資安星際指南

網路安全輕鬆學

－前言－

別讓資安成為最後才想到的事

對多數中小企業或非營利組織而言，資安往往不是一開始就會優先考慮的項目。每天忙於經營、募款、交付成果，能讓組織順利運作已經不容易，更遑論還要騰出心力理解資安議題。

然而現實是，隨著資通系統的使用日益頻繁、雲端服務越來越便利，暴露在資安風險中的機會也隨之提高。一組外洩的帳號密碼、一封偽裝巧妙的釣魚信件，都可能導致整個組織承受沉重的損失。

人們心中多少都存有僥倖心理：「我們組織這麼小，駭客應該不會盯上吧？」「有用 VPN，應該就夠安全了吧？」這些想法或許能暫時帶來安心，但事實上，組織之所以成為攻擊對象，往往不是因為擁有多珍貴的資產，而是因為系統中的弱點過於明顯，成了駭客眼中的低成本目標。

這本手冊，期盼能以簡單易懂、貼近實務的方式，陪伴您一步步認識網路安全，在有限資源下也能做出關鍵防護，守住組織營運的底線。

國家資通安全研究院
National Institute of Cyber Security

本手冊會帶您認識以下主題

① 常見的網路威脅有哪些？

② 公司裡的網路設備，應該怎麼規劃與管理？

③ 每天都在用的智慧裝置、Wi-Fi，可能有哪些安全細節？

④ 電子郵件有什麼陷阱？該怎麼避免被網路釣魚？

⑤ 如何保護自己在使用網路服務時，身分不會被盜用？

無論您是主管、行政人員、IT 或助理，或是經常與外部廠商溝通的窗口，只要多一分資安意識，就能有效降低風險、保護自己與組織。

希望這本手冊能成為您工作上的得力助手，協助您在善用數位工具與網路服務的同時，也能安心、穩健地完成各項任務。

使用指南

💬 **故事劇情：**和大山與老鼻深入資安情境題，破解各式挑戰

⭐ **資安知識：**快速掌握防禦重點，並可留意 🚩 小提醒的秘訣

🖍️ **大山筆記本：**以清單快速確認自身與組織的資安完備狀態

📚 **延伸閱讀：**進一步了解文中以螢光筆標注的專有名詞

本書主角

大山

充滿朝氣的穿山甲，「星際環境保育」星球的社會新鮮人，以環境保護為己任。

初入職場的大山被老闆交付了大任務：「以後公司的資安相關工作就拜託你了！」沒有資訊背景的他，是否能勝任這份工作？

老鼻

機靈的白鼻心，大山的學長兼好鄰居，外表看起來漫不經心，其實非常可靠。

上知天文下知地理的他，熱心且經驗豐富。經歷過組織遭駭的資安大危機，相信能傳承經驗，帶著大山度過重重難關！

Chapter 1
網路安全概述——威脅在哪裡

關鍵字 資安威脅、網路安全、風險評估

大山今年從學校畢業，在「星際環境保育」星球找到夢寐以求的工作。

報到第一天，老闆拍了拍他的肩膀，說：「我們公司裡你最年輕了！年輕人不是都很會用電腦嗎？以後資訊相關的東西都交給你了！」

公司雖然不大，但日常工作早已離不開網路：捐款事務需要透過廠商套裝系統處理、多數資料都儲存在雲端硬碟、採購用 E-mail 往來、商品門市也使用網路攝影機來確保安全。

大山一開始信心滿滿地接下這份工作，心想反正就是管理幾個常見的軟硬體和辦公設備，應該不會太難。直到某天，他聽說某家公司網站被駭、顧客資料外洩，這才讓他開始緊張起來：「這種事會發生在我們身上嗎？」

老鼻是大山的學長，這幾年在資安領域下了不少功夫。曾親歷公司遭駭事件的他語重心長地說：「現在工作越來越依賴網路，資安風險可不能掉以輕心！我們公司當初被入侵後，才真正警覺。我也做了不少功課，剛好可以跟你分享一些心得！」

資安威脅面面觀

① 常見的資安威脅有哪些

勒索病毒攻擊

某公司員工誤點了一封冒名的電子郵件，電腦桌面的資料瞬間被加密。螢幕上只剩一句話：「請支付比特幣贖金，否則資料無法還原！」

網站遭駭被張貼假訊息

駭客入侵某公司的官網，放上假募款連結。所有捐款者的個資與款項，全落入駭客手中！

Wi-Fi 被濫用，成為垃圾郵件跳板

公司使用沒有密碼、或密碼太過簡易的無線網路，遭有心人士連上，藉由此網路大量發送垃圾郵件，導致公司 IP 被封鎖，最後連正常郵件都寄不出去。

遠端連線未加密，帳號被盜

老闆從國外連回公司系統，但沒有使用 VPN 或其他加密方式，結果登入資訊在不安全的連線中被攔截，帳號直接遭盜用。

小提醒：看似平靜的網路日常，其實隱藏了許多想像不到的資安風險。多看案例、多思考風險來源，是建立資安意識的第一步！

② 威脅從哪裡來

大山聽完這些案例後滿臉震驚：「原來外部威脅這麼多啊！」

沒想到老鼻卻搖搖頭說：「事實上，比起外部的危險，內部疏忽更要提防。很多資安事件，其實都是自己人不小心釀成的。」

外部情境

說明	常見情境
• 駭客入侵	• 網站被植入假募款連結
• 惡意軟體感染	• 中勒索病毒，資料被加密勒索
• 釣魚郵件攻擊	• 點擊偽裝成通知信的惡意連結
• 外包廠商資料外洩	• 第三方廠商未妥善保管機敏資料導致外洩

內部情境

說明	常見情境
• 員工操作疏失	• 將機密資料誤寄給錯誤對象
• 帳號權限設定不當	• 在公務設備使用未掃毒的 USB
• 防火牆或系統設定錯誤	• 共用帳號未登出導致異常登入
	• 未封鎖不安全的連線

③ 防護做到哪？資料價值與風險程度說了算

老鼻看到大山臉色發白，笑著安慰他：「你也不需要每天緊張兮兮，資安防護要做到什麼程度，其實跟你手上的『資料價值』，還有『風險程度』有關。先盤點你的系統蒐集了什麼資料、有多重要、可能會面臨什麼風險，再決定資源怎麼配置才有效率。」

來看看幾個例子：

- **官網只展示可被公開的資訊？**
  雖然風險較低，但還是要防範被惡意篡改。
- **是否保存顧客個資或付款資料？**
  若有，則需要訂定更嚴謹的保護措施。
- **辦公室設有內部網路與共享設備嗎？**
  安裝後須考慮誰能存取、是否有加密連線。

小提醒：即使對資訊或資安一竅不通，也可以透過「風險在哪」、「哪些資料不能外洩」的風險分級思維，逐步建立一套實用的資安防護策略。

大山筆記本

Q 公司目前有使用哪些網路服務呢？
Gmail、雲端硬碟、網頁訂單系統、Wi-Fi

Q 有什麼資料是絕對不能外洩的？
客戶個資、交易紀錄、供應商資料、後台管理者的帳號密碼

Q 過去曾發生過哪些資安小意外？
同事誤點釣魚信件、共用帳號出現異常登入紀錄等

Q 目前有什麼資安防護措施呢？
只買了一套防毒軟體，其它還在規劃中

大山這才真正意識到：原來資安之所以常讓人摸不著頭緒，往往是因為少了「資料價值與風險」這道關鍵的盤點程序！

他決定先動手處理這項簡單的工作：把公司擁有的資料分成高、中、低 3 個等級，順便也盤點一下設備，再來好好思考怎麼保存跟維護。

但是，對於辦公室的設備還有哪些風險，他毫無頭緒。因此接下來他還想再向老鼻請教——公司網路設備，還有哪些潛在的資安地雷？

👉第二章：防火牆與網路區隔——我們與惡的距離

Chapter 2
防火牆與網路區隔——我們與惡的距離

關鍵字 防火牆、網路區隔、通訊埠

「你知道什麼是防火牆嗎？」老鼻問。

「聽過，但不太清楚是什麼……好像跟擋病毒有關？」大山一邊說一邊皺眉，其實連防火牆怎麼寫都不太有把握。

老鼻說：「防火牆就像大門的警衛，負責幫忙看守誰可以進出，不是只有擋病毒的作用喔！是所有『不該進來的連線請求』都會擋下來。」

大山點點頭，接著問道：「咦？我還聽過一個東西叫『路由器』，那又是什麼呀？」

老鼻回答：「那你一定也聽過『數據機』對吧？這些名詞聽起來都很像，腦袋一定快打結了。別急，我們先搞懂防火牆這塊，其他的，我之後慢慢告訴你！」

防火牆與網路區隔實務

① 防火牆：網路的第一道防線

防火牆就像檢查哨，負責判斷哪些資料是安全的、哪些不是。防火牆會根據預先設定的規則，決定什麼樣的資料可以進出公司網路。

老鼻舉了個例子：「家門如果沒鎖，誰都能開門進來。網路上的防火牆就像是那道門，透過他的後台設定，可以決定誰能擁有鑰匙。」

他們聊著聊著，大山決定順便來檢查公司現有設備的設定，結果竟發現：公司的防火牆功能根本沒啟用！老鼻在電話中聽到大山的轉述，也感到非常不可思議：「防火牆功能沒打開，就像辦公室的大門沒關，誰都能走進來。」

大山不敢大意，立刻進行修補動作：

- **啟用路由器內建的防火牆功能**
- **修改預設密碼**
- **停用不需要的外部連線（例如遠端桌面工具）**

小提醒：家用路由器大多內建基本的防火牆功能，但預設密碼通常容易被破解。務必更改預設密碼，並開啟相關的安全設定！

② 常被忽略的防火牆關鍵設定

開啟防火牆後大山仍然驚魂未定，因為他突然想到，在開啟防火牆之前，官網可是完全暴露在脆弱當中！於是他開啟後台的管理介面，果然發現一個陌生的登入紀錄。

「這是哪來的 IP ？我們公司沒人來自這個國家啊？」大山皺著眉，截下這個可疑紀錄傳給老鼻，請他幫忙看看。老鼻不看還好，一看差點昏倒。

「你們的官網後台網址很好猜，加上防火牆沒有限制任何 IP 存取，只要知道網址，誰都能嘗試登入，等於後台是對全世界開放的！」

大山此刻已經嚇到臉色發青，想不到防火牆的預設設定，竟然允許外部人士連進他們的官網後台！

老鼻無奈地說：「防火牆不是開啟就無敵，如果關鍵功能沒發揮作用，都是白費呀！以下這些基礎的設定，你一定要記得！」

設定連線規則

防火牆是根據規則來決定哪些連線可以進、哪些必須被擋下。因此，正確設定連線規則非常重要。建議明確指定允許哪些 IP、哪個來源網段、哪些服務或通訊埠可以進入，其他一律封鎖。

不開放過多通訊埠

為了方便遠端連線，有時會開放許多通訊埠 (Port)，像是遠端桌面、資料庫等。但只要其中一個埠所對應的服務有安全漏洞，駭客就可能從那裡入侵。原則上只開啟需要的通訊埠，其他都應該關閉。

啟用日誌監控

防火牆的日誌 (Log) 監控會記錄所有進出流量，幫助追查異常行為，是資安事件後鑑識的重要線索。

定期更新防火牆規則

網路環境會變，防火牆的設定規則也要跟著調整，否則很容易留下過時的漏洞，建議每 3 ～ 6 個月檢查一次防火牆設定。

小提醒：防火牆不是裝好就沒事，定期更新及調整設定才是上策。

③ 內部網路區隔

就在處理完防火牆設定後，大山總算稍微鬆了口氣。但他還沒來得及慶幸，就冒出另一個疑問。

「等一下……辦公室的印表機、同事的筆電，還有 NAS 儲存裝置，這些設備都接在同一個 Wi-Fi 上，這樣會有什麼問題嗎？」

老鼻回道：「你問得很好！其實這種情況也很危險，如果某台設備被攻陷，病毒就會沿著網路擴散出去。」

大山倒抽一口氣：「所以防火牆是對外防守用的，內部網路還得靠我們自己去分散風險？」

老鼻點點頭：「沒錯，我們還要做網路區隔，把不同設備依用途、風險分級分開來，這樣才能把災害影響降到最小。來吧，帶你看看幾種簡單實用的網路區隔方式。」

區隔方式	適用情境
方法一 使用不同 Wi-Fi 設定不同 SSID 與密碼讓訪客與辦公設備分開	適合 小型辦公室
方法二 虛擬區域網路 VLAN 在同一台設備內劃分多個邏輯網路	適合 有資訊專責人力的 中型公司
方法三 子網 Subnet 用 IP 位址範圍區隔設備權限	進階使用者或 有管理需求的 大型公司

大山說：「把網段區隔開之後，我好像開始抓到規劃設備網路的感覺了！」

老鼻笑著點頭：「沒錯！而且重點其實不在設備的種類，反而應該看它處理的資料有多敏感、需不需要對外連線，以及一旦被入侵，會不會波及其他系統。這些風險層面，才是真正決定它該放在哪個網段的依據，我們可以先來做一張盤點表看看。」

設備網段設置盤點表

設備類型	處理資料	需連接外網	風險等級
NAS 儲存設備	公司文件 備份資料	否	高
一般員工筆電	業務文件、 郵件、系統存取	是	中
網路攝影器	控制命令、 裝置資料回傳	是 可能連回廠商雲端	中
無線印表機	列印任務暫存資料	否	低
訪客裝置	無 不應接觸公司資源	是	低

大山筆記本

Q 公司有沒有啟用防火牆？
沒注意過，今天檢查後才打開

Q 誰能進入 Wi-Fi 設定畫面或是連線到 NAS?
以前沒限制，現在設定成來自內部網路，且特定 IP 裝置才可以登入

Q 訪客來辦公室用哪個 Wi-Fi ？
之前都是與辦公室共用同一網路，現在已新增「guest」訪客專用網路

大山發現不是有密碼就安全，重要的是哪些狀況允許連線、哪些必須阻擋，還要把設備之間的網路界線畫清楚，才是真正有效的管理措施。

接著，老鼻將帶大山探討辦公室裡那些看起來「無害」的設備，從印表機到智慧家電，原來也可能是駭客的後門！

👉第三章：IoT 物聯網安全——設備也可能是破口

延伸閱讀

什麼是通訊埠（Port）

把一台伺服器想像成一棟大樓，而通訊埠（Port）就像是這棟大樓的各個**房間號碼**，每個通訊埠負責不同的事情：

房間號碼	功能	說明
80 號	明文傳輸 HTTP	**就像「公開廣播」**，大家都能聽見資料內容，如果用來在網際網路傳輸機敏資料是不安全的
443 號	加密傳輸 HTTPS	**就像「私人秘密對話」**，別人無法偷看你傳的資料。適用於銀行、購物等需保護資料的網站
25 號	寄信 SMTP	用以傳送電子郵件
3389 號	遠端遙控電腦 RDP	用來遠端連到別台電腦或伺服器

當資料（封包）從網路進來時，它會指定要進入哪個「房間」，系統就會把資料交給對應的服務來處理。通訊埠號碼就是電腦的服務門牌，開哪幾個，駭客也看得一清二楚。

如果電腦開了很多通訊埠，駭客就能掃描每個門口，找看看哪一個沒鎖好。因此，平常時只開啟需要的通訊埠，其他關掉或採取限制，能大幅降低風險。

延伸閱讀

防火牆的 Deny All 設定

想像家中大門的電子鎖，只設定幾個家人能用指紋辨識的方法開門進來。

這就叫做 Deny all, allow some—先擋全部，只放行一部分的人。

不確定風險會來自哪個管道，乾脆先全部封鎖，再一一開啟真的需要的幾個通道（像是公司網站、信箱伺服器等等）。雖然一開始會覺得麻煩，但能大幅降低被攻擊的風險。

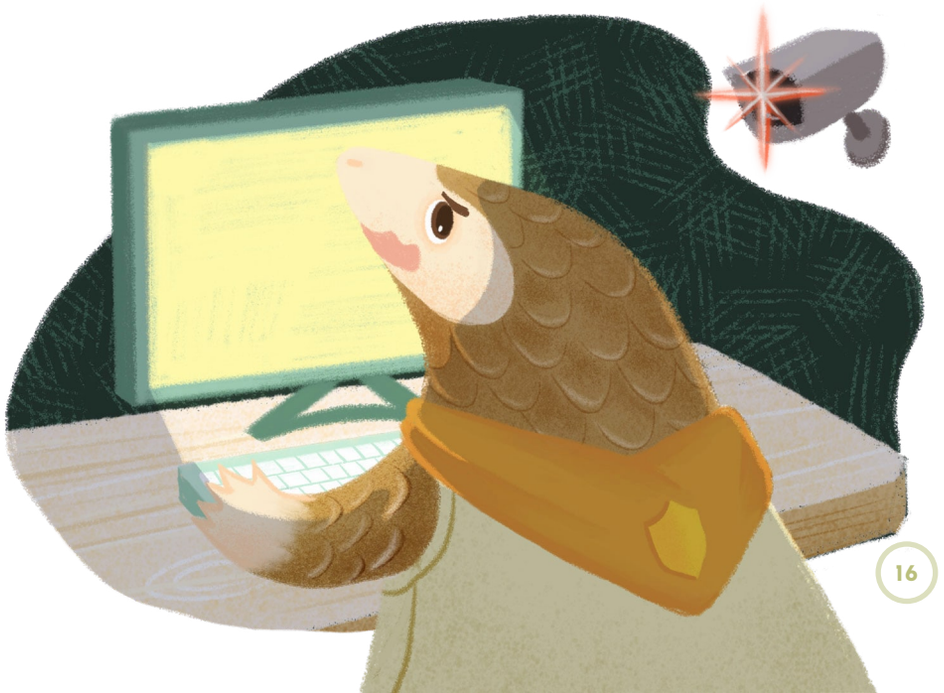
Chapter 3
IoT 物聯網安全——設備也可能是破口

關鍵字 IoT 裝置、預設密碼、佈纜安全

某天下班後，大山還在整理伺服器的設定檔，忽然看到天花板上的網路攝影機亮起燈號，甚至緩緩轉向自己。

大山當場被嚇得冷汗直流、心裡發毛，他心想：「明明昨天才去拜拜，怎麼今天就撞鬼？」

冷靜下來後他仔細一想：「咦？這台攝影機除了我，沒人有後台權限呀？」他納悶地登入管理介面查看，沒想到——畫面上竟顯示出一筆來自外部的遠端連線！



幸好在上個月，大山早就把攝影機架設在與內部核心網段隔離的專屬網段。當下他立刻中斷攝影機的網路連線，衝回家裡向他最可靠的鄰居老鼻求救。

老鼻一聽，眉頭立刻皺了起來：「你們那台攝影機有改過預設密碼嗎？」

大山一愣：「呃，好像沒有欸，帳號 admin、密碼也是 admin……」

老鼻重重嘆了一口氣：「這種看起來無害的網路設備，才是最常被忽略的資安破口。駭客會掃描全世界的預設登入帳戶，你不改預設帳密，就像開著門等他們進來啊！」

IoT 裝置安全指南

① IoT 裝置的常見風險

IoT（Internet of Things）物聯網，指的是透過網路將「實體物品」與「數位世界」連結起來的技術架構。IoT 裝置在我們身邊隨處可見，除了家用電器如掃地機器人、智慧家電等等，也包含許多在辦公場域常見的裝置，像是：

- 監視器
- 多功能事務機
- 門禁系統
- 空調與電力監控設備
- 智慧燈控、音響

這些裝置能提高工作效率，但也可能帶來資安風險，讓我們看看幾個例子：

監視系統

風險 若使用預設密碼或未妥善設存取權限，可能被未授權人士遠端觀看畫面。

案例 某國外網站，曾公開全球許多使用預設密碼的網路攝影機畫面。

電子看板

風險 若安全機制不足，可能被駭客入侵並更改顯示內容，用於散佈不當或惡意資訊。

案例 台灣某超商電子看板曾遭駭客入侵，播放不當或恐嚇訊息影響形象。

多功能事務機

風險 如使用非公司內部信箱傳送資料或文件，可能導致機密資料外洩。

案例 公司向設備廠商租賃印表機服務，在使用掃描寄件功能時，寄件人預設為廠商電子郵件地址，造成資料在傳輸過程中外洩。

大山說：「原來我們身邊的辦公設備有這麼多的風險！但我還是不太理解耶，這些 IoT 裝置是怎麼被入侵的呢？有哪些具體管道嗎？」

老鼻說：「你問得很好，很多時候我們在使用裝置時，忽略了定期更新或是修改原廠設定的重要性，才導致後續風險持續擴大，我們來看看上面這些案例的前因後果吧！」

IoT 設備常見風險

風險一 **使用預設密碼：**設備出廠時的預設帳號密碼未更換

情境說明

原廠帳號密碼多為網路上公開資訊，容易被暴力破解或直接登入。

潛在後果

駭客可輕易的取得設備管理權限，進而讀取、修改或刪除資料。

風險二 **韌體沒更新：**設備長期未進行韌體或安全更新

情境說明

更新提醒被忽略或關閉，而繼續使用已知漏洞的系統版本。

潛在後果

已知漏洞是公開資訊，駭客針對舊版本用戶執行惡意程式，造成系統癱瘓。

風險三 **沒做內網區隔：**所有設備皆部署於同一網段或 Wi-Fi 環境

情境說明

因未實施網段隔離、VLAN 或防火牆等政策導致內部網路缺乏防護界線。

潛在後果

其中一台設備遭受感染後，可進行橫向移動攻擊，快速擴散至其他設備，導致全面資料外洩或服務中斷。

風險四 **設備使用公開 IP 對外開放：**

為了管理便利將 NAS 等設備以公開 IP 提供遠端存取

情境說明

若缺乏 VPN、防火牆與登入驗證等基本安全措施，任何人都能透過網際網路連接該設備。

潛在後果

容易遭自動化掃描、暴力破解，進而被植入惡意程式或納入殭屍網路，成為駭客操控的攻擊工具。

② 如何保護 IoT 裝置？

老鼻說：「這些裝置一不小心就會讓駭客乘虛而入。要守住 IoT 安全不見得要花大錢，可以先從我們能做的——更新裝置設定開始！」

正式使用前先更改密碼及設定

多數設備使用原廠設定的帳號密碼。連網之前，一定要把預設帳密換掉，並設定夠強的密碼。

把裝置關進「小房間」

盡量把 IoT 裝置與內部核心系設置在不同的網段，避免一旦遭駭入，擴散至內部重要業務，並透過防火牆限制哪些 IP 能跟這些裝置聯絡。

定期更新，不當孤島

主動檢查裝置廠商是否釋出更新版本，並安排定期檢查日（例如每月一次）更新韌體與系統。

裝置也要有日誌與監控

開啟日誌記錄，這樣異常連線發生時，才有跡可循。另外也要注意日誌紀錄是否詳實記載事件的內容與時間，校時系統也很重要！

選擇可信賴的廠牌

某些廠牌的設備已被公開其資安風險或已知漏洞。選購設備時，除了要留意廠牌及其產地之外，也要多方蒐集關於該設備之資訊，並選擇值得信賴的品牌。

③ 實體線路也有風險

大山煩惱的同時，老鼻馬上再追問：「你們公司的網路線是怎麼拉的？」

大山說：「應該就是裝修時一起拉的吧？線就走天花板，或是沿著牆壁繞一圈。」

老鼻眉頭一皺：「那你知道線路機櫃有沒有鎖嗎？有沒有從公共區域經過？」

見大山一臉困惑，老鼻語重心長地說：

「再安全的系統，如果誰都可以偷偷把網路線插入實體機櫃，那就等於自己幫駭客開門呀，你想想看喔，如果 .....」

網路插孔沒控管

說明	牆壁上的網路插孔可直接連上內部網路，沒有管制。
風險	客戶、訪客、外包廠商可直接插網路線連進公司內部網路。

線路外露或置於公共區域

說明	網路線走在開放區域或未上鎖的弱電箱中。
風險	線路可能遭人竊聽、擅自接入，或插入流量攔截設備進行資料監控與竊取。

IoT 裝置插線位置未控管

說明	投影機、門禁系統的網路線，與內部主機共線。
風險	IoT 裝置一旦被入侵，就能當跳板攻擊其他設備。

聽完老鼻的分析，大山恍然大悟：「原來危險藏在最安全的地方，這句話是真的耶！本來以為辦公室裡面是絕對安全的領域，都忘了我們偶爾也有訪客。」

老鼻說：「是呀！實體的線路正好成為防守思維的漏洞，也得留意才行！」

老鼻給大山一張檢查清單：

IoT設備安全檢查清單

- ☑ **確認弱電箱、交換器機櫃都有上鎖**

  避免任何人可以打開、插拔網路線

- ☑ **不讓外部訪客隨便用網路插孔**

  可採用 VLAN（虛擬區隔）或僅開放訪客 Wi-Fi

- ☑ **定期巡檢實體線路是否有異常**

  像是多出來的分線器、未知設備、線路被破壞等

大山筆記本

Q 有哪些 IoT 裝置？
門禁系統、印表機、展示間電視、會議室投影機

Q 裝置有改過預設密碼嗎？
通通沒有，都是買來就直接連網啟用了

Q 裝置有做網路區隔嗎？
已經跟辦公室的主要網段區隔開了

Q 裝置有更新過嗎？
沒有主動更新過，不知道廠商有沒有更新版本

Q 系統有日誌可以看嗎？
不清楚，要回去查設定頁面有沒有紀錄功能

Q 弱電箱 / 網路機櫃有上鎖嗎？
沒有上鎖，也沒設監控

攝影機事件在大山心裡投下一顆震撼彈，他決定回去一一檢查公司的所有設備，也準備升級公司的「IoT 安全守則」。

接著他也開始思考：「既然實體的電器都有問題了，無線網路是不是也需要注意？」

👉第四章：無線網路安全——您的 Wi-Fi 在開趴

延伸閱讀

IoT 裝置的原廠設定隱含什麼風險？

很多國外生產的網路設備（例如家用路由器、監視器），出廠時帶有預設的設定和帳號密碼，就有可能造成以下資安疑慮：

① 預設 DNS 設定可能將您的資料送出國外

許多 IoT 裝置在出廠時就內建預設的 DNS 設定，有些甚至設在國外。若未修改，這些裝置在連線過程中可能將使用紀錄傳送至國外，導致上網行為被監控或資料外洩。

② 預設帳號密碼可能讓駭客輕易登入

另一個更常見的風險就是預設帳號密碼。有些裝置預設登入就是「admin/admin」、「user/1234」這類非常簡單的組合，駭客都知道，網路上甚至有公開的帳密清單！

只要沒更換密碼，駭客用自動程式掃一遍就能輕易登入。

③ 若缺乏監控，風險就一直隱藏著

如果平常沒用監控工具（例如記錄 DNS 流量、分析網路封包），根本不會發現這些預設設定已危及安全，直到出現資安事件才知道，卻為時已晚了。

Chapter 4
無線網路安全——您的 Wi-Fi 在開趴

關鍵字 Wi-Fi 安全、公共網路、加密協定

某天早上，大山一如往常坐在辦公室，打開筆電開始處理捐款年度報表。他用手機連上 Wi-Fi，卻發現有一個叫「StarEco_Free」的網路沒設密碼，訊號還特別強。

「奇怪，公司什麼時候多了一個免費 Wi-Fi ？」

大山剛準備點下去，突然覺得不太對勁，趕快打給老鼻求救。老鼻聽聞狀況，馬上說：「等等！你是不是看到一個沒密碼的網路？」

大山點點頭。

老鼻趕緊阻止他：「沒有設密碼的無線網路可別亂連！不論是出現在自家的、還是路邊的都有風險！因為你不知道訊號從哪來，更不能知道他背後的設定是如何。」

Wi-Fi 安全與防護

① Wi-Fi 加密協定要選對

老鼻接著問大山：「你們公司的 Wi-Fi 是用什麼加密協定？」

大山說：「蛤？就是密碼呀。本來密碼是老闆的電話號碼，但現在歸我管了，我想改成自己的電話號碼，哈哈！」

老鼻無奈地說：「我其實不想知道你們家的密碼 ..... 你開心就好。但有密碼不代表安全，要看它在連線傳輸的過程中，是用什麼方法加密。來，給你看看目前幾種無線網路常見的加密協定。」

	安全性	說明
WPA3	最安全 現代標準	建議新設備 全都升級使用
WPA2 (AES)	較安全 目前普遍使用	使用此協定 是安全底線
WPA/WPA2 (TKIP)	有漏洞 不建議再用	較老舊裝置 才會支援
WEP	極弱 幾分鐘就能破解	已過時 不應再使用

小提醒：即使設定了 Wi-Fi 密碼，如果加密方式是「WEP」或「WPA（TKIP)」，駭客一樣可以輕鬆破解。

② 公司內部 Wi-Fi 不應該任意對外開放

老鼻還順帶提醒了大山，關於公司無線網路應該注意的事：

無線網路安全注意事項

- ☑ 路由器應該設定強密碼，使用最新加密協定 WPA3（或至少要 WPA2）
- ☑ 禁用老舊、不再使用的 Wi-Fi 名稱與設備
- ☑ 設定訪客 Wi-Fi 並與內部網路隔離
- ☑ 避免將 Wi-Fi 密碼貼在牆上，或避免使用過於簡單好猜的密碼（如 12345678）

③ 公共 Wi-Fi 隱藏的風險

下午，大山被派去參加其他星球的環保成果發表會。現場熱鬧非凡，他在咖啡廳坐下來用筆電修改簡報。準備連上網路時，他看到一個名稱「FreeWi-Fi」的訊號，他想也沒想就按下連線。

剛準備把檔案傳給同事，大山就看到老鼻的訊息跳出來：「你現在有開 VPN 嗎？你不會直接用公共 Wi-Fi 傳公司資料吧？」

大山愣了一下：「蛤？這也有風險嗎？」

老鼻回：「公共 Wi-Fi 誰都能連上，但安全性有疑慮，駭客就等你上鉤。」

大山心想，還好自己動作慢，資料還沒傳送出去。同時另一件令他心裡發毛的事，就是為何老鼻好像隨時都知道自己在做什麼呢？

公共 Wi-Fi 看起來方便，其實暗藏陷阱。如果駭客也連上同一個 Wi-Fi，因為雙方都在同一個未經加密的網路上，傳出去的資料就像公開的紙條，可能發生的風險：

- 駭客設置「看起來正常」的 Wi-Fi 名稱，如「Cafe_Free」，誘導使用者連線
- 若網路傳輸內容未經加密，駭客可透過工具攔截資料，竊取帳號、密碼、信用卡資訊等敏感資訊

大山說：「這也太危險了！那是不是公共 Wi-Fi 都不能用了？」老鼻表示：「其實不然。可以使用 VPN（虛擬私人網路）加密連線，傳輸資料將經過加密，即使駭客設法攔截資料，也只會拿到一堆亂碼。不過，記得要選用可信的 VPN 服務，才不會反而讓資料暴露在其他風險中。」

④ VPN 的主要功用

大山頓時感到疑惑：「VPN ？那不是拿來追劇用的嗎？」老鼻解釋，的確有些人會利用 VPN 來跨域追劇，但 VPN 最主要的用途，是用來保護在公共 Wi-Fi 或外部網路上傳輸的資料安全與隱私。例如以下 3 種情況：

- **加密資料傳輸**

  上網傳送的資料（像是帳號密碼、文件內容）會先被加密，即使駭客攔截了也無法讀取。

- **確保使用公共 Wi-Fi 時的安全**

  使用 VPN，可保護在公共場合傳輸的資料不被惡意攔截。

- **連回公司內網——遠端工作好幫手**

  員工使用 VPN，可從辦公室外安全地連進公司內部系統；就像開了一條私人的道路，只有公司內部可以通行。

大山筆記本

Q 公司用什麼 Wi-Fi 加密協定？
使用舊版的 WEP，現在已不再安全

Q 有設定訪客專用的網路嗎？
沒有，訪客也是用同一組網路

Q Wi-Fi 密碼多久換一次？
好像兩年沒換過，還貼在櫃子上

大山此時才知道，原來日常生活中常見的公共 Wi-Fi，竟然暗藏這麼多玄機；等他回到辦公室後，也要好好了解一下公司的無線網路設定。

沒想到才過了幾天，大山收到了來自老闆的緊急信件。

👉第五章：電子郵件安全——暗藏陷阱的聯絡管道

延伸閱讀

Wi-Fi 名稱（SSID）也會透露風險？

一般人以為 Wi-Fi 的名稱（SSID）只需要好記、好辨識，其實它也可能洩漏組織資訊、設備型號，甚至成為駭客攻擊的線索！

SSID 就是連接 Wi-Fi 時看到的「網路名稱」，例如：

- StarEco_WiFi
- Office_Admin
- TP-Link_123456
- FreeWifi

Wi-Fi 名稱看似簡單、沒什麼問題，但是光憑這些蛛絲馬跡，駭客就可以去推測判斷：

- 您是誰？
- 您用了什麼設備？
- 這個網路可能連接哪些內部資源？

延伸閱讀

不適當的 SSID，可能會洩漏以下資訊

① 暴露公司名稱或部門資訊

案例 GreenNGO_Admin、EcoFund_ 會計部、StarEco_POS

駭客看到這些名稱，就知道這是組織內部在用的網路，甚至能猜到哪條線是跟財務、收銀、主機相關。

這種「直接標註用途」的命名方式，等於幫駭客指路：「這邊是主系統，攻這裡就對了。」

② 顯示使用的路由器品牌與型號

案例 TP-Link_2.4G、DLink-5GHz、ASUS-RTAC86U

這些是路由器的預設名稱，會讓駭客知道使用哪個品牌與型號的設備。這些資訊可以讓駭客搭配已知漏洞，或預設的帳密做攻擊。

例如，有些品牌的某幾款型號裝置，若曾被爆出韌體漏洞，駭客就針對那些特定型號裝置大規模入侵。

③ 看起來是免費 Wi-Fi 的名稱，容易被複製或偽冒

案例 FreeWifi、Cafe_WiFi、Guest_Net

駭客可以建立一個假的 Wi-Fi 熱點，名字取得一模一樣來混淆視聽，資料就在沒察覺的情況下被攔截或竊取。

如何命名 Wi-Fi 才安全？

建議做法	說明
✗ 避免出現組織名稱或內部用途	不要用 XXX 公司 _Admin、帳務部 _WiFi 等命名，內部公務使用的 SSID 也要設定隱藏，不開放給外部搜尋
✗ 不要使用預設名稱	像 TP-Link_1234、ASUS-RT56 都應改掉
✗ 不要叫 Free_WiFi	容易被駭客複製冒充
✓ 使用中性名稱不具辨識性	OfficeNet_24、Network_Alpha 等等
✓ 不同用途分開命名（可搭配 VLAN）	如 Net_A 是內部使用，Net_Guest 是訪客用，但不要明「server」、「POS」等敏感用途
✓ 定期檢查周邊是否出現可疑 SSID	避免附近有人假冒自家的 Wi-Fi 名稱並設下陷阱

Chapter 5

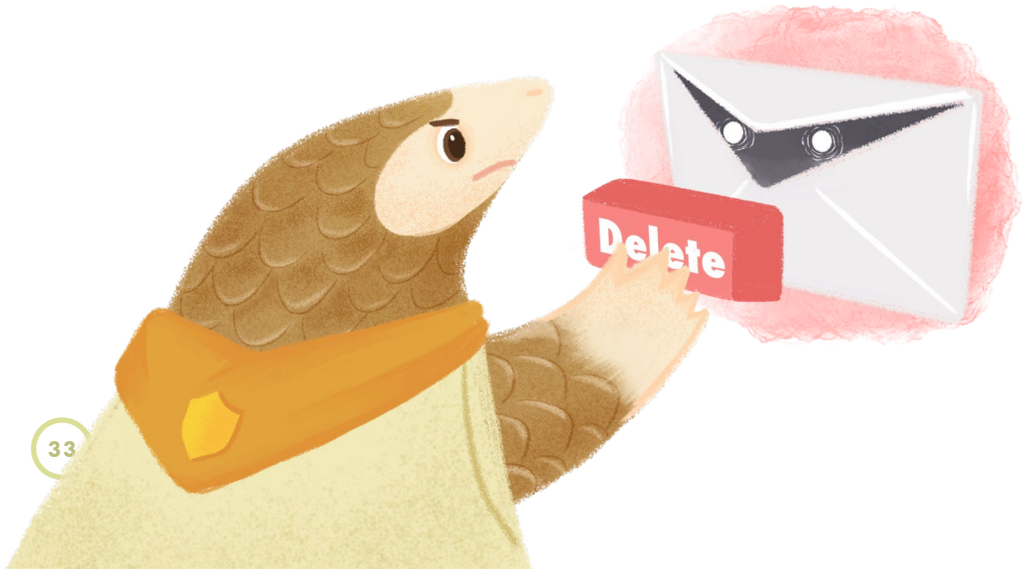
電子郵件安全——暗藏陷阱的聯絡管道

關鍵字 釣魚信件、帳號異常、委派功能

某天，大山收到了標題為「發票開錯，請立即回覆處理！」的催促郵件。寄件人顯示是老闆，信件語氣十分強硬：「這份付款文件要馬上補寄過去，否則供應商將開罰！」

一時慌亂的大山正準備打開附件，腦中卻忽然閃過老鼻的叮嚀：「語氣急迫、充滿指示的郵件，一定要提高警覺！」他停下手來，重新審視這封信，越看越覺得可疑。首先，按理應該是由會計部門處理這類通知；其次，這封郵件與老闆平常的信件格式完全不同。

就在這時，老鼻的一句話浮現在他腦海中：「讓你自願點開惡意郵件、輕鬆奪取你的資料，這就是社交工程！」



電子郵件安全實戰守則

① 開信前的資安 SOP——養成日常習慣

大山立刻跑去找老鼻：「還好你之前提醒過我，不然我差點就信了！這封信寫得太像真的了！」

老鼻點點頭說：「我們在網路上留下的足跡越多，駭客就越容易仿造出看起來『真實無比』的釣魚信件。要防範這些陷阱，最有效的方法就是建立一套開信的『SOP』。就像你剛剛那樣，一層一層抽絲剝繭地判斷與核對。」

學會判斷郵件是否為社交工程——常見手法參考

釣魚信 Phishing

說明	假冒常見單位（如銀行、IT 部門），引誘點連結或輸入密碼。多半是大量寄送，非針對特定個人。
案例	收到來自「銀行」的通知信，要求重新驗證帳戶資料，並附上登入連結。

商業電郵詐騙 Business Email Compromise; BEC

說明	假裝是老闆或合作廠商，語氣逼真，要求匯款或給內部資料。通常是量身訂做，針對特定個人。
案例	假冒合作廠商會計寄信更新付款帳號，要求匯款到新的帳戶。

惡意附件或連結

說明	寄送看似正常檔案或網址，實際內藏惡意程式或病毒，一旦開啟，可能感染整個系統。
案例	誘導點 Google Docs、 Dropbox、 PDF 內連結，實際導向惡意網站。

開信前的檢查順序

老鼻頓了頓，語重心長地補充：「有時候，危險就來自於我們太習慣『直接點』了。」於是，大山決定建立一個簡單的開信SOP：在點開任何郵件或連結之前，先停下來想一想——

檢查項目	檢視方向
☑ 寄件人資訊	寄件人是否為平常聯絡的對象？Email 地址是否可疑，有沒有拼錯，或使用奇怪的網域
☑ 語氣與內容	語氣是否急促或帶有命令、威脅，使用限時優惠等字眼，意圖製造壓力？內容是否與職務或目前狀況不符？
☑ 附件與連結	是否夾帶了未說明的附件？連結網址是否怪異、過長或非官方網域？
☑ 簽名與格式	是否缺少簽名檔、數位簽章或與過往信件格式不一致？
☑ 資訊合理性	是否有不合邏輯的情境？例如：該人目前應該不在辦公室、或通常不是由他處理這類事務？
☑ 個資 / 機密要求	是否要求輸入帳號、密碼、身分資料或開啟金融文件？
☑ 多方驗證	是否能夠用其他方式（電話、與本人核對）再次確認這封信的真實性？

小提醒：開信前多留心信件資訊，就能避開不少陷阱。認清常見詐騙手法，養成檢查習慣，是保護自己最簡單的方法。記得：可疑就別點，確認再行動！

② 聰明收發信件：善用密件副本和委派帳號

密件副本 (BCC) 不是小技巧，更是保護自己與他人的基本功！

如果直接使用「收件者 (To)」或「副本 (CC)」，每位收件人都能看見其他人的電子郵件地址。除對收信人失禮外，更可能違反個資保護原則。特別是在寄送捐款人、會員、志工、或任何團體性名單時，若不慎外洩，可能導致雙方信任受損，甚至引發申訴或法律風險。正確做法應是：

- 大量寄送時，將所有收件人放在**「密件副本 (BCC)」**欄位，保護他們的電子郵件隱私
- 可在**「收件者 (To)」**欄填入自己的信箱，避免被信件系統誤判為垃圾信

信件委派功能——讓對話都留下足跡

當客服或業務信箱只有一組帳號，卻需要由不同人處理各自範圍的信件時，最忌諱的就是共用帳密。這不僅難以控管，還容易留下資安漏洞。

這時候建議使用郵件的「帳號委派」功能：主帳號可以授權多位使用者「以該帳號身分」收信、回信，但無法更動帳號設定或密碼。

Microsoft Outlook（Exchange/365）、Gmail 等郵件平台都有類似的功能，通常稱為「委派」或「代表寄信」功能。委派功能的好處有：

- **減少共用帳密風險：**不需把密碼交給對方也能讓人代處理信件
- **可追蹤信件處理情況：**信件回覆者會顯示「XX 代表 YY 回覆」
- **靈活管理授權：**人員異動時只需移除授權無需更改主帳密碼

帳號異常，怎麼辦？

大山問老鼻：「對了，我昨天才收到 Google 提醒帳號有異常登入，這也有關嗎？」

老鼻點頭：「有些 APP 會嘗試用第三方平台連進你的信箱，如果你沒有印象有登入過，就要小心帳號被冒用了。記得要開啟雙因子驗證，並定期檢查帳號活動紀錄。而那些主流的電子郵件服務平台，通常會在以下情況發出警示通知：」

- 從新地點或設備登入
- 不是本人直接操作的應用程式（例如跳轉外部服務、連結其它 APP），試圖使用您的帳號權限去存取電子郵件內容
- 檢測到大量發信、退信、登入失敗

守護帳號安全，建議開啟以下功能：

- **使用雙因子驗證（2FA）或多因子驗證（MFA）**
- **登入通知提醒（可寄至備用信箱或手機）**
- **可疑活動報告（如 Gmail 的「最近活動」紀錄）**

大山筆記本

Q 最近有收到可疑郵件嗎？
有，收到疑似老闆寄的付款指示信

Q 是否會在寄群組信時忘了 BCC ？
偶爾會用「收件者 (TO)」，但並未特別注意

Q 是否有共用帳號處理郵件？
有，對外聯繫的電子信箱由兩人共同管理

Q 有設定兩步驟驗證嗎？
沒有，但決定今天就開啟

Q 是否使用電子郵件的委派功能？
還沒用過，準備研究看看

大山感嘆，原來不能小看電子郵件的威脅性，畢竟一封信就可能成為滲透整個公司的開端！尤其當老闆被偽冒成寄件人時，大家往往毫不猶豫就點開、回覆，甚至依照指示匯款或提供敏感資料。

下一章，大山又遇到什麼樣的突發事件呢？

👉最終章：網路身分驗證安全——收好您的數位鑰匙！

Chapter 6
網路身分驗證安全——收好您的數位鑰匙

關鍵字 密碼管理、雙因子驗證、帳號安全

「老鼻，我不是才剛換了密碼嗎？為什麼今天又收到異常登入的通知信了？」大山一臉困惑地推開老鼻的家門。

老鼻放下手邊的咖啡杯，他顯然已經習慣大山時不時闖入他家。他皺起眉頭問：「你換的密碼是什麼？」

大山有點心虛：「我家狗狗的名字，加我自己的生日。」

老鼻忍不住翻了個白眼：「你這密碼跟 123456 沒兩樣啊。駭客根本不用破解，只要猜猜就好，你的密碼是 Lucky0319 對吧？只需要在臉書上搜尋你的名字就能猜出來了。還是趕快換一組吧！」

大山一臉苦惱的說：「天哪，換了密碼還要記耶，而且這樣的資訊量組合已經是我的極限了。」

老鼻嘆了口氣說道：「還是要注意啦，駭客不一定會從技術攻擊下手，很多時候，他們只需要猜到你的帳號密碼，就能假冒你的身分，到時候可是會衍生出更多問題。」

帳號與身分驗證策略

① 什麼是身分驗證？

「帳號」就像數位世界裡的身分證。每當登入一個服務，系統會用「帳號 + 密碼」確認您是本人，這就是身分驗證。

一旦被冒用，駭客可能會：

- **偽裝成您寄出詐騙信件**
- **下載公司雲端資料**
- **竄改內部文件或設定**

② 一個密碼走天下？千萬不要！

老鼻接著說：「現在很多駭客會用你在社群上的公開資料，試著猜你的密碼。你有沒有在其他平台使用過同一組密碼？」

大山點頭：「有啊，不然我的小腦袋哪塞得下那麼多組密碼？」

老鼻一臉嚴肅：「這就危險了。如果其中一個平台的帳號被駭了，你所有的帳號也就跟著淪陷。」

大山瞬間緊張了起來：「天哪，可是這麼多組密碼我怎麼記？就算使用密碼管理工具，不是也有一定的風險嗎？」

老鼻說：「你的觀念很正確，不管是什麼樣的密碼管理方式都是有風險的！即便你用小筆記本記著，帶在身上也可能會遺失。任何管理方式都不可能做到萬無一失，只能盡量把風險降到最低。」

「話說回來，不少人為圖方便，會跟你一樣使用同一組帳密走遍天下，但只要有一個地方洩漏，駭客就可以拿同樣的帳號密碼去其他平台試試看。」

老鼻建議比較安全的做法是：

- 各系統設定不同密碼
- 每組密碼都設定到足夠的強度 (8 位元以上)
- 使用多種不同類型的字元組合，例如英文大小寫、數字、符號等
- 避免使用常見詞彙或組合模式，例如 qwerty、abcd1234、password、或其他個人資訊
- 中文輸入法的鍵盤順序作為密碼也是一種選項
- 但請不要設定如 ji32k7au4a83（注音鍵盤輸入：我的密碼）au4a83（注音鍵盤輸入：密碼）等台灣常見組合，因為這些組合也已經被駭客列入常見密碼清單內，只要一使用，很容易被猜中！

參考中文輸入法的鍵盤順序，也是設定高強度密碼的一種選項。

③ 帳號共用有什麼風險？

老鼻轉頭問大山：「你和其他公司同事之間，有共用帳號嗎？」果不其然，大山心虛的答道：「呃，我們採購系統是兩個人一起用一個帳號。」

老鼻搖搖頭：「每個人都應該使用自己的帳號，不要共用。這樣一來，如果系統發生問題，才能清楚知道是誰、在哪個環節出了問題。除此之外，共用帳號還有很多風險，你看——」

風險	說明
操作者身分難以追溯	多人使用同一帳號，難以追蹤誰進行了哪項操作，發生問題時無法歸屬責任
密碼管理風險	密碼可能隨意傳遞、抄寫、存放在不安全的地方，增加被竊風險
權限過大	共用帳號往往具備高權限（如管理者），若遭濫用或被駭風險更大
離職風險	若員工離職但共用帳號密碼未變更，前員工仍可存取公司系統

老鼻繼續說：「很多中小型組織因為人力有限，為了操作便利或降低管理成本，常會共用帳密。但是，這樣的作法容易導致權責不清與資安風險。要盡量能做到以下事宜：」

- **降低或禁止共用帳號的情況**
- **實施權限管理制度，設定不同的權限角色（如管理者、一般使用者）**
- **使用委派帳號，或其他可留下軌跡的方式執行任務**
- **確實調整或關閉帳號權限，特別是離職、職務異動人士**

④ 加一道鎖：雙因子驗證 Two-Factor Authentication (2FA)

「密碼已經更新了，至於共用帳號和權限的問題，我得再跟老闆討論看看。除了這些之外，還有什麼步驟是應該要做的嗎？」大山好奇地問。

老鼻笑了笑，像早已預料到這一問：「當然還有，你可以注意自己有沒有再加上那一道鎖——雙因子驗證（2FA）。」

老鼻接著解釋：「雙因子驗證的原理很簡單，就是輸入正確密碼之後，還要通過第二道驗證。第二道通常會是你獨有的東西，像是手機簡訊收到的驗證碼、認證信，甚至是實體的安全金鑰。這樣就算駭客偷到你的密碼，沒有這第二道認證，也無法成功入侵。」

老鼻補充：「以 Google 帳號為例，你可以在帳號安全設定中開啟『兩步驟驗證』。支援的方式很多：簡訊認證碼、備用驗證碼、甚至硬體金鑰都有。對一般使用者來說，這是最簡單又有效的資安強化手段。」

建議所有涉及重要資料的平台，都要開啟雙因子驗證，例如：Gmail、雲端硬碟、募款平台等

大山筆記本

Q 有重複使用密碼的情形嗎？
有，好幾個平台都使用一樣的密碼

Q 密碼強度怎麼樣？
過於簡單，都是自己熟悉的資訊

Q 是否啟用 2FA ？
Gmail 有，其它平台尚未設定

Q 有使用密碼管理工具嗎？
還沒，但有規劃開始使用

Q 是否有帳號共用的情況？
公司採購系統為兩人共用一個帳號

網路帳號一旦遭到盜用，駭客不僅能查看信件、刪除檔案，還可能冒名對外發信，導致客戶誤信、資料外洩，造成嚴重損失。

從設定強密碼、劃分權限，以及啟用雙因子驗證（2FA）開始，為帳號多上一道鎖，打造更穩固的防線！

延伸閱讀

雙因子驗證（2FA）與多因子驗證（MFA）的差異

雙因子驗證（2FA）的意思是：使用兩種不同類型的驗證方式來登入。常見的驗證因子驗證類型包括：

- **基於所知 (Something You Know)**
  例如：密碼（通行碼）
- **基於所有 (Something You Have)**
  例如：晶片卡、安全金鑰、智慧型手機
- **與生俱備 (Something You Are)**
  例如：指紋、面容、虹膜

而多因子驗證（MFA）則是使用「兩種以上」的驗證方式（可能是 2 種、也可能是 3 種或更多）。**因此，2FA 是 MFA 的一種，但 MFA 不一定是 2FA**。我們用以下表格來簡單舉例：

登入方式	屬於 2FA	屬於 MFA	說 明
密碼 ＋指紋辨識	✅ 是	✅ 是	基於所知 ＋與生具備
密碼 ＋ 簡訊 ＋指紋辨識	❌ 否	✅ 是	使用三種驗證方式 超出 2FA 範圍
兩組密碼 （例如網站密碼 ＋磁碟密碼）	❌ 否	❌ 否	僅使用同一類型的 驗證方式（基於所知）

– 結 語 –

從個人行動到團隊責任
成為組織最堅固的防火牆

在多數中小型組織中，資安往往不是從「有預算、有專人、有計畫」開始的。更多時候，是在某次異常事件發生後，才驚覺——原來那封信、那台設備、那組帳號密碼，都可能是潛藏的破口。

這本手冊想傳達一件事：資安，其實可以從日常的習慣、心態的轉變開始慢慢養成。

就像大山，不懂寫程式也沒關係。資安意識的建立，從來不是技術門檻，而是態度的選擇。

資安，是一種團隊默契與日常習慣

一套系統再完善，若沒人維護，也會逐漸失效；防火牆功能再強大，如果大家都用相同密碼，整個環境一樣是危機四伏。

真正堅固的防線，不只是來自工具或政策，而是來自於每一位成員都清楚：「該注意什麼，該怎麼做」，由下而上共同建立組織文化，提升資安意識。

讓我們從每一次的「多想一步」開始

- 面對自己天天在用的服務或設備時，順手檢查——
  「基本的防護設定有開啟嗎？」
- 安裝新的網路設備，記得提醒自己——
  「預設的帳號密碼改掉了嗎？」
- 在外連接公共無線網路前，問自己——
  「這個網路安全嗎？」
- 看見語意模糊的可疑信件，先停下來想一想——
  「這是真的嗎？怎麼確認？」
- 收到帳號異常時，除了重設密碼，檢查看看——
  「雙因子驗證有啟用嗎？」

從理解出發、行動落實
一起建立起屬於組織的資安文化

《資安星際指南：網路安全輕鬆學》

出版單位　國家資通安全研究院

召 集 人　林盈達

主　　編　許建榮

副 主 編　鄭瑋

執行編輯　胡馨元

作　　者　邱元貞、張恩鳳、陳思帆

審　　訂　鄭郁翰、王弘儒、陳奕穎、謝采軒、魏鈞培

設　　計　施逸青

出版日期　2025 年 9 月　初版一刷

ISBN　978-986-5436-73-5

本手冊由 Google.org 提供資金挹注「NICS 台灣資安計畫」出版

ISBN: 978-986-5436-73-5