臺灣雲市集

臺灣雲市集-雲端解決方案

個資保護及資訊安全教育訓練

主辦單位：數位發展部數位產業署 Administration for Digital Industries, moda

執行單位：CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C.

授課講師：tsc 德欣 TSC CAPITAL GROUP

簡報大綱

一 資訊安全簡介

二 個資及資安事件案例分享

三 個人資料保護簡介

個資保護及資訊安全教育訓練

一、資訊安全簡介

什麼是資訊安全？

- **您是否有在日常生活中做過以下事項?**
  1. 為了方便使用，都用同一組密碼，且放置於隨手可得查詢密碼的地方，如：便利貼、桌面。
  2. 將會員資料存放至未授權之雲端服務及隨身碟，且未進行資料加密保護或其他安全控管，如：私人雲端服務、個資於業務活動結束未刪除。
  3. 會員資料放置雲端服務系統時，未進行帳號權限控管，無論誰都可以查詢相關資料，如：帳號權限未區隔管理員、使用者。
- **當使用雲市集的CRM、POS、HR等系統、或各行業的預約系統，涉及客戶的個人資料時，或是同仁可能於系統中觸及公司的機敏資料等等，即為資訊安全相關的議題**

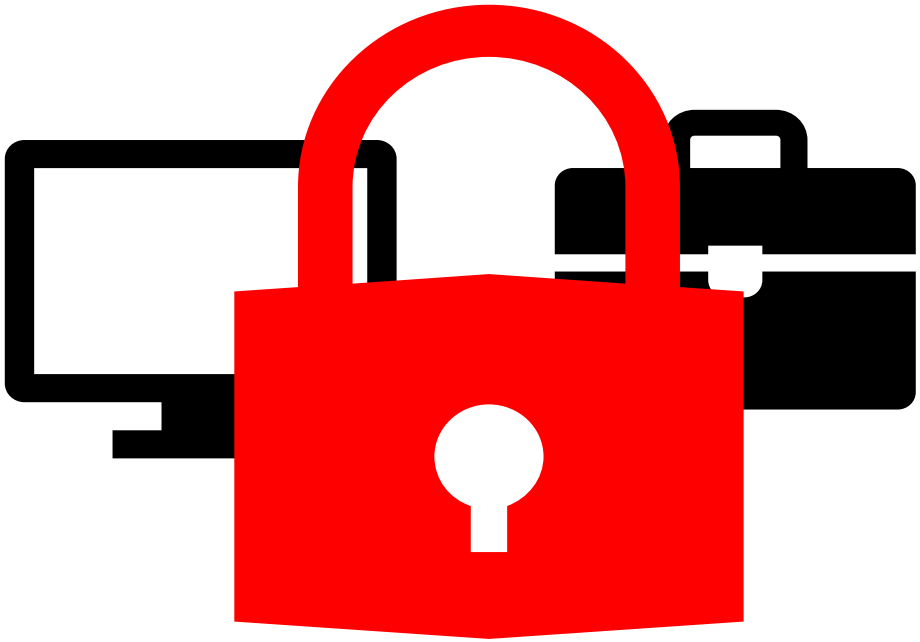
什麼是資訊安全？

- **何謂資訊安全？**

  保護資訊的**機密性**、**完整性**與**可用性**;另外也涉及如：不可否認性、驗證性、可歸責性、及可靠性等特性。

什麼是資訊安全？

- 何謂機密性?



上鎖了嗎?

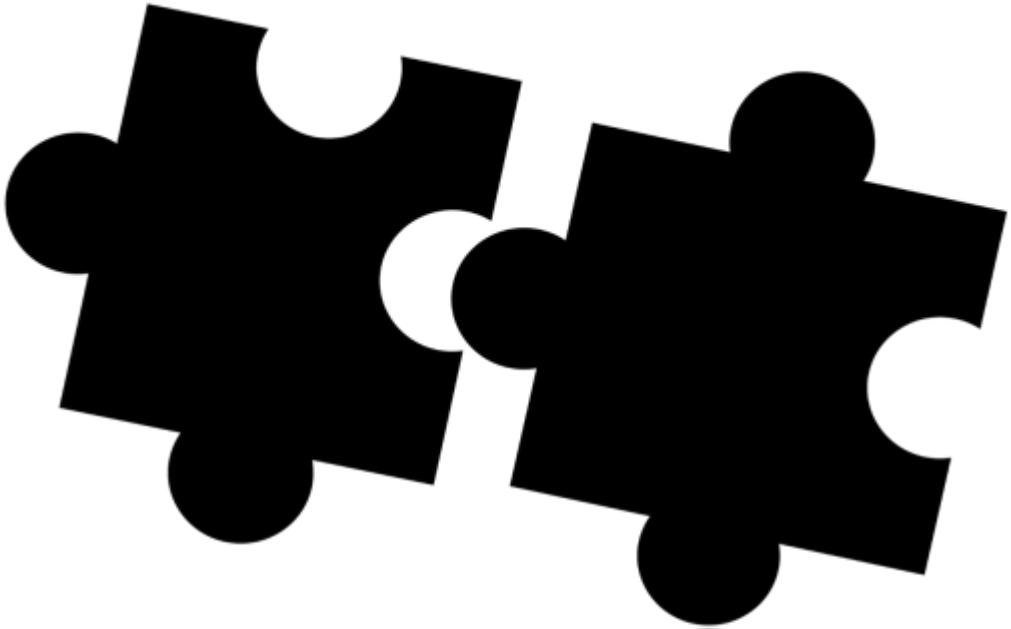
什麼是資訊安全？

- 何謂可用性?

能正常使用嗎?

什麼是資訊安全？

- 何謂完整性?



有被竄改嗎?

什麼是資訊安全？

- 為什麼需要資訊安全？

圖片來源：網上圖片

什麼是資訊安全？

➢資訊安全的迷失

1. 我的單位已經百分之百的安全！
2. 單位資訊沒有價值，有需要保護嗎？
3. 朋友、同事、長官寄來的信一定安全嗎？

近期政策重點

- 研究人員發現駭客利用Google雲端硬碟進行社交工程郵件攻擊，駭客將惡意檔案存放Google雲端硬碟並開啟分享，接著將下載網址內嵌在社交工程電子郵件附檔並寄給政府機關人員，誘導收件人透過附檔文件，下載藏有惡意程式檔案。
- 研究人員發現駭客偽冒資安廠商、政府機關及技服中心，對台灣企業機構發動針對性社交工程電子郵件攻擊，要求台灣企業機構執行「資安檢測審查」與查看「資安訊息警訊」，企圖誘騙受駭者下載與執行惡意郵件附檔夾帶的惡意程式。

資料來源：資通安全網路月報(112年1月)

近期政策重點

- 近期資安事件逾時案例，發現多起原因為承辦人不熟悉系統操作或因業務未詳盡交接，導致知悉事件後未於法遵時效(1小時)內完成通報。
- 使用雲端文件辦理相關業務(如調查教育訓練時數、彙整報名資料等)使用共用設定時，若資料包含個資或敏感內容，應限制具備存取權使用者，方可透過連結開啟檔案，檔案應以加密方式儲存；勿允許知道連結者皆可使用，以避免資料過度揭露。

資料來源：資通安全網路月報(112年1月、111年12月)

整體威脅趨勢

- 某機關活動網頁遭惡意置換，經查發現網頁為機關辦理活動時委託廠商所建置，活動結束後，未要求廠商下架活動網頁，遭入侵成功。
- 政府機關常委請廠商建置網站以宣導或發布活動相關訊息，惟業務或活動結束後，網站可能因疏於維護管理導致資安風險。機關可參考數位發展部之「政府網站管理服務規範」，於活動結束後將域名撤銷且辦理網頁下架作業，並訂定相關要求於合約中，避免衍生相關資安疑慮。

資料來源：資通安全網路月報(111年12月)

什麼是資訊安全？

- 資安宣導短片 - 一分半看懂資安

影片來源：NCCST

二、個資及資安事件案例分享

會員資料外洩(1/3)

- 提供汽機車共享服務的iRent和雲行動服務公司，發生外洩用戶個資事件，經查是資料庫出現防護性缺口，交通部公路總局要求限期改正，但複查發現改正未達標準，且外洩個資高達40萬筆。
- 交通部公路總局認定違反個人資料保護法第27條第1項及第2項規定，依個人資料保護法第48條第4款規定，處最高罰鍰新台幣20萬元。
- 目前台北市政府交通局、新北市政府交通局及桃園市政府交通局都認為iRent未善盡管理之責，依違反各縣市府之「共享運具經營業管理自治條例」，各處以最高9萬元罰鍰並限期改善。

資料來源：https://reurl.cc/3Oo8dM

會員資料外洩(2/3)

- 格上租車也傳出個資外洩風險疑慮，並針對格上Go Smart APP資安事件的回應，該公司表示，在2月2日晚間接獲通報，於一小時內即刻關閉格上Go Smart APP出租單查詢及存取功能，並立即清查該資料庫狀況，初步並未發現異常。
- 超過10萬筆的PDF訂單資料，沒有設定存取限制就擺放在雲端空間上，等同於任何人都可以看到車籍等私人資料，對此格上租車表示，接獲通報後，第一時間就關閉程式，並且清查資料庫狀況，也發送信件給所有使用者，確保資安無虞。
- 被使用者發現透過租車APP，下載訂單的資料夾，不但可以看到多達10萬筆其他人的訂單，還可以下載包括生日身分證字號等個資，約造成16000人個資外洩，科技工程師王景弘說：「應該要在下載的當下，那個網址必須要先做權限的管理，必須要明確的事我有授權，我才給你這個人的訂單檔案。」

資料來源：iThome 2023-02-06

會員資料外洩(3/3)

- iRent用戶個資疑外洩

資料來源：https://youtu.be/BdBkA6-i8kk

華航資料外洩(1/2)

- 華航於1月初收到匿名網路勒贖信件，隨後有部分客戶個資被揭露於駭客網站，且名單涉及政商演藝界名人，包括副總統賴清德、台積電創辦人張忠謀、鴻海集團創辦人郭台銘、藝人林志玲等。
- 華航表示，日前接獲匿名網路勒贖信件後，已立即報警及依法通報主管機關，配合警方追查事件及釐清原因。該公司尊重主管機關裁罰，也將持續嚴格落實個資保護，提升資安品質，強化資通安全。對於所涉個資事件造成的紛擾及社會關注，表達最誠摯歉意。

資料來源：https://money.udn.com/money/story/5612/7006191

華航資料外洩(2/2)

- 華航遭匿名勒贖

資料來源：https://youtu.be/afs7GePzbio

企業個資外洩罰則

- 國發會3月2日於行政院會提報「防止非公務機關個資外洩精進措施」，提出強化聯繫會議、提高個資法罰則及設立個資保護獨立專責監督機關3大策略。
- 國內個資法罰鍰僅2萬到20萬，修法後將提高到什麼程度？國發會副主委高仙桂說，會參考國際立法，從營業額或固定額都有，屆時會在修法專案小組進行討論，但她坦言國內罰則確實偏低，至於提高到多少將再衡酌。
- 罰則訂定上也將參考國內個資外洩特別法，如人體生物資料庫、癌症防治法、電信法、資安法等法令，如資安法現有罰鍰是10萬到100萬，人體身體資料庫是50萬到250萬，都比現行個資法的20萬來得高。

資料來源：https://reurl.cc/9VDd2x

感應刷卡盜個資

- Prelix惡意軟體自 2014 年起入侵 ATM 提款機，並在幾年內滲透到 POS 系統，成為最先進的 POS 系統威脅。它有獨特的加密方案，可以即時修補目標軟體、強制協議降級、執行虛擬交易，逃避詐欺交易檢測，針對最複雜的晶片密碼（CHIP and PIN）技術信用卡進行攻擊。
- 感應支付會觸發信用卡上的 RFID 晶片，將獨有 ID 和交易資料發送到終端，兩種資料不能再次使用，於是駭客無法從中竊取任何資訊。疫情期間人們對經手現金變得更加謹慎，這使 Prelix 加速進化，開發新的手法來竊取資料。
- 目前保護自己受到 Prilex 等惡意軟體攻擊的方法很有限，因為無法得知 POS 系統是否已遭入侵。除了非接觸式交易錯誤這種異常情況要多留心，定期注意自己信用卡交易紀錄，如有疑慮應立即回報發卡銀行尋求協助。

資料來源：https://reurl.cc/ykmjRD

密碼管理器真的安全嗎？

- 111年8月密碼管理服務商LastPass公司網路遭駭客竊走部份技術資訊及程式碼，引發了11月用戶密碼儲存庫的駭入事件。
- 駭客利用第一次攻擊取得的資訊，進行偵察、列舉及資料外洩行動，入侵LastPass的雲端儲存環境。這個位於AWS S3的儲存環境儲存了客戶檔案備份，包括公司名稱、電子郵件、IP位址、密碼及加密儲存庫資料，廠商於112年1月證實已外洩。
- LastPass的回應措施包括啟動以微軟Authenticator的條件式存取PIN比對多因素驗證（PIN-matching）、輪換關鍵及高權限的登入憑證、撤銷且再發放憑證。
- 已有用戶因這起資料外洩案，112年1月對該公司提起集體訴訟。

資料來源：iThome 2023-03-01

雲端服務安全

- 雲端資安防護5秘訣：
  1. 使用第三方提供的服務時，應審慎評估第三方設定了哪些既有功能且是否會造成資安疑慮，如：防火牆。
  2. 金鑰權限應視其所對應的任務來設定，避免過份授權而讓有心人士能為所欲為。
  3. 要將專案上傳以協作時，務必記得先檢視專案中是否含有機敏性資訊，也可以透過平台（如：Git）本身的設定，避免人為失誤洩漏資訊。
  4. 將資料搬遷至雲端後，可以在平台上設定預算通知，若有因異常流量而產生突發性的費用增高，也能讓用戶盡快發現此情況。
  5. 除了雲端平台本身的設定之外，針對常見的外部的威脅（i.e. DDoS、DNS攻擊 etc.），也可透過服務商提供的服務，依自身需求定義WAF或透過服務商清洗DDoS。

軟體更新

- 檢查重要軟體是否為最新版本：
  - 作業系統(Windows、Linux…等)
  - 網頁瀏覽器
  - 辦公室應用軟體(Office、Adobe PDF…等)
  - 電子郵件收發軟體(如outlook、outlook express…等)
- 善用Windows Update
  - 自動更新

防毒軟體

- 不關閉、不移除防毒軟體
- 隨時保持病毒碼是在最新的狀態
- 定期執行掃毒
- 小心使用隨身碟
  - 關閉自動播放功能
  - E-mail傳送檔案

重要資料應妥善保管

- 重要文件
  - 不可任意放置桌上，避免輕易丟失
  - 應存放於安全地方，避免被盜取使用
  - 加密保存，增加資料安全性
  - 勤加備份，避免資料遺失

你的密碼安全嗎？

資訊來源：https://official-blog-tw.line.me/archives/37682230.html

影片分享

- 資己資彼

資訊來源：https://youtu.be/O4FqzfqwgmE

三、個人資料保護簡介

資料可攜之權限管理

- 以雲端收銀POS機為例：
- 從系統攜出會員相關資料時，應注意下列事項：
  ① 資料分類要做好權責分明，非相關業務同仁不得存取。
  ② 查詢資料應避免非業務權責人員閱覽、擷取及破壞。
  ③ 必要時透過加密和權限控管。
  ④ 資訊使用目的消失應立刻刪除。
- 可攜式設備之管理：
  ① 作業系統更新。
  ② 安裝防毒軟體、開機更新及掃描。
  ③ 與其他設備交換資料前先經掃毒。
  ④ 敏感資料非經許可禁止儲存。
  ⑤ 允許儲存之敏感資料應加密處理，用畢後清空。

資料可攜之權限管理

- 高階主管往往擁有所謂的特權帳號，對資料存取或系統維護有很高的權限，若管理不當恐讓企業付出重大代價(如：商譽)。
- 所以需建立一套完整的制度，並且落實分權管理，也提升企業環境內的資安強度，避免特權帳號淪為任何人開啟機密大門的鑰匙。
  1. 每個部門都要有不同的帳號、權限。
  2. 避免讓每個人都擁有刪除的權限。
  3. 避免將重要資料放置於網路空間。
  4. 帳號密碼勿記載於他人垂手可得之地方。
  5. 帳號密碼定期更新。

個資議題 - 法規摘要1

- 個資法第 2 條，個資定義如下：
  - ① 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。
  - ② 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。
  - ③ 蒐集：指以任何方式取得個人資料。
  - ④ 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。
  - ⑤ 利用：指將蒐集之個人資料為處理以外之使用。
  - ⑥ 國際傳輸：指將個人資料作跨國（境）之處理或利用。
  - ⑦ 公務機關：指依法行使公權力之中央或地方機關或行政法人。
  - ⑧ 非公務機關：指前款以外之自然人、法人或其他團體。
  - ⑨ 當事人：指個人資料之本人。

資料來源：個人資料保護法

個資議題 - 法規摘要2

- 個資法第 3 條，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：
  - ① 查詢或請求閱覽。
  - ② 請求製給複製本。
  - ③ 請求補充或更正。
  - ④ 請求停止蒐集、處理或利用。
  - ⑤ 請求刪除。

資料來源：個人資料保護法

個資議題 - 法規摘要3

- 個資法第6條 (特殊類別個資限制)
- 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
  - ① 法律明文規定。
  - ② 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
  - ③ 當事人自行公開或其他已合法公開之個人資料。
  - ④ 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，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。
  - ⑤ 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內 ，且事前或事後有適當安全維護措施。
  - ⑥ 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制 不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者 ，不在此限。
- 依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

資料來源：個人資料保護法

個資議題 - 法規摘要4

- 個資法第8條 (蒐集之告知)
- 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：
  ① 公務機關或非公務機關名稱。
  ② 蒐集之目的。
  ③ 個人資料之類別。
  ④ 個人資料利用之期間、地區、對象及方式。
  ⑤ 當事人依第三條規定得行使之權利及方式。
  ⑥ 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。
- 有下列情形之一者，得免為前項之告知：
  ① 依法律規定得免告知。
  ② 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
  ③ 告知將妨害公務機關執行法定職務。
  ④ 告知將妨害公共利益。
  ⑤ 當事人明知應告知之內容。
  ⑥ 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

資料來源：個人資料保護法

個資議題 - 法規摘要5

- 個資法第9條 (處理或利用前之告知)
- 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。 有下列情形之一者，得免為前項之告知：
  - ① 有前條第二項所列各款情形之一。
  - ② 當事人自行公開或其他已合法公開之個人資料。
  - ③ 不能向當事人或其法定代理人為告知。
  - ④ 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供 者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
  - ⑤ 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。
- 有第一項之告知，得於首次對當事人為利用時併同為之。

資料來源：個人資料保護法

個資議題 - 法規摘要6

- 個資法第19條
- 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
  - ① 法律明文規定。
  - ② 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
  - ③ 當事人自行公開或其他已合法公開之個人資料。
  - ④ 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。
  - ⑤ 經當事人同意。
  - ⑥ 為增進公共利益所必要。
  - ⑦ 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
  - ⑧ 對當事人權益無侵害。
- 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

資料來源：個人資料保護法

個資議題 - 法規摘要7

- 個資法第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：
  - ① 法律明文規定。
  - ② 為增進公共利益所必要。
  - ③ 為免除當事人之生命、身體、自由或財產上之危險。
  - ④ 為防止他人權益之重大危害。
  - ⑤ 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。
  - ⑥ 經當事人同意。
  - ⑦ 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。

資料來源：個人資料保護法

通知當事人

- 個資法第 12 條
  - 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，**應查明後以適當方式通知當事人。**
- 個資法施行細則第 22 條
  - 本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他**足以使當事人知悉或可得知悉之方式為之**。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路 、新聞媒體或其他適當公開方式為之。 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

資料來源：個人資料保護法

個資法規罰則

- 個資法第 28 條
  - 公務機關**違反本法規定**，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
  - 被害人**雖非財產上之損害，亦得請求賠償相當之金額**；其名譽被侵害者，並得請求為回復名譽之適當處分。
  - 依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，**以每人每一事件新臺幣五百元以上二萬元以下計算**。

資料來源：個人資料保護法

個資三原則

- 不要拿
  - (非業務使用之必要，勿存取個資)
- 不要留
  - (業務上必要之個資，使用後立即刪除)
- 不要傳
  - (勿恣意傳遞業務上之個資)

響應資安政策，6/30 前智邦生活館加碼優惠

1. 資安產品買一送一

- 購買【單次網站弱掃服務】了解並修補網站漏洞，預防損失
- 購買【郵件S/MIME 數位憑證】讓信件往來可以簽章與加密
- 新購買【 DV等級SSL憑證】讓網站傳輸都能使用加密連線

2. 主機購買優惠碼

- 凡新購買【共享型虛擬主機】與【 WordPress專用主機】系列，填寫優惠碼「 JgyFpeVc00」， 現折 $1,500

24小時免付費專線

0800-248-013

活動備註：本活動目的為推廣資訊安全意識及加強個資安全，歡迎您將簡報內容及優惠訊息與您的親友分享，杜絕詐騙需要你我共同努力。

智邦生活館 www.url.com.tw