主題	編號	常見問題	資安觀念說明	建議與應對措施
帳號管理	Q1	我的帳號好像怪怪的，密碼是對的但登不進去，該怎麼處理？	帳號無法登入的原因有很多，不一定是密碼錯了，有可能是大小寫、全半形等設定錯誤，若您經檢查密碼無誤後仍無法登入，或是其他人收到您帳號發出的異常訊息，這表示您的帳號極可能已被竊取，建議立即向平台客服反映。	如果發現密碼正確卻無法登入，請嘗試依照以下步驟進行排查： **1. 確認大小寫與全半形：** 請檢查鍵盤的 Caps Lock 是否開啟。 **2. 帳號被鎖定：** 如果短時間內輸入錯誤次數過多，系統為了安全會暫時鎖定帳號（通常是 15 分鐘到 24 小時）。 **3. 時間設定問題：** 如果你有開啟手機驗證或 App 驗證，請確認手機時間是否準確，如果手機時間與標準時間不符，驗證碼會失效。 經上述程序仍無法排除登入問題，建議透過**「忘記密碼」重設密碼**，可以強制更新伺服器上的帳號狀態。 ⚠ **安全提醒：如果你發現密碼被改過，或者電子信箱收到非本人操作的重設請求，請立即聯繫該平台的官方客服進行「帳號申訴」。**
	Q2	我懷疑帳號被盜用，經常會有不是我自己的操作或者不明的通知，該如何處理？	若您發現帳號設定被改、收到未知的刷卡驗證碼，或是他人收到您帳號發出的詐騙訊息，這表示您的數位身分極可能已被竊取，這不僅影響您個人，更可能讓駭客藉此滲透公司內部系統。	1. **立即修改密碼：**若還能登入，請馬上更改高強度密碼；若不能，請聯繫服務商取回權限。 2. **強制登出：**在設定中選擇「登出所有裝置」。 3. **啟用二階段驗證 (2FA)**：綁定手機或驗證App，增加第二道防線。 4. **通知平台客服：立即向通報平台反映**，若涉及信用卡，建議立即停卡。
	Q3	為了方便好記，密碼很久沒換可以嗎？	密碼萬年不換或設定太簡單（如123456），駭客幾秒鐘就能破解，一旦密碼外洩，駭客可長期潛伏。建議密碼應設置一定長度與複雜度，且不可與私人帳號（如FB、IG）共用同一組密碼。	1. **密碼複雜度：**建議至少15碼，混合大小寫、數字與符號，或使用密碼管理工具生成及管理密碼。 **2. 啟用二階段驗證：**如開啟簡訊驗證碼、臉部或指紋驗證，使用身分驗證器等。 **3. 定期檢視登入活動：**建議定期檢視帳號登入紀錄,透過檢視登入的時間、地點或裝置設備，檢查是否存在異常存取，如發現不明登入足跡，應立即登出所有裝置並更換密碼。
釣魚訊息防範	Q4	廠商突然寄信說換銀行帳號要我匯款，這能信嗎？	駭客為針對企業財務進行詐騙，往往會潛伏在電子信箱中觀察，最後選在請款時，冒充廠商或老闆寄信要求「變更匯款帳號」，這類信件通常模仿得極為逼真，單看Email地址很難察覺差異。	**1. 檢查寄件者：**不要只看顯示名稱，要查看詳細Email地址是否正確。 **2. 第二管道確認：**絕對不要只看Email就匯款，務必透過電話、Line或傳真向對方窗口「口頭確認」。 **3. 建立查驗機制**：超過一定金額需要有主管查驗。
	Q5	如何辨識假冒客戶資訊進行詐騙？該如何防範？	所謂「社交工程」攻擊是假借客戶資訊，更甚是利用同情心、恐懼或貪小便宜的心態，假冒身分（如IT人員、高層）騙取員工信任，進而套出資訊，或引誘業主匯款至錯誤帳戶。	1. **零信任原則：**接到要求提供帳密或匯款的電話，一律先持保留態度，先行查證後再予回撥確認。 2. **不透露個資：**正規機構不會以電話中要求您提供登入密碼或至ATM執行轉帳作業。 3. **員工演練：**定期分享詐騙案例，提高警覺。
	Q6	員工收到銀行或政府的電郵要確認資料，怎麼分辨是不是詐騙釣魚信？	「網路釣魚」常偽裝成銀行通知、包裹查詢或政府公文。特徵是會製造「緊急感」（如：不處理帳號會被停權），誘使您點擊連結進入假網站輸入帳號密碼。這是目前最常見的入侵起手式。	1. **檢查寄件者：**不要只看顯示名稱，要查看詳細Email地址是否正確。 2. **不點連結：**若是銀行通知，請自行開啟瀏覽器輸入銀行官網網址，不要點選對方來信內的連結。 3. **查證：**對於任何要求輸入個資的連結保持懷疑。
	Q7	最近常聽到的AI 詐騙，中小企業該如何防範？	AI 讓釣魚郵件更擬真，甚至能深偽（Deepfake）老闆的聲音或影像要求轉帳。	**1.雙重確認流程：**凡涉及匯款或變更受款帳戶，必須透過第二種通訊管道（如電話確認）核實，不能僅憑語音或影片訊息。 2. **查證：**對於任何要求輸入個資的連結保持懷疑。
	Q8	我們的系統都是外包廠商做的，如何選擇好的廠商？	在委外前，應先設想委外可能有哪些風險，會威脅到組織正常運作，並判斷這些風險的影響程度，以確認專案是否適合委外。	1. **慎選廠商：**簽約時可要求廠商提供資安證明（如ISO 27001）。 2. **合約規範：**在契約中明訂資安責任與賠償條款。 3. **權限控管：**不要給廠商永久的最高權限，維護結束後應立刻關閉帳號。

主題	編號	常見問題	資安觀念說明	建議與應對措施
資產防護	Q9	大家工作都很忙了，為什麼還要花時間做資安教育訓練？真的有用嗎？	資安不僅是IT人員的事，更是全體員工的責任，統計顯示，絕大多數的資安事件源於「人為疏失」（如誤點釣魚信、設弱密碼），員工是公司的第一道防火牆，有資安意識才能在第一時間阻擋威脅。	1. **定期培訓：**每半年至少一次，包含識別釣魚信、密碼保護等主題。 2. **社交工程演練：**不定期寄送模擬釣魚信，測試員工警覺性。 3. **獎懲機制：**將資安表現納入考核或給予獎勵。
	Q10	公司想把資料放上雲端比較方便，選擇雲端服務要注意什麼資安問題？	雲端雖然方便，但資安責任是「共同承擔」的，服務商負責機房安全，但「誰能看這些資料」是您的責任，若權限設定錯誤（如設定為公開），資料就會有外洩的風險。	**1. 盤點資料：**確認公司內部有哪些機敏機訊(例如公司營業秘密、特種個資資料)，並評估是否上雲。 **2. 檢查權限：**確認雲端資料夾設定為「僅限特定人員存取」，而非「公開」。 **3. 啟用防護：**開啟雲端平台提供的二階段驗證 (2FA)與加密功能。 **4. 異地備份：**雲端資料也應該在公司本地端留有一份備份。
	Q11	電腦一定要馬上更新嗎？如果使用停止更新會怎樣？	系統更新通常包含「安全性修補」，廠商發現了漏洞會釋出更新檔，若您不更新，等於告訴駭客這裡有漏洞可以鑽，這就像屋頂破了洞，廠商寄來材料，您卻不處理一樣危險。	1. **開啟自動更新：**作業系統（Windows/Mac）務必開啟自動更新。 2. **常用軟體定期更新：**常用的Office軟體、瀏覽器、甚至防火牆設備都要定期檢查更新，勿使用已停止更新支援之軟體。 3. **不要拖延：**收到重大安全性更新通知時，請優先處理。
	Q12	如何安全的使用監視器或連網設備？	許多物聯網設備出廠預設密碼都是公開的（如 admin/admin），駭客有專門的工具能在網路上掃描這些沒改密碼的設備，一旦連上，您的監視器畫面就可能變成直播秀，或設備被駭客控制。	1. **啟用即改：**設備安裝第一件事就是修改預設帳號與密碼。 2. **隔離網路：**若技術許可，將IoT設備（如攝影機）與公司內部資料網路分開連接。
	Q13	備份很佔空間又要花錢，真的有必要嗎？資料備份的重點是什麼？	備份是遭受勒索軟體攻擊後的「保命符」，不僅是勒索病毒，包含硬碟壞掉或火災等，備份是讓公司能繼續營運的唯一依靠，假如公司重要資料沒有備份，資料可能有永遠遺失的風險。	1. **備份321原則：**重要資料建議宜至少備份3份、使用2種不同儲存媒體、其中1份要放在異地（離線）。 2. **離線備份：**最重要的一點，備份硬碟備完後要「拔掉」，避免一起中毒。 3. **還原演練：**定期嘗試還原資料，確保備份檔未毀損，及備份資料之有效性。
	Q14	我們只是小公司，沒太多預算，至少要做到哪幾點基本的資安防護？	資安不一定要花大錢，有基礎的資安防護，並強化員工資安意識，只要做好基本功，就能降低資安風險，建議從軟體更新、安裝防毒軟體、密碼安全、資料備份，以及提升人員資安意識等面向優先著手處理。	1. **軟體更新：**系統與軟體隨時保持最新。 2. **安裝防毒軟體：**安裝並啟用防毒軟體。 3. **密碼安全：**注意密碼複雜度，可使用密碼管理工具生成及管理密碼，或啟用二階段驗證 (2FA)。 4. **備份：**定期備份重要資料。 5. **提升人員資安意識：**提高警覺，不點選可疑信件與連結。
	Q15	在家辦公（WFH）或外勤人員多，如何確保公司內網安全？	建議使用企業級VPN或者導入零信任 (Zero Trust)架構，並強制要求所有端點（筆電、手機）安裝防毒與資安監控軟體。	1.**遠端連線**:對於每一種允許之遠端連線，均應先取得授權，連線來源應為允許之設備，連線方式應為公司指定之方式。 2.**權限設定**:修改權限、管理帳號，必須人在公司內部（或連上 VPN 後進入特定管理網段）才能操作。 3.**加強監控**:安裝監控軟體。 4.**加密:**建議安裝企業專用VPN加密軟體，進行連線。
	Q16	導入AI代理工具（如OpenClaw，俗稱龍蝦）應如何避免成為資安破口？	AI 代理工具在提升作業效率的同時，因具備極高的系統權限與24小時自主運作特性，若未妥善設定防護機制，極易成為駭客入侵個人主機與企業網路的破口。	1.**落實環境隔離**： 應將其部署於全新、已格式化的獨立電腦，或是專屬的虛擬機或容器中。 2.**外部帳號權限最小化**： 為AI代理註冊專屬的獨立帳號（包含專用電子郵件及社群平台帳號），避免將個人日常使用的帳號與密碼直接提供給AI代理。若AI代理必須登入外部服務，建議設定具有時效性的臨時授權憑證，時間一到權限即自動失效。 3.**設置人類審核機制**：針對高風險操作（如存取憑證、發送郵件或執行系統指令），應於系統設定中強制啟用人工審核，要求每次執行前必須經由人員手動確認方可放行。 4.**親自審查Skill擴充套件**： 在安裝任何第三方技能擴充套件前，應先對其內容說明與程式碼進行完整的安全掃描。若發現內容中有要求下載不明檔案、連線至不明網站等可疑行為，應立即停止安裝並向平台檢舉，同時企業用戶應於組織內部進行資安通報。 5.**將安全守則寫入「長期記憶」**： 定期審閱且備份AI的長期記憶檔。務必將重要的安全限制（例如：刪除郵件前必須經過人員同意）直接寫入「核心記憶檔案」（如：OpenClaw的MEMORY.md）中。

主題	編號	常見問題	資安觀念說明	建議與應對措施
資安事件預防及處理	Q17	新聞常說「個資外洩」，這對我們公司到底有什麼影響？	「個資外洩」指公司的客戶名單、信用卡號、員工個資等敏感資料，被未授權者取得。這通常源於系統漏洞或人為疏失（如寄錯信）。對企業而言，這會導致商譽受損、面臨法律訴訟及高額罰款（依個資法規定）。	1. **盤點資料**：確認公司存了哪些機敏、沒必要的資料應定期刪除。 2. **權限控管**：設定誰能看、誰能改，不要全公司都能存取。 3. **加密儲存**：敏感檔案應加密保護。 4. **事件通報**：若發生個資外洩，依法需通報主管機關並通知當事人。
	Q18	電腦檔案突然全部打不開，還跳出視窗要我付比特幣贖金，這是什麼情況？	這是遭到「勒索軟體(Ransomware)」攻擊，駭客將您的檔案加密上鎖，把資料當作人質，這就像綁架案，駭客會要求支付加密貨幣才給解鎖金鑰，甚至威脅公開資料。	1. **斷網**：立刻拔除網路線或關閉Wi-Fi，避免感染其他電腦。 2. **不支付贖金**：付錢不保證能拿回檔案，且會助長犯罪。 3. **尋求專業協助**：聯繫資安公司評估是否有解密工具。 4. **還原備份**：這是唯一取回資料的解方，從乾淨的備份中還原資料。 **5. 報案**：向所在地之(縣)市檢警調報案。
	Q19	工程師說電腦有「惡意軟體」，那跟病毒一樣嗎？	惡意軟體包含病毒、勒索軟體、間諜軟體等。它們潛伏在電腦裡，有的會偷側錄您打字的密碼，有的會把您的電腦當成殭屍跳板去攻擊別人。	1. **定期檢視程式清單**：檢查「已安裝的應用程式」清單內是否有沒印象的奇怪軟體。 2. **監控效能**：注意電腦有無異常變慢或風扇狂轉。 3. **更新系統**：修補漏洞讓惡意軟體無機可乘，尤其Windows Update應即時更新。 ⚠ 電腦已有異常狀況且無法排除，建議盡快尋求專業人員協助。
	Q20	公司網站突然跑不動甚至掛掉，流量大增，是不是被攻擊了？	若網站流量瞬間暴增且來源單一，極可能是「分散式阻斷服務(DDoS)」攻擊。駭客控制大量電腦同時連線您的網站，像是一群人惡意塞爆商店門口，讓真正的客人進不來，導致服務中斷。	建議針對公司重要系統或服務要有備援機制，例如準備備用網站或以靜態頁面維持基本公告，如短時間無法排除且懷疑有遭到DDos攻擊，建議採取以下步驟： **1. 流量清洗**：聯繫您的電信商 (ISP)尋求協助，必要時啟動流量清洗服務。 **2. 保留紀錄**：記錄攻擊時間與IP，以利後續通報或分析。
	Q21	如何避免內部員工不當外洩公司資訊？	「內部威脅」往往最難防範，擁有權限的惡意員工（或離職員工）可能刪除重要資料、竊取客戶名單帶去競爭對手公司，甚至植入後門程式報復。	1. **離職即停權**：員工離職生效當下，立即停用所有帳號與門禁權限。 2. **最小權限原則**：平常工作時，只給員工「剛好夠用」的權限，不要人人都是管理員。 3. **行為紀錄**：保留系統存取日誌(Log)，以便事後追查。
	Q22	糟糕！發現電腦正在被駭或資料不見，當下的第一反應動作該做什麼？	請保持冷靜，您的第一反應決定了災損大小，就像家裡失火要先關瓦斯，發現駭客入侵首要任務是「阻斷連線」。	1. **拔網路線/關Wi-Fi**：物理性斷網，阻止駭客繼續竊取資料或加密檔案。 2. **不要關機**：若非必要建議保持開機（但已斷網），以便專家鑑識記憶體中的犯罪證據。 3. **拍照錄影**：將螢幕上的勒索訊息或異常狀況拍照存證。 ⚠ 電腦已有異常狀況且無法排除，建議盡快尋求專業人員協助。
	Q23	如果真的不幸被駭客攻擊了，接下來該怎麼處理？要報警嗎？	若已造成損失，請至台灣電腦網路危機處理暨協調中心(TWCERT/CC)進行通報，或可撥資安署專線02-2380-8500尋求免費諮詢與協助。	1. **通報窗口**：可聯繫 TWCERT/CC (台灣電腦網路危機處理暨協調中心) 尋求免費諮詢與協助。 2. **報案**：若涉及詐騙資金，撥打165反詐騙專線；若為入侵案件，向警察局報案。 3. **蒐證與復原**：保留日誌(Log)紀錄供調查，並找專業資安廠商協助清除後門與還原系統。
相關資源	Q24	政府有何種資源協助中小企業進行資安防護	政府目前已整合多元資源，協助中小企業解決在資安防護上面臨的「缺人、缺錢、缺技術」困境。	**1. 諮詢服務**：除可撥打馬上辦服務中心免付費諮詢電話：0800-280-280外，亦可使用24小時線上智能客服獲取即時諮詢服務。 **2. 學習資源**：網路大學校平台(https://www.smelearning.org.tw/class.php?course=18442)設有「資安專區」，包含基本防護、網路管理、個資保護等教育訓練影片，方便企業落實內部資安教育。 **3. 自我檢核**：資安署提供中小企業基本資安防護自檢表(https://www-api.moda.gov.tw/File/Get/acs/zh-tw/1rpP5Mb1iyZwZUF)，讓企業「自我檢測」資安現況，了解自身所需防護與急需補強的環節。 4. **免費資源**：可參考「中小企業基本資安防護指引」之附件2「中小企業資安參考資料資源區」。
	Q25	「中小企業基本資安防護指引」及自檢表可在那裡下載	提供自我檢核以落實防護，將專業的資安要求轉化為明確易懂的清單，涵蓋帳號管理、設備管理及資料備份等實務建議，讓中小企業透過自檢表進行檢核，循序漸進地建立資安基本防護。	**可至資安署官網**，首頁/資安法規專區/相關作業指引/相關作業規定及指引(https://moda.gov.tw/ACS/laws/guide/rules-guidelines/904)下載，**或至TWCERT/CC官網**，首頁/資安宣導/公開文件(https://www.twcert.org.tw/tw/lp-13-1.html)下載。

主題	編號	常見問題	資安觀念說明	建議與應對措施
	Q26	要資安健檢團來幫我的公司做健檢，我可以去那裡申請或跟誰聯絡	「資安健檢團」係委由國家資通安全研究院補助大專院校資安領域教師開設實務型資安課程，學生先接受扎實訓練，再組成投入實地服務，深入了解中小企業運作現況並提供資安改善建議。	**相關問題可洽資安院**，聯絡方式:TE-COD@nics.nat.gov.tw或電02-2380-0939陳小姐、02-2380-0941張小姐。
	Q27	中小企業有哪些可以參考的免費資安資源	針對中小企業在資安防護上面臨的「缺人、缺錢、缺技術」困境，中企署、資安署及資安院皆提供有相關免費資源，可供中小企業參考使用。	1.**中小企業網路大學校「資安刊物」參考** https://www.smelearning.org.tw/publication.php 2.**勒索軟體防護指南TWCERT/CC** https://www.twcert.org.tw/tw/cp-14-4843-7060c-1.html 3. **國家資通安全研究院推廣資源**https://s.moda.gov.tw/8WPGTuqkjD6m 4.**企業資安事件應變處理指南** https://www.twcert.org.tw/tw/lp-160-1.html 5.**中小企業資安教育訓練影片** https://www.smelearning.org.tw/class.php?course=18442