資通安全及基本防護觀念宣導

財團法人中華民國國家資訊基本建設產業發展協進會

簡報大綱

- 資通安全簡介
  - 資通安全管理法規暨標準
  - 資通安全概念
- 資通安全基本防護觀念
  - 個人電腦防護
  - 帳號密碼管理
  - 社交軟體/資安事件議題
  - 資通安全案例分享
  - 問題與討論

資通安全簡介

資通安全相關法規

- 資通安全管理法 (107年06月06日公布)
- 資通安全管理法施行細則 (107年11月21日公布)
- 資通安全責任等級分級辦法 (108年08月26日公布)
- 資通安全事件通報及應變辦法 (107年11月21日公布)
- 特定非公務機關資通安全維護計畫實施情形稽核辦法 (107年11月21日公布)
- 資通安全情資分享辦法 (107年11月21日公布)
- 公務機關所屬人員資通安全事項獎懲辦法 (107年11月21日公布)

資通安全相關標準

- CNS 27001「資訊技術-安全技術-資訊安全管理系統 - 要求事項」(103年04月24日)
- ISO 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirement (102年10月)

重要名詞定義

- 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
- 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。
- 資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
- 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

資訊安全管理制度

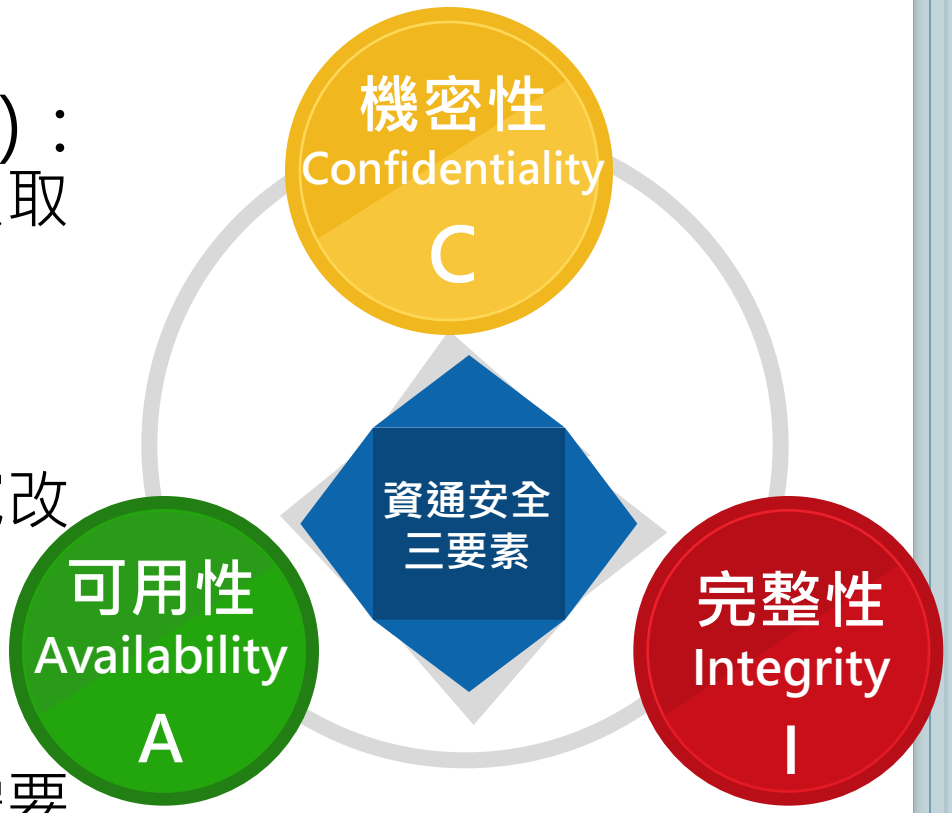
- **資訊安全管理制度 (Information Security Management System, ISMS)**

  整體管理系統的一部份，以營運風險方案為基礎，用以建立、實施、操作、監督、審查、維持及改進資訊安全。

資料來源：CNS 27001

資通安全三要素

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。



目的在於保護資訊資產的機密性、可用性與完整性。

資通安全的範圍

- 資訊使用之『環境』
- 資訊使用之『技術』
- 資訊使用之『制度』
- 資訊使用之『人員』

資通安全簡介(木桶理論)

- 企業管理中有一個被熟知的 "木桶理論"，指的是企業能力的整體水平取決於企業各項具體能力中最弱的一項。
- 資通安全中有的 "木桶理論"，指的是組織內整體資訊安全防範能力，取決於組織中最弱的一項。
- 就像一隻木桶，裝水的容量最多只能達到所有擋板中最短的擋板的高度。

資通安全簡介(續)

在資訊安全裡，我們說：

Security is a chain.

It's only as secure as the weakest link

（系統安全程度＝最弱環節）

資通安全基本防護觀念

個人電腦防護觀念(1)

- 個人重要文件檔案應勤勞定期做備份
- 隨時更新修補程式(如 Windows、Office、Flash、Adobe 等)
- 複雜密碼原則
- 定期更換密碼
- 使用正版軟體、不安裝來路不明軟體
- 安裝防毒軟體並更新病毒碼定期掃毒

個人電腦防護觀念(2)

- 開啟及使用防火牆控管
- 即時通訊軟體傳來的連結要先跟發訊者確認，不要隨便點擊
- 登入任何網站時請先確認網址是否正確，以免遭釣魚網站詐騙
- 勿隨意點擊廣告網頁及上來路不明網站
- 檔案下載後先掃毒
- 正確使用隨身碟，如使用前先掃毒、以檔案總管模式開啟、關閉 autorun 功能等

猜猜看

- Line網站
  - http://line.me/zh-hant
  - http://line.pm/zh-hant/

猜猜看

猜猜看

猜猜看

- Line網站
  - http://line.me/zh-hant真正的 **LINE** 官方網站
  - http://line.pm/zh-hant/假的 **LINE** 釣魚網站 （千萬不要按、不要輸入帳號密碼）

假的~~

[redacted]
已傳送郵件: 2018年8 月29日, 星期三 上午 7:11:26
主旨: 20-GB

HiNet網頁郵件

尊敬的用戶，

感謝您長久以來對HiNet電子郵件服務 的支持，為了提供您更好的服務品質

點擊後會導入釣魚頁面，騙取帳號密碼

「點擊這裡 加大HiNet 郵件信箱儲存空間儲存空間至20GB」

郵件系統升級後，將可提供您加大(至20GB)的信箱空間以及更便利的垃圾信件防護功能。

祝您 身體健康 萬事如意

中華電信數據通信分公司 敬上
客服專線：0800-080-412

蘋果用戶小心！網路釣魚最愛仿冒蘋果，攻擊比率從 2% 衝到 10%

- Check Point 發現，擁有高品牌認知度的蘋果（Apple）在 2019 年第 4 季占全球所有品牌網路釣魚攻擊比率 2%、名列第 7，但今年第 1 季飆升至榜首，占比也提高至 10%；在武漢肺炎（2019 冠狀病毒疾病，COVID-19）疫情期間訂閱人數激增的 Netflix 以 9% 占比位居第 2。
- 網路釣魚攻擊中最常遭仿冒的品牌第 3 名至第 10 名依序為 Yahoo、WhatsApp、PayPal、美國大通銀行、Facebook、微軟、eBay、亞馬遜。
- Check Point 指出，網站釣魚占 2020 年第 1 季所有網路釣魚攻擊的 59%，成為最常被利用於網路釣魚攻擊的平台。行動裝置釣魚從 2019 年第 4 季的第 3 名躍升至第 2 大受攻擊平台，占比 23%，主要原因在於人們在疫情期間花費更多時間查看手機，使網路犯罪者有機可乘

資料來源-科技橘報2020/04/24

個人電腦防護觀念(3)

- 自我檢視是否中毒、被植入後門或木馬程式
  - 電腦變的異常緩慢
  - CPU使用率是否處於高使用率（95%以上）
  - 經常出現記憶體不足的訊息
  - 使用電腦或上網時是否會跳出不明視窗
  - 某些系統程式無法開啟或執行
  - 電腦中是否有不明檔案產生
  - 無法顯示隱藏檔
  - 工作管理員內有不明處理程序在執行
  - 電腦自動寄送廣告信件
  - 啟動時帶起不明程式運作
  - 不明服務被啟動或是系統服務遭停用
  - 防火牆被開啟不明 Port 或無法啟動
  - 防毒軟體不停跳出攔截到病毒訊息
  - 防毒軟體自動關閉或是無法啟動
  - 無法更新病毒碼

個人電腦防護觀念(4)

- 網路是否異常
  - 無法連線
  - 網路正常但是無法瀏覽網頁
  - 網路速度緩慢
  - 未使用網路時是否有持續大量上傳及下載流量
  - 是否有不明連線
  - 無法連到防毒軟體網站或Windows Update網站
  - 連接網頁遭轉址連到非正確網站

帳號密碼管理

帳號密碼

2018常見密碼

2019常見密碼

1:123456 (unchanged)
2:123456789 (up 1)
3:qwerty (up 6)
4:password (down 2)
5:1234567 (up 2)
6:12345678 (down 2)
7:12345 (down 2)
8:iloveyou (up 2)
9:111111 (down 3)
10:123123 (up 7)
11:abc123 (up 4)
12:qwerty123 (up 13)
13:1q2w3e4r (new)
14:admin (down 2)
15:qwertyuiop (new)
16:654321 (up 3)
17:555555 (new)
18:lovely (new)
19:7777777 (new)
20:welcome (down 7)
21:888888 (new)
22:princess (down 11)
23:dragon (new)
24:password1 (unchanged)
25:123qwe (new)

2019網友最常用的密碼

安全業者針對旗下推出一款名為「NordPass」密碼管理器應用程式，就數據庫資料的統計分析，公佈了2019這一年以來，最易被破解為網友最常使用的200組密碼排名榜單。

排名前三名安全性最差，都是採用阿拉伯數字組合的密碼，分別為：第一名的「12345」，統計共有超過281萬筆；第二名的「123456」，統計共有超過248萬筆；第三名的「123456789」，統計共有超過105萬筆。

資料來源：https://nordpass.com/blog/top-worst-passwords-2019/
自由時報2019/12/14

2019網友最常用的密碼-特色

觀察前200名安全性最差的常用密碼排行榜單，之所以很容易被竊取盜用，其共同特色就是**很容易被猜到**，彙整歸納主要有六大重點：

- 使用簡易的阿拉伯數字組合（如：12345、111111、123321、55555、654321、0987654321）
- 使用電腦鍵盤上垂直或水平排列的組合（如：qwerty、asdfghjkl ，qazwsx，1qaz2wsx）
- 使用受歡迎的男性或女性英文名稱（如：Nicole、Jessica、Hannah、charlie、michael）
- 使用體育運動健身相關的英文單字（如：football、baseball、fitness、basketball）
- 使用與食物相關的英文單字（如：chocolate、cookie、cheese、banana）
- 使用耳熟能詳的卡通明星（如：snoopy、hellokitty）

比較特別一提的是，知名科技品牌 Samsung 也被網友拿來作為密碼，此次入榜排名第198名。

資料來源：https://nordpass.com/blog/top-worst-passwords-2019/

常見密碼特色

- 只有數字組成。
- 依照鍵盤順序排列。
- 預設密碼。
- 含有個人資訊(喜好)。
- 英文單字。

建議

- 長度至少??碼。
- 包含英文數字參雜且區分大小寫。
- 包含特殊符號。
- 沒有意義的組成。
- 可以有屬於自己的規則。
- 避免多個系統使用同一組密碼。
- 密碼要記得住。

密碼遭破解的統計數據

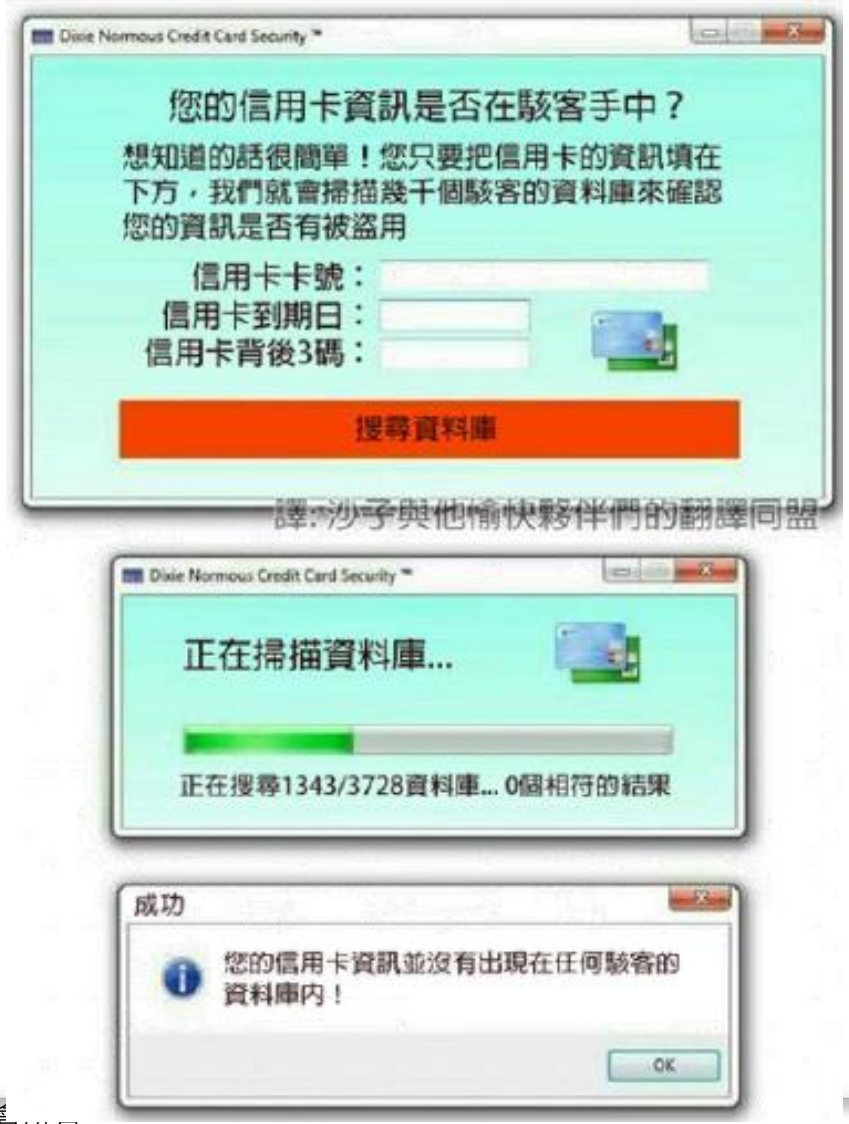
密碼長度	26 英文字母	26 英文字母+10 數字	52大小寫英文字母	96可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

資通系統防護基準控制措施

- 身分驗證管理
  - ✓ 使用預設密碼登入系統時，應於登入後要求立即變更。
  - ✓ 身分驗證相關資訊不以明文傳輸。
  - ✓ 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。
  - ✓ 基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。
  - ✓ 使用者更換密碼時，至少不可以與前三次使用過之密碼相同。
  - ✓ 第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

社交軟體/資安事件議題

【釣魚騙局】黑客盜取信用卡資訊低能新招切勿上當 網民：騙老人家 9 成 9 中！



【釣魚騙局】還在玩遊戲嗎

信用卡遭盜刷的原因,除了網路釣魚外,還有哪些意想不到的原因？

資料來源：https://blog.trendmicro.com.tw/?p=64761

五個意想不到信用卡遭盜刷原因-1

把信用卡交易資料，存在 Chrome、IE、Firefox……瀏覽器裡

- 買 PC HOME、買淘寶、逛 MOMO、上各大平台、網拍買東西，這些應該都是現代人很熟悉的事情，因為貪圖方便，所以把交易資料(像是卡號)，存在你的 Chrome、IE、Firefox……瀏覽器裡，但你有想過你的瀏覽器裡可能已經被裝入惡意的插件或程式，非法獲取你的交易資訊嗎？
- 現在**很多竊取你信用卡資料的方式，是透過瀏覽器的插件進行盜用的**，你可能完全沒發現你的瀏覽器插件裡暗藏這些惡意軟體，或者被一些釣魚網站拿到你的卡號

資料來源：https://blog.trendmicro.com.tw/?p=64761

前三名線上購物高風險賣場-1

資料來源：https://165.npa.gov.tw/#/article/news/235

前三名線上購物高風險賣場-2

知名購物網「MOMO」驚傳疑似會員個資外洩，**詐騙集團按圖索驥打電話給消費者，冒充網站客服行騙**，刑事警察局165反詐騙諮詢專線從今年2月起陸續接獲民眾通報，表示在「MOMO購物網」消費後遭遇詐騙，累計至6月21日止，被騙人數已達192人，財損金額達新臺幣2,824萬餘元。另分析是類**「解除分期付款」詐騙手法，交付管道以「網路轉帳」占最多(41.53%)、ATM轉帳次之(35.79%)**，民眾依歹徒指示操作**操作網路銀行(APP)或ATM**時，通常於受騙當下都不知道正在把錢轉給歹徒。

資料來源：https://165.npa.gov.tw/#/article/news/235

五個意想不到信用卡遭盜刷原因-2

看個熱門新聞列表推薦,不疑有詐的點入詐騙網站

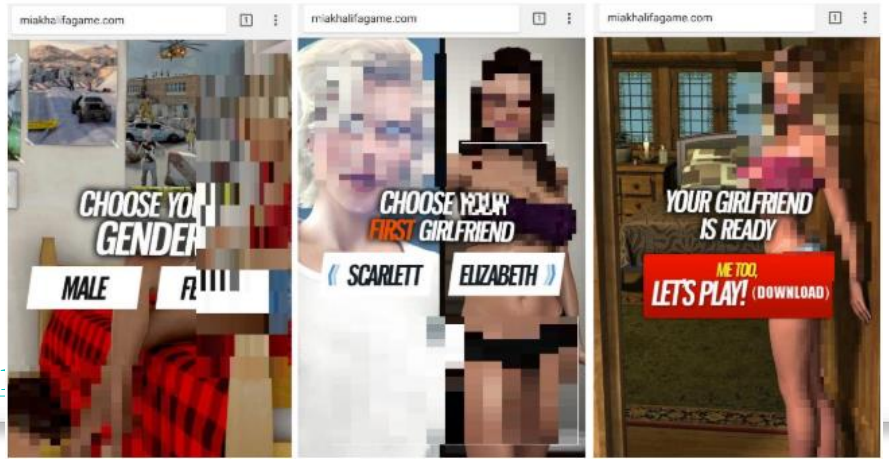
- 詐騙集團在入口網站刊登的廣告,可能夾雜在熱門新聞的列表中,一般人不容易分辨, 這類詐騙也會**藉由假過卡方式進行詐騙,也就是假裝該購物網頁可以刷卡，然後之後客服聯絡你刷卡失敗改貨到付款**？
- 這些強調超低價、免運費等各種誇大優惠的一頁式詐騙廣告,不僅在 Facebook 刊登廣告,也在各入口網站刊登廣告,網友很容易掉入陷阱,在詐騙集團建立的假網頁上買了東西，除了收到的東西可能跟下單的商品完全不一樣外，也可能讓詐騙集團掌握你購物時輸入的個資

資料來源：https://blog.trendmicro.com.tw/?p=64761

五個意想不到信用卡遭盜刷原因-3

下載 app，可能也會出事

- 一時好奇下載免費成人遊戲,卻遭「虛擬女友」刷爆信用卡還偷錄音!提醒您,下載手機 app 時,當心遇到間諜軟體。
- 有一個會竊取個資的多平台間諜軟體: Maikspy,偽裝成人遊戲: Virtual Girlfriend（虛擬女友）,當使用者進行註冊時，駭客不僅可以取得受害者的信用卡資料，還會取得註冊該網站時的刷卡費用。
- 偽裝正常的銀行應用程式，將自己的網頁覆蓋在正常的銀行應用程式操作介面上，進而騙取使用者的帳號密碼。此外，BankBot 還能攔截手機簡訊，因此不怕使用者啟用手機簡訊雙重認證。



資料來源：https://blog.trendmicro.com.tw/?p=6476

五個意想不到信用卡遭盜刷原因-4

刷卡消費時,對著結帳螢幕的攝影機,可能全都露

- 商店和金融機構內的攝影機也被駭客用來取得個人身份資料和付款資訊。地下論壇有人出售可以收集信用卡資料的網路攝影機影像串流(如下圖),也有人表示願付出每秒15美元來觀看被駭攝影機
- 一篇地下論壇文章出現了多達 2,000 台據說連到咖啡館、醫院、辦公室、倉庫和其他地點的IP攝影機。而另一個網站上的群組成員可以分享和觀看網路攝影機影像並進行惡作劇。
- 這些被駭的網路攝影機經常都是用預設密碼或是無需身份認證的影像串流，因此並不需要特殊知識或高級駭客技能,就能入侵這些網路攝影機。

資料來源：https://blog.trendmicro.com.tw/?p=64761

五個意想不到信用卡遭盜刷原因-5

知名網站未必安全,你輸入信用卡個資,駭客默默側錄

- 去年發生一連串針對連鎖旅館的訂房網站的Magecart信用卡側錄攻擊, 該病毒會用假網頁替換原始訂房網頁。
- 該側錄器可能經由地下論壇取得, 用以收集線上訂房者的姓名、電子郵件地址、電話號碼、旅館房間偏好和信用卡詳細資訊。側錄器會檢查客戶使用哪種語言進入網站，並注入相對應的偽造信用卡表單。

例如：知名飾品Claire's官網遭植入信用卡側錄程式

資料來源：https://blog.trendmicro.com.tw/?p=64761

該如何自保呢

- 再三確認網購網站上的 URL 是否為官方網址。
- 固定檢查信用卡刷卡的紀錄是否異常。
- 確實保管好卡片，背面3碼驗證碼不外流。
- 不要讓瀏覽器儲存登入帳號、密碼或信用卡等資料
- 請發卡銀行在刷卡時發送提醒簡訊或email。

*注意:已有惡意程式會攔截刷卡簡訊

- 別下載到假冒的熱門 app, 免得被植入惡意程式側錄或攔截刷卡簡訊通知。
- 在實體店面刷卡時,不要讓信用卡離開自己的視線。

*前述網路攝影機遭駭的案例不適用,消費時盡量找重視資安的廠商

- 安裝防毒軟體，並維持在最新版本的狀態。

資料來源：https://blog.trendmicro.com.tw/?p=64761

資通安全案例分享

資通安全的威脅來源與動機

無意 Unintentional

操作缺失

設計缺失

認知不足

自然現象

故意 Intentional

資料來源：https://nordpass.com/blog/top-worst-passwords-2019/
自由時報2019/12/14

台灣宅配通不會使用「台湾鹈鹕快递」發送相關郵件及簡訊

pelican 宅配通

尊敬的客户，
这可以通知您您的包裹已到达我们的办公室。
由于发件人填写的地址不正确，我们的快递员无法递送包裹。
要接收您的包裹，请访问我们的任何办公室并出示所附文件。
标签编号：PE-Pelican-8263832
预计交付日期：2020年4月30日，星期四
类别：包裹服务

真诚的
Zhang Wei Chen
南码头15号 桃园大公园337
台湾
宅配通消費者服務專線 (02)6618-1818
簡訊查件專線 0977-777-192

近期台灣宅配通公司發現，詐騙集團利用公司統編及客服專線，以「鵜鶘快遞快車」及「delivery.notice@e-can.com.tw 」郵件，亂槍打鳥發送郵件，請提高警覺，勿回復該郵件

資料來源： https://165.npa.gov.tw/#/article/rumor/732020/5/05

北韓駭客將木馬程式藏於MACOS雙因素認證程式中

資安業者Malwarebytes近日發現，北韓駭客集團Lazarus Group (又稱Hidden Cobra與APT 38)改變原本僅鎖定Windows與Linux作業系統之Dacls遠端存取木馬程式(Remote Access Trojan, RAT)，轉而瞄準macOS用戶，透過感染合法支援macOS之雙因素認證應用程式MinaOTP進行散布，將Dacls植入於使用macOS作業系統之電腦，而該應用程式主要使用者為中文人士。

Dacls最早於去年底由資安業者奇虎360之網路安全研究實驗室(Qihoo 360 NetLab)發現，當時實驗室專家即認為Dacls係由Lazarus Group所開發，並指出Dacls為模組化之遠端木馬程式。Windows作業系統版Dacls可自遠端動態載入模組，而Linux作業系統版Dacls則是直接將模組內建於程式中。

依據Malwarebytes分析，當macOS用戶執行MinaOTP後，會透過開機排程程式LaunchDaemons或LaunchAgents建立一個屬性列表文件(Plist)，指定為開機後須執行之程式，使其可長駐於電腦中，前者以登入之用戶身分執行程式，後者則是以管理員身分執行程式。此外，macOS版Dacls與Linux版Dacls架構相近，主要差別在於Linux版載入6個外掛程式，而macOS版則有7個，新增名為Socks之外掛程式，用於代理惡意程式與命令暨控制伺服器(Command and Control Server, C&C Server)間之網路流量。

資料來源：https://blog.malwarebytes.com/threat-analysis/2020/05/new-mac-variant-of-lazarus-dacls-rat-distributed-via-trojanized-2fa-app/ 2020/5/11

全球衛生機構電子郵件帳密遭外洩

美國專門追蹤網路極端主義與恐怖組織活動之團體「賽德情報集團」(SITE Intelligence Group）指出，全球各大衛生機構員工之公務信箱帳密，遭不明人士於匿名論壇4chan、推特(Twitter)及即時通訊軟體Telegram頻道上公開。

該集團表示，共計約2.5萬筆公務信箱帳密遭洩漏，受駭機構包括世界衛生組織(World Health Organization, WHO)、美國國家衛生研究院(National Institutes of Health, NIH)、美國疾病管制暨預防中心(Centers for Disease Control and Prevention, CDC)、世界銀行(World Bank)等與新型冠狀病毒(COVID-19)防疫相關之機構，其中高達9,938筆外洩資料來自美國國家衛生研究院，其次為美國疾病管制暨預防中心6,857筆、世界銀行5,120筆及世界衛生組織2,732筆帳密遭駭。至於臺灣衛生福利部疾病管制署(以下簡稱疾管署)則有69筆公務信箱帳密遭外洩。

澳洲網路安全專家 Robert Potter推測外洩資料係經由暗網販售流出，並曾嘗試用遭外洩之公務信箱帳密，成功登入世界衛生組織電腦系統，其中48人係以「password」為密碼，亦有使用者以名字作為密碼，顯示該機構人員之密碼安全性十分不足。

疾管署則表示遭外洩公務信箱帳密非屬現有之有效帳號，目前已停用遭外洩之公務信箱，另該批在外流傳之密碼規則多與疾管署制定之密碼規則不符，疑為公務信箱遭人註冊於外部網路服務，而相關服務遭駭客入侵竊取帳密所致，非直接由疾管署系統外洩。

資料來源：https://www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/2020/4/29

舊金山國際機場網站遭駭客掛碼竊取使用者帳密

舊金山國際機場(San Francisco International Airport, SFO)於2020/4/7發布資訊外洩公告(Notice of Data Breach)，證實今年3月隸屬於SFO之兩個網站(SFOConnect.com與SFOConstruction.com)皆遭駭客植入惡意程式碼，以竊取使用者帳號與密碼。

依據公告內容，受攻擊之影響範圍涵蓋經由外部網路(非SFO機場內部網路)使用Windows作業系統內建之IE瀏覽器存取受駭網站的使用者，以及經由內部網路使用非SFO維護設備存取受駭網站之使用者，主要遭竊取資訊為使用者主機設備之帳號與密碼。

SFO已於2020/3/23關閉受駭網站，並移除網站上之惡意程式碼，同時強制重設所有SFO相關人員之電子郵件密碼；另呼籲所有經由外部網路使用Windows作業系統內建之IE瀏覽器存取相關網站的使用者，應立即修改個人設備之登入帳密與其他使用相同帳號與密碼之憑證。

資料來源：https://www.forbes.com/sites/daveywinder/2020/04/11/san-francisco-airport-cyber-attack-confirmed-windows-passwords-stolen/#34f4be2125b9/2020/4/14

以色列選舉系統漏洞導致選民資料外洩

根據以色列新聞媒體「Haaretz」2/9報導，資訊廠商Feed-b幫以色列政黨「聯合黨」(Likud)建置之選舉管理平台Elector，有重大資安漏洞，只要檢視Elector首頁原始碼，就能看到系統管理者帳號與密碼，讓任何人都能藉由管理者權限下載以色列所有選民約645萬人個資。這些選民資料包含姓名、身分證號碼、地址、性別及電話號碼等，Feed-b已在得知消息後馬上修補該漏洞。

以色列規定政黨可在選舉前收集所有登記選民資料，不過須承諾保護選民隱私，不得複製資料或與第三方分享，還要求在選舉結束後須刪除所有資料。聯合黨把選民資料上傳到用來管理選舉活動的Elector系統上，該系統可用來發布或更新選舉消息。以色列隱私管理局於2/10發表緊急聲明，將深入調查此事，聯合黨高層與Feed-b有可能因違反隱私法令而面臨刑事或民事處分。

資料來源：https://www.haaretz.com/israel-news/elections/.premium-app-used-by-netanyahu-s-likud-leaks-israel-s-entire-voter-registry-1.8509696 2020/2/26

伊朗駭客入侵美國電網、油氣公司

媒體Wired引述資安公司Dragos最新發布，名為「North American Electric Cyber Threat Perspective」報告，近期傳聞與伊朗政府相關Magnallium駭客組織正積極活動中，該組織又名APT33、Refined Kitten或Elfin。Dragos偵測到Magnallium已成功駭入美國電廠、煉油及天然氣公司網路。

報告指出，伊朗駭客使用「密碼潑灑」(password spraying)手法，即以特定簡單常見之密碼組合，針對目標企業帳號進行破解測試，藉此進入受害企業網路。不過Dragos研究人員發現，有另一個名為Parisite駭客組織也參與Magnallium行動，但前者是利用美國油、電公司之VPN軟體漏洞入侵公司內網。根據Dragos追蹤，Magnallium與Parisite從2019年起，就一直頻繁活動並延續至今，且Magnallium攻擊對象也不限於美國能源業，2018年也曾攻擊沙烏地阿拉伯、南韓石化廠及美國航太產業。該報告並未說明駭客活動是否導致美國企業資料損失，不過指出未有跡象顯示伊朗駭客已成功駭入電網、油氣設施實體控制設備軟體。

另一方面，沙烏地阿拉伯國家網路安全署(National Cybersecurity Authority)下之國家網路安全中心(National Cyber Security Center, NCSC)，也於近期對該國能源相關企業發出警告，因為2019/12/29在巴林國家煉油廠一名員工電腦上，偵測到一支能刪除電腦資料的惡意程式，NCSC將之稱為Dustman。沙國研究人員相信它利用VPN軟體漏洞，藉由VPN連線取得受害公司網域管理員帳密，最後在其內網電腦上自我複製。不過這次所發現的Dustman攻擊，似乎是伊朗持續進行之駭客活動，與1月美、伊衝突事件沒有直接關係

資料來源：https://www.wired.com/story/iran-apt33-us-electric-grid/
https://dragos.com/resource/magnallium/ 2020/1/17

中油等3 家國內企業遭駭，調查局鎖定駭客組織、警告恐有新一波 ...

國內多家重要的能源、科技公司如台灣中油、台塑集團、力成科技日前接連遭到勒索軟體攻擊，法務部調查局成立專案小組進行偵辦，15 日公布涉案的駭客組織與犯案手法，情資更顯示駭客預謀近日針對國內 10 家企業再度發動新一波攻擊。

包括中油、台塑、力成在 5 月 4 日至 5 日期間，接連遭到惡意攻擊。駭客入侵並將勒索軟體植入公司系統、個人電腦以及伺服器等資訊設備，造成重要檔案無法開啟、系統停擺，同時公司也被要求交付贖金。一連串攻擊造成像是中油加油站無法正常使用捷利卡、中油 Pay 等服務，力成湖口廠區的部分伺服器遭病毒感染後緊急關閉，隨後都已恢復正常運作。

經過調查局調查，駭客是在數個月前透過員工的個人電腦、網頁以及資料庫伺服器，入侵企業內部網路並展開刺探與潛伏，等待竊取帳號權限後侵入網域控制伺服器，並利用凌晨時段竄改群組原則（GPO）以派送具有惡意行為的工作排程。

資料來源： 科技新報 2020/5/16

總結
個人-十大資訊安全好習慣

- 不明人士要盤查
- 社交工程要小心
- 電腦不用要登出
- 機密文件要保護
- 密碼設定要穩固
- 重要資料要備份
- 電腦防毒要更新
- 應用系統要更新
- 使用網路要提防
- 電子郵件要過濾

簡報完畢，敬請指教