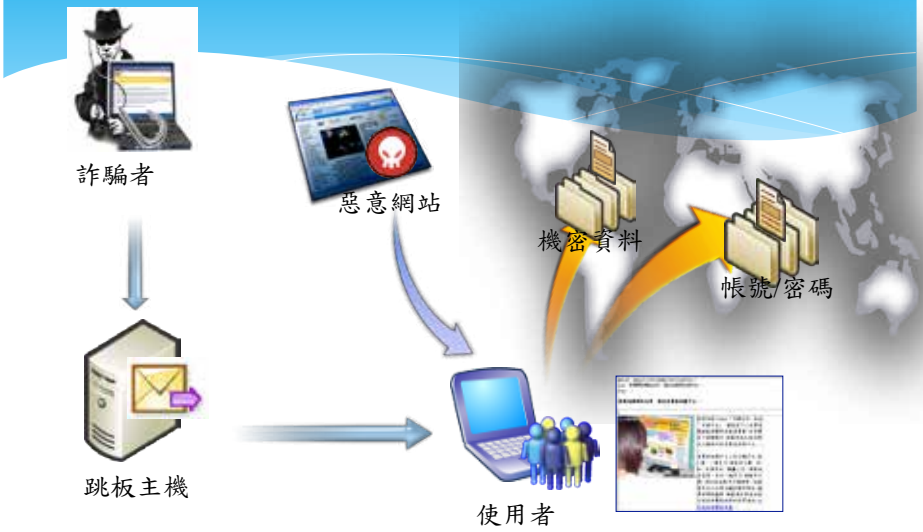

chrome
危險：發現惡意軟體！
Google Chrome 封鎖了這個網頁 (位於 67.159.2.18) 的存取權。
這個網頁已經置入知名惡意軟體散佈者 nicosurvey.net 的內容，現在瀏覽該網頁極可能使您的電腦受到惡意軟體損壞。
惡意軟體可能竊取個人資訊，造成財務損失及永久刪除檔案。
返回


加密政策
密碼強度原則性
五分鐘後自動鎖定
密碼輸入錯誤次數超過自動還原預設

# 更換密碼


# 管理實務：
# 電子郵件管控實務建議

# 電子郵件社交工程手法




# 同仁對於可疑電子郵件應有警覺性

* 為何我會收到這封郵件?
  * 應確認寄件來源及寄件者
* 我是否應該收到這封郵件?
  * 應確認郵件主旨及郵件內容
* 我是否應該開啟這封郵件?
  * 是否與業務工作相關
  * 不開啟(點選)連結是否有影響
  * 審慎查證(寄件者或資訊單位)

# 判斷網路釣魚郵件方式

- 發信人的名稱或郵件地址
  - 是否有異常？需確認發信者的身分
- 電子郵件的主旨與內容
  - 與本身的工作、業務是否有關連
- 網頁連結或夾帶附件檔案是否可疑
  - 郵件內異常網址連結判斷
    - www.microsoft-mis.com
    - www.hinet1.net , www-hinet.net
    - www.paper-pchome.com , www.pchorne.com
    - 使用不明IP 代替URL（如：http://220.33.444.12/）

# 惡意郵件攻擊

資料來源：法務部全球資訊網

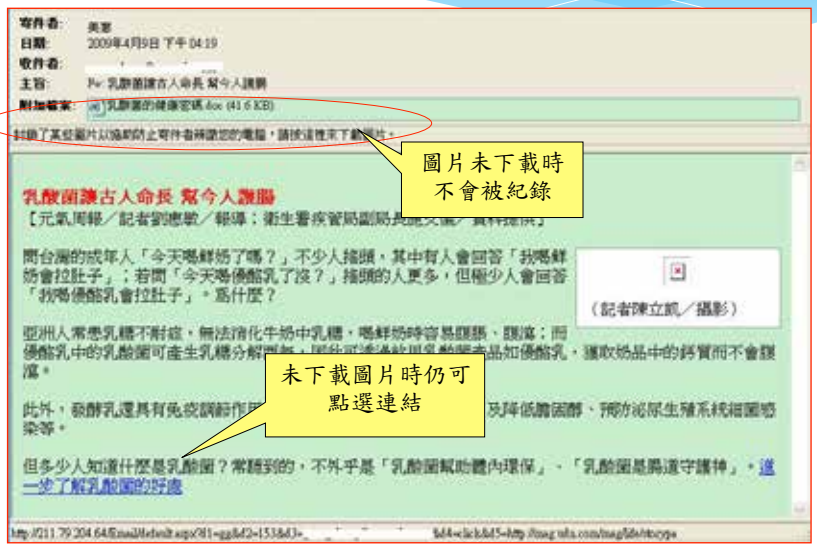
- 好康報、養生保健、休閒娛樂、公務相關、美食、八卦新聞…

# 測試郵件清單

| 郵件 | 郵件種類 | 郵件標題 | 寄件者 |
|---|---|---|---|
| 1 | 趣味遊戲 | Fw:台灣神魔之塔破關第一人 | 婷婷<tintin336@yahoo.com.tw> |
| 2 | 教育 | 李家同：免試入學，窮人孩子出頭不易 | 教改聯誼會 <callcenter@tw.standardchartered.com> |
| 3 | 衛生保健 | Re:多吃B群吧，新聞說國人維生素B群最缺 | 菁菁<annie0908@mail2000.com.tw> |
| 4 | 趣味遊戲 | Fw: LINE 銀河特攻隊，好友招集令 | 蕙玲<linlin@npm.gov.tw> |
| 5 | 情色 | 林嘉綺代言電玩演出，最後一次裸露 | 電玩週報<game@ms66.url.com.tw> |
| 6 | 新聞時事 | 像世界末日般，雪梨沙塵染紅歌劇院圖集 | weather<weather@yam.com> |
| 7 | 旅遊休閒 | 日本旅遊Passport搶手 | 雄貓旅行社<travel_cat@pie.com.tw> |
| 8 | 新聞時事 | 汽車貨物稅減徵3萬最後倒數，腳步加快 | 汽車雜誌<car@ferrari.com> |
| 9 | 網路新知 | 青年安心成家方案，逾5成買前不知道 | 永慶房仲網<customer@sinyi.com.tw> |
| 10 | 八卦 | 連父親都瞞? 林志玲爸爸要當阿公卻不知?! | 阿震<info@log.1-apple.com.tw> |

# 網頁型測試郵件範例

# 釣魚郵件記錄方式




# 防範惡意程式與詐騙

個人資訊勿隨意登錄於不明網站

* E-mail 管理
  - 區分公司及個人使用之信箱
  - 在外登錄註冊之信箱，容易收到許多垃圾郵件，使用時務必小心
  - 不回覆來源不明之郵件
* 定期安檢作業
  - 即時更新軟體修補程式
  - 即時更新防毒軟體及病毒碼
  - 經常對系統進行檢測
* 實體隔離
  - 機敏資料應於實體隔離主機上作業

## 防範惡意電子郵件使用者防護

* 停－使用任何電子郵件軟體前，須先確認以下設定
  * 是否已安裝防毒軟體並確實更新病毒碼
  * 取消郵件預覽功能(outlook express/檢視/版面配置/預覽窗格，不要勾選顯示預覽窗格的設定)
  * 儘量使用純文字模式開啟信件(outlook express/工具/選項/讀取/讀取郵件，☑在純文字中讀取所有郵件)
* 看－收到信件後必須注意
  * 信件主旨是否與本身業務相關
  * 開啟信件前須先確認信件來源，否則建議刪除
* 聽－若懷疑信件來源必須進行確認
  * 透過電話或電子郵件向寄件人確認信件真偽

## 改善個人習慣

- 不要瀏覽非工作相關或不信任的網站
- 不要下載安裝未經認可的軟體或程式
- 隨時更新作業系統與應用程式
- 安裝必要的防護軟體
- 不要開啟可疑或非工作相關的信件附檔
- 對任何提到”緊急”或”個人金融”保持懷疑態度
- 對信件有任何一點疑慮千萬不要點選Email裡的超連結
- 不要填寫Email裡有關個人金融資料的表格
- 在網站上輸入信用卡號或個人資料時先確認該網站安全性

## 改善個人習慣(續)

- 不將Email留在任何公開的網頁上
- 不開啟來歷不明之信件
- 不轉寄非必要之信件
- 不回應任何未知的信件
- 安裝防止網路釣魚詐騙的工具軟體
- 經常或定期登入你的網路帳號
- 定期確認你的銀行帳戶、信用卡的交易狀態都正確無異常
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式
- 自助互助，告知相關單位你發現的網路釣魚事件

## 結論

- 預防重於治療
- 隨時注意更新
- 正確的觀念

# Q&A 問題與討論

**聯絡資訊**

王吉祥(Davies) 講師暨資深經理
+886 970 350 128
dvings@gmail.com