Civil Society Organizations

數位防禦手冊

注重隱私與安全的開放原始碼工具

OpenCulture
Foundation_

OpenCulture
Foundation

開放文化基金會

自 2014 年創立起，開放文化基金會（OCF）以法人組織形式支持台灣 40 多個開放科技社群，在過程中，除了推廣開放科技概念，我們也開始參與政策倡議，為眾人的數位人權發聲，進而創建了一個在台灣發展開放科技的基地。攜手科技社群與公民夥伴，我們共同努力促進台灣的數位／網路環境更加公開、透明、公眾參與 — 不論這樣的參與是以個人、社群或是組織為名義。

近年來，OCF 與科技社群協力以人才培育、工具包研發、辦理活動等方式來提升台灣公民團體的資訊安全及數位能力。透過推廣開放科技與跨界合作，OCF 將持續銜繫台灣科技社群與其他公／私領域，促成開放共創保障數位人權、支持透明涵融的數位公民社會。

網站 : https://ocf.tw
電子信箱 : hi@ocf.tw

有關本手冊

2023 年 5 月初版

2024 年 7 月再版

圖片來源

- Chrome、Safari、Microsoft Edge、Firefox、Firefox Focus、Brave、Librewolf、Tor 各瀏覽器的圖示取自維基共享資源 (Wikimedia Commons) 網站：https://commons.wikimedia.org/wiki/Main_Page
- KeePassXC 之圖片為該軟體操作截圖。
- Nextcloud 之圖片為該軟體操作截圖。

目錄

目錄

緒論

數位安全為何重要？

在幾乎所有工作都要上網的時代裡，全世界的公民社會組織 (Civil Society Organization) 越來越習慣利用數位工具進行倡議，工作環節包含日常的行政運作、內外人員的往來溝通、勸募、記者會或宣傳等。可以說，沒有網路，公民組織的工作將窒礙難行。

當工作空間從實體延伸到線上，公民組織倡議和行動的空間增加，同時也讓公民組織暴露在更多的風險和威脅之中。根據開放文化基金會 2024 年 4 月公開的研究報告[1] 指出，受訪的 35 家人權及民主倡議組織，都曾遭受程度不一的數位攻擊和威脅。每個組織除了在官網或社交平台頻繁地收到言語騷擾和威脅之外，一半以上的組織都遭受過更沉重的數位攻擊，包括監控、機密資料外洩 (如捐款人資料、服務對象行蹤等)、惡意癱瘓網路、資訊操控等，有些甚至是來自極權國家的強力攻擊，讓人難以招架！這些數位攻擊傷害了組織所倡議及保護的價值，且導致組織的員工、聲譽和資產面臨不可抹滅的損害。

倡議最重要的資產就是「人」與「聲音」；「人」指的是組織的倡議者，「聲音」指的是倡議的管道或官網上呈現的歷年成果。《CSOs 數位防禦手冊》是一本寫給公民社會組織，同時也便利人人自學的數位安全初階教科書。透過建立概念、認識威脅、了解更好的管理方式和防禦工具，幫助公民組織和人權工作者學習並應用基礎防禦知識，來保護最重要的資產。

數位攻擊通常從使用者「日常使用網路的行為」切入，協助國際公民組織和獨立記者的非營利組織 Internews 從多年協助經驗發現，只要組織與個人做好基礎防禦，即有機會大幅降低傷害，甚至避開威脅。(2024 年 3 月)[2]

本手冊主旨即是夯實數位安全能力的基本概念，針對公民組織工作過程中的四個環節：上網用的瀏覽器、工作帳號的密碼管理、資料管理及備份、官方網站的保護，分別以四個章節介紹，從概念、解方到推薦工具，讓讀者快速掌握數位安全概念。並且，最後提醒當遭遇數位攻擊時該如何求救。

---

1 https://ocf.tw/p/defendhrd/

2 https://internews.org/resource/global-trends-in-digital-security-civil-society-and-media/

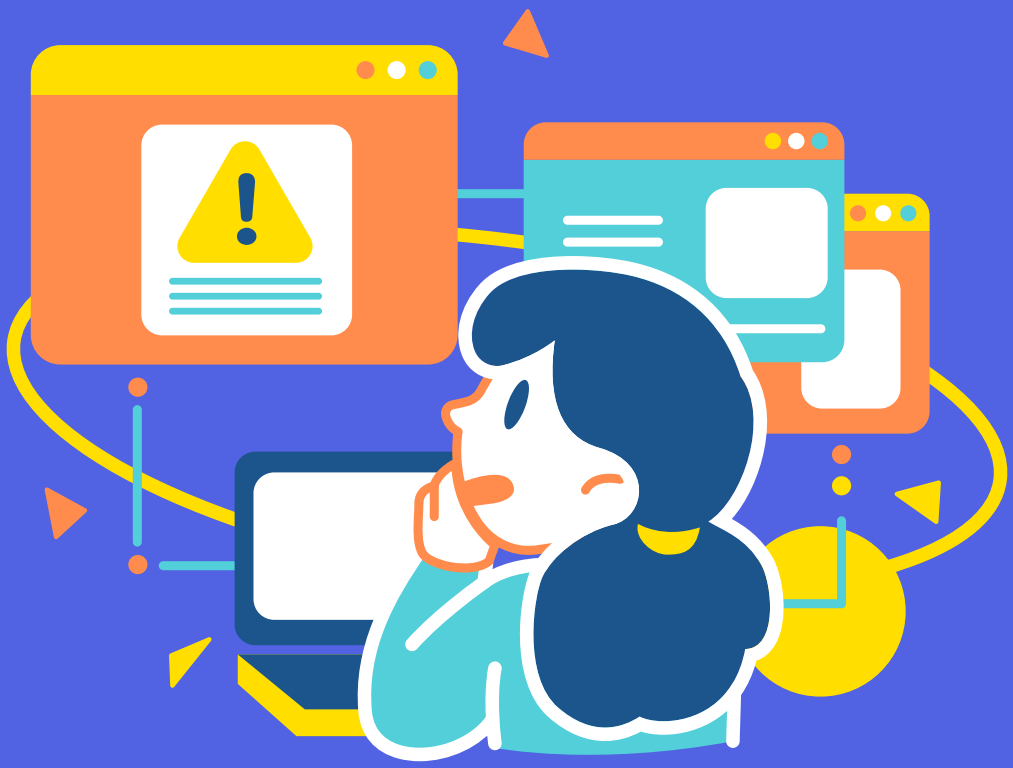
緒論

數位安全 × 開源工具

開放原始碼、開源，意思就是將原始程式碼開放出來，讓眾人看得到、能參與改善，更能監督，換言之，在程式碼都可能會有安全漏洞的前提下，開源能夠集合眾人智慧並擁有更快速修正的優勢。

程式碼與數位使用息息相關，所有的網路和數位服務都是建立在一組又一組的程式碼之上，並以此來決定如何運作 (包括攻擊、收集資料、找到地址等)。我們所知的網路和數位服務大多屬於私人商業公司，這也代表它們基於營利考量而不會公開程式碼，因此使用者，也就是你我的數位隱私和安全就會有一定程度的漏洞和風險；這也說明了為什麼有些高風險人權工作者使用社交平台會招致一定風險 —— 他們可能使用了不夠安全的社交平台，導致行蹤或個人資料曝光，甚至成為組織工作的破口。

本手冊建議的數位工具皆以開源數位工具為主，它們不僅是全球開放原始碼貢獻者的智慧結晶，更獲得資安和技術人員認可與推薦。本手冊中所提的工具皆符合三個原則：可在網路上或可信賴的平台上提供公開免費下載、很少受到商業利益的限制、開發過程更注重使用者的安全與隱私。透過這些工具，可更進一步強化公民組織工作者的數位安全。



風險評估

風險評估

科技工具普及，為公民團體帶來嶄新的工作方式 —— 倡議：可透過更便利的自媒體平台；募款：有更多元的金流串接方式接觸支持者；執行第一線工作、與他人合作或提供服務給目標群眾：可透過線上會議或虛實整合的方式。與此同時，隨數位化而來的風險，我們必須正視並為此制定管理政策。

從社群媒體、雲端裡的工作檔案到捐款人資料，我們在數位世界的每一步都留下數位足跡。就像貓咪如廁完會撥砂掩蓋氣味，以免被敵人追蹤，公民團體也需要了解如何在數位叢林中保護自己。

自我保護的第一步，是辨識要保護的資產，才能分析潛在危險以及擬定相應的風險管理機制，這就是「威脅建模」(Threat modeling) 的概念。以下將解析威脅建模的六大步驟，並以假想的組織 A[3] 為例，幫助大家理解如何為組織評估風險、建立安全政策。

步驟零 建立正確觀念

首先，我們應了解沒有「絕對安全」這回事，我們能做的是建立一套流程，盡可能確保相對安全的狀態。就像為了保護家裡的資產，你會裝設大門和門鎖，透過控管持有鑰匙的人數來掌握能進出你家的人員。這些措施雖無法保證小偷不會破門而入，至少有一定程度的安全保障。

❖ 組織 A

在制定安全政策之前，先向所有與會者宣導上述觀念，避免錯誤的期待，幫助大家聚焦於提出可操作的方法。

步驟一 釐清需要保護的目標

你最重視、需要保護的「資產」是什麼？在數位世界裡，電子郵件、聯絡人清單、捐款人資料、服務對象的個資、行程與位置等資訊，甚至是通訊設備本身，都是你的資產。先列出組織的資產，這包括保存資料、保存位置、誰有權存取這些資料、阻止其他人存取這些資料的原因。[4]

❖ 組織 A

身為救援政治難民的團體，所列資產包括政治難民的現居地址、通訊方式、遷徙管道等資料。這些資料保存在 Google 雲端資料夾，且我們所有職員與外包的合作人員習慣登入共用帳號「Staff」去存取這些資料。我們認為應限制接觸這些資料的人員，避免資料不慎外流，危及政治難民的安全。

3 為這是為了幫助讀者理解本手冊的應用方式所設定的假想組織，並非真實案例。

4 「威脅建模」也適用於保護實體世界的資產，例如組織若判斷員工的人身安全是重要資產，因此制定員工開車的最高時速限制、加強駕駛安全宣導等規則。由於本手冊以協助公民團體建立應對數位世界的風險為目標，因此威脅建模將以數位世界裡常見的威脅與防禦手段為主。

風險評估

步驟二 識別威脅來源

首先，列出的資產，思考哪一個單位 (公司、政府、民間組織) 或個人會想取得這些資產 —— 他們，就是你的「對手」。對手可能是同行競業、前老闆、前員工、駭客或先前的合作單位。若你是對抗極權政府的人道救援者，那麼政府、執法單位、特定政權的代理人或團體，都可能是你的對手。須注意的是，這份對手清單也可算是組織的重要資產，待完成風險評估，可考慮是否銷毀此清單。

❖ **組織 A**

對手包含政治難民母國的政府單位、執法部門、中介組織 (遊說團體與駭客)。這些對手想取得我們的資產以追捕政治難民。

步驟三 視覺化所有威脅的潛在後果

如果你想保護的資產遭竊，狀況會有多糟？討論並記錄對手有哪些手段可獲得這些資產。可能的手段包含誘使你點擊惡意連結，從而「釣魚」 —— 在你的電腦裡植入竊取資料的程式。對手不一定使用複雜技術，也可能透過「社交工程[5]」獲取你的信任來取得資料。

別忘了考量對手的能力，舉例來說，若你的對手是政府，它就有能力向電信商取得通聯紀錄。此外，須思考並寫下對手會拿這些資產做什麼事？會帶給組織什麼危險？盡可能寫下各種可能的後果，有助組織設想可能發生的各種狀況。

❖ **組織 A**

對手可能滲透到外包組織以取得帳號 Staff 的密碼，藉此取得政治難民個資，導致政治難民行蹤曝光。

5 社交工程：社交工程是指在資訊安全方面操縱人的心理，使其採取行動或洩露機密資訊。

風險評估

步驟四 評估資產保護程度

我們接著要評估步驟三梳理出的壞事發生機率有多高？我們願意承擔這些後果嗎？這牽涉到主觀判斷，舉例來說，公民團體可能面臨的情境分為：

- 機率低但代價高：人權工作者至極權國家出差，被當地政府逮捕的機率雖低，可一旦發生，組織失去人才的代價高昂。
- 機率高但代價低：辦公室裡四散著合作對象的名片，不過，名片的資訊敏感性低，即使被揭露也不會帶來重大危害。

逐一判斷所有威脅發生的機率，討論這些威脅是值得嚴陣以待，或太過罕見、相對無害而毋需擔心。

❖ 組織 A

儘管步驟三推估後果的發生機率不一定高，可一旦發生，將危及政治難民的人身安全，代價慘重，因此我們判斷須極力保護資產。

步驟五 決定願意付出的保護成本

務實的安全策略在於能在便利性與成本之間取得平衡，舉例來說，為了追求極致的安全而在家門安裝數十道門鎖，還加裝保全系統，每月的保全支出所費不貲，結果家人嫌回家開鎖太久太麻煩，每天只上一道鎖就出門 —— 顯然這項不便、財務負擔沉重的安全措施並不適合你。

請寫下能降低威脅發生機率或減輕損失的方法，同時考量你的財務、注意力、能力等資源限制，找到組織成員都能認同且做得到的方法，才能真正落實安全策略。

❖ 組織 A

我們決定犧牲一點便利性，要求每位職員使用自己的帳號，不再開放共用同一組帳號密碼，以便清楚管理每份資料的索取權限；同時制定權限分級制度，僅賦予專案相關職員使用資料的權限，組織外成員須經申請獲准才有權限。這項決議符合大家的能力（每位職員都熟悉雲端協作），也不會造成額外的財務負擔，具可行性。

風險評估

步驟六 找到互助同盟

建立數位安全空間是一項團體活動，不只因為合作力量大，也因為合作網絡中的任一方若被擊垮，最終也會禍及自己。從合作網絡裡開始檢視，尋找有哪個團體或個人面臨與你類似的威脅，或保護相同的資產。

可以與面臨類似威脅的團體(或個人)協議互助，作法可以是共享資訊(例如潛在對手和威脅手段的清單)、共享資源(例如一起出資聘請資安講師)，幫助彼此降低成本、提高安全意識與強化組織韌性。

❖ 組織 A

組織 B 因提供政治難民暫時居住所而與我們往來密切，因此我們決定與其共享對手和可能威脅方式的清單，幫助組織 B 掌握威脅來源、建立安全政策。

定期重新評估風險，經常複習安全政策

新的風險與威脅隨時會產生，組織也可能因為新舊成員交替而有不同使用習慣，因此要記得定期評估風險，確保組織針對眼下須保護的目標制定合宜的安全流程。同時，也要讓舊職員複習、新員工了解安全政策。

❖ 組織 A

規定新進員工須閱讀安全政策，全員年末時一起檢視風險評估流程，確保彼此對守護的資產、願意付出的成本有共識。鼓勵職員提出疑慮，例如有人怕忘了自己的帳號密碼，索性用便利貼記錄貼在電腦上，這對於不時有訪客且與其他團體共用辦公空間的我們來說，不啻於隨處放置資料庫鑰匙，因此判斷須修正安全政策，禁止此類作法。

個案故事

個案故事

為什麼重視風險並開啟威脅建模、數位防禦之路，是這麼重要呢？本章節繼續用組織 A 為例，邀請你化身為組織 A 的職員 —— 小明來看看日常行為中數位風險都在哪裡。

現在　完蛋了！我們搞砸這些事……

組織 A 這段時間密集籌備救援一群被 C 政府迫害的政治難民，不僅與其他團體合作安排好救援路線，也找好安置這群人抵達台灣的暫住所。為了籌備所需資金，組織 A 自行架設網站，發表報告揭露政府 C 令人髮指的人權侵害行徑，獲得不少民眾重視，也募集到許多善心人士匿名捐款。

怎料，在啟動救援的前一天，救援路線上出現了政府 C 的執法單位；安排好的暫住所被惡意潑漆。救援對象嚇得隱匿行蹤，提供暫住所的單位因備感威脅而終止合作。組織 A 的救援任務徹底失敗，甚至小明隱約感覺自己在上班途中被跟蹤，他驚慌失措地跑到附近的派出所後，看到跟蹤者離去的身影。

雪上加霜的是，網站遭受「分散式阻斷服務」(DDoS) 攻擊，使網站無法瀏覽。原來，C 政府動員支持者同時大量連線至組織 A 網站，以耗盡網站的系統資源。小明想改用其他方式發布報告，卻發現網站上的報告消失了！他與同事線上協作的成果不翼而飛，而存有初版報告的筆電因當機而無法取回資料；另一方面，捐款人打電話向組織 A 抗議自己的捐款個資外洩，政府 C 威脅要對其在 C 國經商的家人不利。組織 A 不僅失去支持者信任，也失去對外發聲的管道，辛苦累積的報告更成泡影。

小明與同事抱頭痛哭，不僅憂慮自己的安全，更是為了無法完成對難民的協助感到難過。他不禁對天大喊：「神啊！到底哪裡出錯了啊！？」此時，一位神明從天而降，表示願意帶讓小明回到過去來看到哪裡出錯了，也許能幫助他們面對現在正發生的組織危機。

個案故事

回顧過去 事情是從哪裡開始出錯的？

借助神威，小明的視角回到事發前一個月的某天。

一如往常，小明打開綁定個人帳號的導航地圖 Nono Map[6]，點開儲存好的住家與辦公室地址，讓系統安排路線與銜接的公車班次。謹守組織 A 安全政策的小明，遵守不使用組織共用帳號 Staff 的規定，以自己的工作帳號登入 Nono Drive 雲端硬碟，閱覽救援對象的資料。

小明點開 Nono 瀏覽器，快速鍵入那組萬用密碼 —— 為了避免忘記帳密，小明向組織 A 登記自己的個人帳號為工作帳戶，繪圖軟體 Canva、專案管理工具 Trello 等帳戶也都設定相同的帳號密碼。順利登入帳戶後，小明整理了預計救援的路線。當然，他也用同一組帳密登入同事小美用免費網站架設平台 Woodless 所設立的網站後台，最後確認完成政府 C 劣跡斑斑的迫害報告。

遙想撰寫這份報告的過程，小明帶著筆電勤跑各處，訪問學者、迫害事件見證人與各種利害關係人，耗費數月，終於將這些珍貴素材整理成條理清晰、豐富又扎實的報告。接著，他從筆電將這份報告上傳到 Woodless 草稿區，以便同事線上編修。兩週來，他跟同事反覆修改，今天終於編修完成，發布上線。鬆了一口氣的小明，決定在 Nono 瀏覽器上點開新分頁，用 Nono 搜尋引擎尋找免費小說網站，打算沉浸在小說構築的奇幻世界一陣子，犒賞自己這段時間的辛勞。

「好討厭，只不過想休息一下，怎麼又看到某國際人權組織的募款廣告？」這陣子不管是滑臉書還是看網購，那個組織下的廣告總是冷不防跳進視線，搞得小明覺得自己一直沒下班，精神疲勞持續累積，現在，這幅廣告又蓋版了自己找到的小說網站。

不過，另一件事馬上讓小明分心：「真奇怪，為什麼跳出『不安全連線』的警告？」看到網址列左方的鎖頭符號被槓上一條紅色斜線，小明感到困惑。轉念一想，不過是看個小說，礙不著別人，不用大驚小怪吧！他用自己的萬用帳密在這個網站建立帳戶，觀看會員才能讀的小說內容；為了下次更快登入，他將這個頁籤加入「我的最愛」，也同意 Nono 瀏覽器記憶帳密。

「真是人性化的設計啊！」小明心想，這樣連輸入密碼的時間都省了，讚！

到了下午，小明按照 Nono Map 的路線規畫，去拜訪提供救援對象抵台暫住所的組織 B，實際參訪空間布置與生活機能。拜會到了一個段落，他分神看了手機訊息，同事來訊告知網站上顯示已有數筆匿名捐款。感受到自己的志業有他人支持，小明深受感動，相信在群眾支持下，一個月後的救援行動必定能募得足夠資金，按計畫順利進行，助這批政治難民安心在台灣開啟新生活。

---

6 為了敘事方便，本篇故事使用的數位服務皆為虛構。

個案故事

上帝視角　「對手」到底耍了什麼手段？

「嗯？這不就我一天的日常，我有做錯什麼嗎？」小明依舊困惑，更顯得慌張。

「還記得你的組織在評估風險時討論過的威脅來源，也就是『對手』嗎？」神明沉吟半晌，開口說道：「這次，我讓你回到一個月前，看看這些對手做了什麼事，幫助你找到答案。」

為了干擾組織 A 的救援行動，政府 C 命令仰賴其市場的 Nono 集團鎖定組織 A 的 IP 位址，命其交出組織 A 的所有數位足跡紀錄。透過長期的追蹤與分析，政府 C 逐漸比對出接觸政治難民的工作人員，小明正是其中之一。政府 C 拼湊小明個人與工作帳號所查詢的資料、地圖搜尋紀錄與移動軌跡等資訊後，小明的數位輪廓清晰到可鎖定他的上下班路線。

當小明登入免費小說網站並讓 Nono 瀏覽器記憶帳號密碼時，政府 C 不費吹灰之力就拿到小明的帳密，並用這組帳密成功取得救援政治難民的所有資料。再比對小明的地圖搜尋紀錄後，政府 C 找到此次救援行動的接應路線與暫住所。

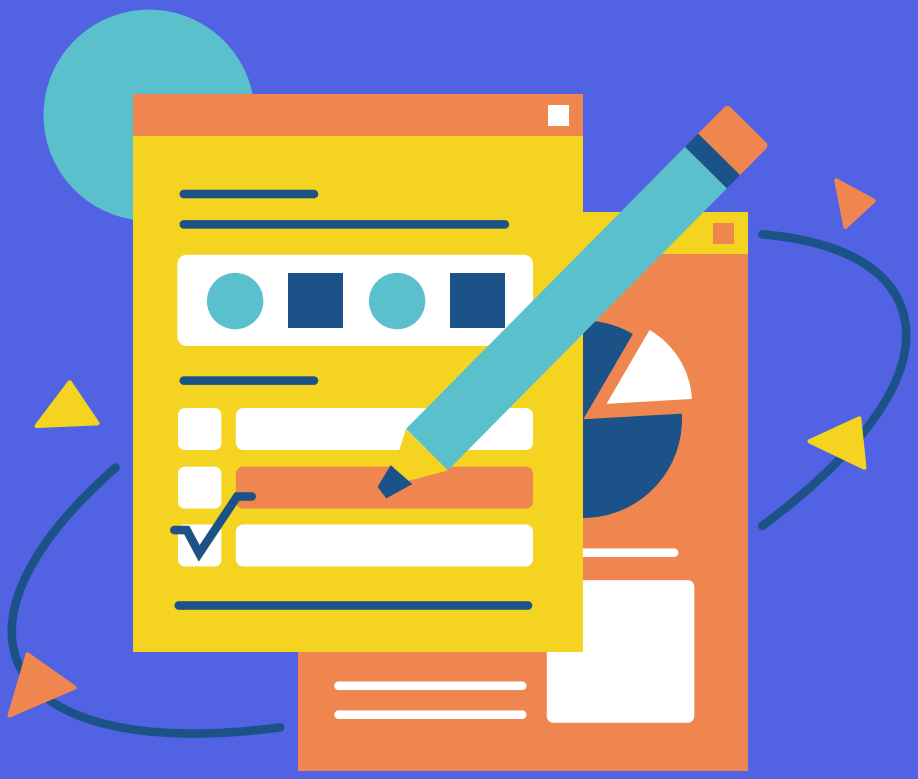
為了讓組織 A 難以東山再起，政府 C 雇用駭客，發動 DDoS 攻擊以癱瘓組織 A 的網站，讓民眾無法再捐款或閱讀指控政府 C 的報告；針對組織 A 使用 Woodless 架設的網站，駭客抓到組織 A 加裝免費外掛裡的漏洞，堂而皇之進入網站後台，一舉刪除報告、竊取所有捐款人的資料。

從頭來過，該怎麼避免重蹈覆轍？

「我究竟該怎麼做，才能避免發生現在的災難？」儘管看到過去和全貌，畢竟小明沒有超級英雄的設定，不知道如何挽救錯誤是很正常的。

「為了防止世界被破壞，為了守護世界的和平……咳！」神明從空中變出了一個捲軸，遞給小明並大發慈悲地說：「回去好好修練此天書，我把所有秘訣都寫在裡面了，也許還能給你們一線生機！」

現在，跟著小明一起開始走上學習之道吧！



前　　測

前測

小明和組織 A 的故事令你震驚嗎？也許你覺得小明是因為太倒楣才遭遇不幸，但用〈風險評估〉一章的例子來說，若平時就放任家門敞開，家裡本就有更高機率遭歹徒闖入，因此我們不能認為小明的悲劇只是特例，不會發生在自己身上。

為了讓這趟學習之旅更有效率，我們將小明遭遇的各種情境拆解成下列題目，邀請你拿起紙筆，記錄你的行動與選擇。請按照你的習慣作答，這有助於你了解自己後續應該加強哪個面向的數位安全。

瀏覽器使用習慣

1. 下列哪些描述符合你的使用習慣？（可複選）

- [ ] 我在工作跟私人生活都使用同一台電腦，或是使用同一支手機。（1 分）
- [ ] 無論是上班還是下班時間，我習慣使用同一種瀏覽器做網路搜尋。（1 分）
- [ ] 我習慣使用個人帳號處理工作事務。（1 分）
- [ ] 我清楚區分工作帳號和個人帳號，不用個人帳號收發工作信件。
- [ ] 為了方便同事快速取得資料，我使用公司的公用電腦處理文件時，通常不會登出自己的工作帳戶。（1 分）
- [ ] 在外面使用陌生的電腦時，我會開啟無痕瀏覽模式，並在結束使用時登出我的帳戶。

2. 請問你在選擇使用瀏覽器時，會做以下評估嗎？（可複選）

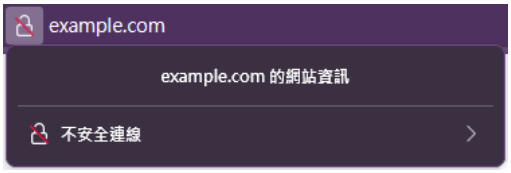
- [ ] 我看重瀏覽器性能，例如介面簡潔好使用、加載資料快、支援我同時開啟很多分頁，這是我評估是否使用此瀏覽器的主要考量。（1 分）
- [ ] 我會尋找較能保護我隱私的瀏覽器，例如能阻擋廣告、清除數位足跡。
- [ ] 跨平台同步功能對我來說非常重要，我需要在不同裝置間同步書籤、密碼和設置。（1 分）
- [ ] 我偏好使用開源瀏覽器，因為其源碼的透明度讓我更安心。

前測

3. 我們每天瀏覽很多網頁，使用滑鼠捲動頁面點擊，或是動動手指在螢幕上勾選，可能已變成無意識的動作。現在請你回想一下，**當朋友用 LINE 傳給你一個網頁，你點開對話框後的下一步會是什麼？**

- ☐ 從 LINE 的對話框點擊網址，進入該網頁。（1 分）
- ☐ 複製網址，打開瀏覽器，將網址貼到瀏覽器後進入網頁。

4. **當你點進頁面，看到網址列左方出現一個鎖頭被槓掉的圖示。不過，網頁沒跳出其他警告，網頁也能繼續瀏覽。你接下來會做什麼呢？**



- ☐ 繼續用平常使用的瀏覽器看網站。（1 分）
- ☐ 點開無痕模式，或是換一個以保障隱私著稱的網站。會特別注意不在瀏覽此網站時輸入任何個資，並在瀏覽完畢後馬上關閉該網站。
- ☐ 馬上關閉網頁，不看了。

5. **當你正要開始瀏覽網頁，網頁下方跳出一則訊息遮擋住你的視線，逼迫你馬上選擇，否則無法繼續瀏覽網頁。你會怎麼選呢？**

- ☐ Cookies 是什麼？左邊都亮出白色提示我按下去了，當然選左邊！（1 分）
- ☐ 點右邊，多花幾十秒看看我可以怎麼管理 Cookies。

如果你在「瀏覽器使用習慣」這部分的分數超 5 分，強烈建議你好好研讀〈數位足跡的基本防禦：開源與安全的瀏覽器〉一章，建立安全的使用習慣。

前測

密碼管理

1. 不管是個人娛樂、購物，還是工作上需要使用的軟體，每個服務都要你設立帳戶。你都怎麼記下這些密碼？（可複選）

- ☐ 一組萬用密碼行走江湖，只要開新帳號都用這組密碼。（1 分）
- ☐ 隨身攜帶記事本，帳號密碼寫在上面。老派方法不僅浪漫，也防止密碼被駭客取得。（1 分）
- ☐ 用便利貼記錄密碼，再將便利貼黏在電腦螢幕或辦公桌上，需要時瞄一眼。（1 分）
- ☐ 因為密碼太多組了，實在記不起來，所以存放在密碼管理器裡。
- ☐ 我都設定不登出，如果被該服務強制登出，只要按下「忘記密碼」，使用該服務自動發配的密碼就好。（1 分）
- ☐ 我對自己的金頭腦很有自信，每一組帳號密碼都存在我的腦袋裡。（1 分）
- ☐ 瀏覽器很貼心，都會問我要不要儲存密碼，我就讓瀏覽器記憶，即可自動輸入密碼。（1 分）

2. 你正要下單購買演唱會門票，結果在結帳前的最後關卡，系統要求你註冊會員。快速鍵入基本資訊後，你會怎麼設密碼呢？

- ☐ 當然是用我的萬用密碼，走到哪用到哪，此生忘不了。（1 分）
- ☐ 使用 12 字元以上的字串，就算使用有意義的單字也沒關係，長度夠比較重要。

如果你在「密碼管理」這部分獲得超過 4 分，強烈建議你好好研讀〈一次保管所有的密碼：密碼管理器〉一章，建立安全的使用習慣。

前測

網站管理與維護

1. 你的公司有自己架設的網站嗎？或是有委託他人架設，但由自己維護的網站嗎？你們通常是怎麼使用、維護這個網站呢？(可複選)

- ☐ 每位同事都有進入網站後台的權限，方便大家各自更新要放上網站的內容。(2 分)
- ☐ 我們有討論過網站可能會遭遇什麼樣的攻擊，可是由於不知道能怎麼應對，始終沒有擬定應對方案。(1 分)
- ☐ 定期掃描網站的安全性，檢查是否埋有程式漏洞。
- ☐ 因為沒有遇過網站被攻擊的問題，大家沒有討論過應對方案，船到橋頭自然直。(2 分)
- ☐ 我們有蒐集可靠的資安專家名單，遇到自己無法解決的問題時，可以向他們求助。

2. 為了方便使用，網站或多或少會安裝一些第三方外掛程式。請問你的公司在選擇使用外掛程式時，會做以下評估嗎？(可複選)

- ☐ 查詢是否有人回報外掛程式的安全問題。
- ☐ 向資安專家諮詢外掛程式是否值得信任。
- ☐ 查詢外掛程式的更新頻率與維護紀錄。
- ☐ 公司沒有這個要求，功能符合需求即可使用。(1 分)
- ☐ 因為不具備評估安全的專業與資源，故無法評估。(1 分)

如果你在「網站管理與維護」這部分獲得超過 4 分，強烈建議你好好研讀〈保障公民團體自建網站的安全〉一章，建立安全的使用習慣。

前測

資料備份

1. 你多久進行一次重要資料 (例如工作文件、個人照片) 的備份？

- ☐ 我有定期備份的習慣 (例如固定每週、每月)。
- ☐ 我有在資料搜集到一個段落時備份的習慣 (例如報告完成到一個版本的進度時)。
- ☐ 有想到、有空時會備份。(1 分)
- ☐ 沒有資料備份的習慣。(2 分)

2. 如果你主要使用的電腦或手機突然陣亡，你能恢復大部分或全部的重要資料嗎？

- ☐ 可以，我最近有做資料備份，能恢復到最新版本的檔案。
- ☐ 我只能恢復部分檔案，因為我的備份資料不是最新的。(1 分)
- ☐ 不能，我平時沒有備份的習慣。(2 分)

3. 你在做資料備份時，會怎麼進行呢？
如果你從未做過備份，試著假想你要備份資料時，會怎麼做。

- ☐ 資料存放在電腦的不同資料夾內，若原資料夾打不開，就去另一個資料夾拿檔案。(2 分)
- ☐ 檔案一份存電腦、一份存雲端空間 (例如 Google Drive、WordPress 後台)，互為備援。(1 分)
- ☐ 檔案存一份在自己的電腦、一份在 USB，以備不時之需。(1 分)
- ☐ 檔案存一份在電腦、一份在雲端空間、一份在 USB 或外接硬碟。

如果你在「資料備份」這部分獲得 1~3 分，代表你有基礎的備份知識，但還不夠周全；如果你獲得 4 分以上，強烈建議你好好研讀〈做好備份 321，不再擔心資料遺失〉一章，建立安全的使用習慣。

單 元 課 程

數位足跡的基本防禦
開源與安全的瀏覽器

01 數位足跡的基本防禦：開源與安全的瀏覽器

案例 你知道在個案故事裡，小明有哪些風險是因為瀏覽器使用習慣而造成的嗎？想好之後，再往下對答案喔！

答案：

★ 小明的工作帳號和個人帳號都使用同一台筆電、同一個瀏覽器，也沒有設定不讓瀏覽器記憶自己的搜尋紀錄，所以小明工作時查詢的紀錄，讓廣告商判斷他對人權議題有感，因此小明進行私人的購物、娛樂等搜尋時，會讓他看到與工作相關的廣告。

★ 承上述使用習慣，小明使用同一個瀏覽器開發的導航服務，因此同網路集團得以掌握小明每日通勤路線、工作查訪地點。

★ 小明在免費小說網站建立帳戶，讓瀏覽器記住自己的帳號密碼，帳號密碼儲存在瀏覽器內不是安全操作，帳號密碼資訊容易外洩或遭惡意擷取。

★ 免費小說網站沒有 HTTPS 加密連線，他在此瀏覽、輸入的內容 (包含登入頁面時的密碼)，很容易在網路傳輸過程中被人看光光。

透過小明的故事可以了解，無論生活或工作，瀏覽器就是我們在電腦、手機裝置造訪各式網站時的交通工具，數位安全自然成為評估瀏覽器的重要項目。

概論

瀏覽器就像我們通往網路世界的「門戶」，我們使用瀏覽器進入網路世界搜尋資料、與人交談甚至觀看影片；同時，現代的網站也盡其所能地收集使用者資訊，用以賺取廣告利潤，這不僅是行之有年的商業行銷基礎功能，有些不安全、惡意的網站，甚至會側錄使用者輸入的敏感資訊，或是竊取瀏覽器已經儲存的瀏覽紀錄、帳號密碼，藉此進行數位攻擊。以下是幾個使用瀏覽器必須注意的威脅或風險：

1. Cookie，背後是大大的隱憂
什麼是 Cookie？

Cookie 在這裡並非指餅乾，而是一種會將存取該網站的使用者資訊加以記錄，並儲存在電腦或手機瀏覽器中的機制。

圖： 網站詢問是否開啟 Cookies

為何大部分網站只要輸入一次帳號密碼，之後就可以不用再頻繁登入？為了避免使用者每次登入同一網站都要重新輸入個人資訊的困擾，現在絕大多數網站會使用 Cookie 技術。當你首度造訪網站，通常會被詢問是否開啟 Cookie，如果同意，代表使用這個網站會讓你的各式資訊被記錄下來。

這個技術就像沿路撒餅乾 (Cookie) 屑記錄你的足跡，並將使用者登入網站的帳號資訊、購物車清單、去過哪些網站的瀏覽紀錄，甚至是上傳的圖片、影音檔案，全部暫時存放在瀏覽器軟體於電腦裡的某個資料夾。。

Cookie 相當方便，但它也可能被濫用，例如你的網站瀏覽紀錄，會成為廣告商了解你的依據，包括最近去過哪裡、需要什麼、使用過哪些網路服務。可能你只是搜尋了一次「蘋果電腦」，接下來所有你在網站看到的廣告都會問你是不是想買電腦、要不要買更多周邊產品？如果 Cookie 未加密，駭客甚至可以輕易地利用你的 Cookie 偽造身分登入服務。

2. 數位指紋追蹤技術 (Browser fingerprinting)：
偷聽對話的手機、偷窺生活的網路

什麼都還沒輸入，但是網站已經知道你的位置、語言、正在使用的裝置？

當你使用瀏覽器，瀏覽器就能得知你使用的特定裝置資訊、作業系統、瀏覽器、螢幕大小、時區、字體、語言等資訊 —— 這一整組資訊成為每個使用者的數位指紋。許多廣告商會使用追蹤器蒐集網站使用者的數位指紋。數位指紋追蹤技術比 Cookie 更過分的是，它甚至未徵詢你的同意就不斷記錄上述資訊。

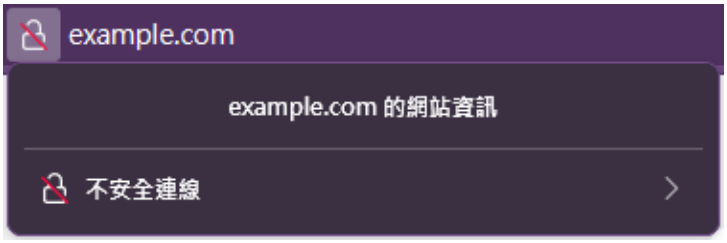
現在有許多網站，它們同屬一家公司，或是不同公司基於某些合作協定，可彼此分享使用者資料。例如 FB 與 IG 都屬於 Meta 公司，或是 Google 搜尋引擎與 Chrome 瀏覽器同屬一家公司。你瀏覽過的網站越多，追蹤器越能比對你的數位指紋 (使用者的特定裝置和瀏覽器特徵) 與 Cookie (去過的網站及瀏覽內容)，廣告商對你的認識也就越多。這些資訊讓廣告商能對你精準投放更可能說服你的廣告，若政府或極權組織透過公權力獲取了異議人士的數位指紋等資料，也就能鎖定他們的網路身分，並進一步推敲出真實身分與位置。

3. HTTP v.s. HTTPS 一字之差，風險暴增

當你瀏覽網站時，儘管網站會收集你的 Cookie 或數位指紋追蹤，然而，現在大部分網站都是 HTTPS，S 是 Secure 的縮寫，表示網站具加密保護，也就是說你只讓網站方能夠知道你在那裡進行瀏覽，網路上其他陌生人不會知道。

而沒有加密保護的 HTTP 網站，你只要一連上，就如同立即同意開啟網路直播鏡頭、打開擴音般，在網路上廣播你的各種動作與資訊，數位容貌一覽無遺。這種無加密保護的網站，就有可能讓你在網路世界曝光，除了你以外的任何人都可以大肆蒐集資料之外，更有入侵電腦、監視你生活的可能。

如何辨別這樣的網站呢？你在瀏覽網站時，有時會收到不安全連線的警告，網址左方會顯示鎖頭被劃掉的符號，如下圖：



圖： HTTP 未加密警告示意圖

這表示該網站與你的連線過程沒有提供加密保護，若繼續連線到這種沒有加密保護的 HTTP 網站，在網站上的瀏覽行為、輸入內容、滑鼠移動位置、輸入的帳號密碼或金融資料，等於毫不遮掩地分享給網路上的任何人 —— 可能是在同一間會議室、教室、咖啡廳、機場中使用同一個 wifi 的其他人，其中如有不懷好意者，他們不費吹灰之力就能拿到你的資料，然後不當利用。注重安全及隱私的使用者絕對要避免上述情形，因此最好要在瀏覽器就強制開啟 **HTTPS**，才能保障傳輸過程有加密保護，不至於因一次疏忽，使關鍵資料外流。

可用工具

市面上瀏覽器非常多樣，了解並挑選一個符合自己需求且注重隱私與安全的瀏覽器，是非常重要的事情。我們來看看如何挑選適合自己的瀏覽器吧！以下是台灣常見的瀏覽器選項：

Google Chrome	Safari	Microsoft Edge	Firefox
最多人使用的商業瀏覽器	蘋果電腦內建軟體	Windows電腦內建軟體	非營利組織開發的軟體

從小明的案例來看，輕忽瀏覽器的安全性，輕則個人資料被網站收集、使用者的數位足跡遭洩露，重則導致帳號、密碼、金融資訊被竊，甚至瀏覽畫面、傳輸的對話內容被監控。

如同在路上跑的交通工具，速度快並不代表安全，最多人用的瀏覽器也不見得適合須注重安全與隱私的公民團體。為了讓公民團體從瀏覽器的使用就具備基礎數位防禦能力，本節介紹幾個格外強調隱私與安全的瀏覽器，它們都符合開放程式原始碼的規範，所有使用者都可以看見程式背後運作的規則，一方面可供所有人檢視其運作漏洞，另一方面也讓使用者可按照自己的需要改造出不同功能的版本； 尤其是Firefox、LibreWolf、Tor 都是非營利組織或網路社群志工開發並維護的軟體，它們相對不受廣告利益的限制，並且專注於保護使用者安全。

另外，Chromium 是 Google 為發展 Chrome 所釋出的開源軟體，以 BSD 授權條款等數種授權發行，有開放其核心供其他廠商開發出基於 Chromium 的瀏覽器。

以下是幾個較注重隱私與安全的開源瀏覽器：

Firefox	Brave	LibreWolf	Tor	Chromium
非營利組織開發的軟體	強調隱私的商業瀏覽器	由志工開發維護的非營利軟體	由志工開發維護的非營利軟體	Google 為發展 Chrome 釋出的開源軟體

瀏覽器功能一覽表

如何在使用便利性和隱私安全之間取得平衡呢？ 若以公民組織希望資訊不外洩、不被惡意監控作為準則，那如上所述，嚴格挑選瀏覽器是極為重要的。以下是就目前市面上所知瀏覽器，與本手冊推薦瀏覽器的功能比較表，可幫助大家選擇自己通往網路世界要走的大門：

	保護並能在關閉時刪除 Cookie	嚴格阻擋指紋追蹤	強制使用 HTTPS 加密	特點
Firefox	有	有 (須自行開啟)	有	• 非營利 • 更新快速 • 有隱私權與安全擴充套件可使用
Brave	有	有	有	• 更新快速 • 使用 Chromium 的核心技術 • 內建擋廣告套件
Librewolf	有	有	有	• 社群維護 • 內建各式擋廣告追縱的套件
Tor	有	有	有	• 非營利 • 為美軍情報人員使用而開發，加密性特別高，完全隱蔽追蹤與使用者身分。 • 不適合一般日常生活情境使用，因無法瀏覽大多數網頁。
Mullvad Browser	有	有	有	• 基於 Tor 瀏覽器、不須要有 Mullvad 自家的 VPN[7] 也能使用。 • 附帶預先安裝的 uBlock Origin[8] 和 NoScript[9] 擴充功能
Chrome	無 僅可封鎖第三方 Cookie	無	有	• 最多人使用，駭客的熱門目標 • 更新快速
Safari	無 僅可阻擋第三方 Cookie	有	無 【提示連線安全 (HTTPS)/ 不 安全 (HTTP)】	• macOS 作業系統內建 • 內建智慧防追蹤功能
Edge	有	無	無 【提示連線安全 (HTTPS)/ 不 安全 (HTTP)】	• Windows 作業系統內建 • 使用 Chromium 核心技術

註：本表製作時間為 2024 年 3 月，瀏覽器會定期更新，各瀏覽器詳細資料請翻閱其公開資訊。

7 VPN 為虛擬專用網路，可加密網路流量並隱藏 IP (網際網路通訊協定) 位址，以防止第三方窺探或蒐集資料。

8 uBlock Origin 為一個自由、開源、跨平台的內容過濾瀏覽器擴充套件，可以為使用者移除廣告和網站追縱，並提供可以自行實施設定過濾的選項。

9 NoScript 為一個自由、開源的瀏覽器擴充套件，可以白名單選擇性執行 JavaScript、Java、Flash、Sliverlight 以及其他外掛程式和指令碼內容。

小撇步

每一個廠牌的瀏覽器使用上幾乎大同小異，任何人都可以輕易上手，而提高數位防禦能力的關鍵在於瀏覽器的內部設計，以及個人使用方式。以下有幾個小撇步，幫助你養成瀏覽器使用的好習慣，讓你出入網路更加安全：

1. 盡量使用瀏覽器打開網頁，避免直接安裝軟體到電腦

我們在電腦上造訪各種網站時，經常被詢問是否要另外下載特定軟體並安裝在電腦或手機裡面，例如 Facebook Messenger、Slack、Discord 或所有的郵件軟體 (例如 Outlook) 這些經常用於工作的通訊軟體。事實上，經由瀏覽器使用這些通訊服務，能確保這些軟體只能在瀏覽器這個外殼中活動，而不會輕易危及裝置的其他功能。若直接在你的裝置內安裝軟體，反而可能另外提供這些軟體錄製你的螢幕畫面、直接存取資料夾內容，甚至是操作其他已安裝軟體的權限，並非安全的作法。

2. 避免在手機或平板的社交軟體內直接瀏覽網頁

同樣的，我們平常在手機或平板使用各式社群平台軟體時，經常會點擊連結後直接在軟體內進行瀏覽，例如直接點開朋友在通訊軟體傳來的購物網站連結，然後登入進行購買。但這其實提供了軟體直接側錄我們一切輸入內容的機會，一旦輸入其他服務的帳號密碼或金融資訊，都會直接被軟體獲取。因此，也建議盡可能在手機或平板內複製連結後，改用前述的開源與安全軟體進行瀏覽。

3. 自動啟用無痕模式的瀏覽器 Firefox Focus

在公共或陌生電腦時使用瀏覽器的無痕模式，可以增加一點瀏覽安全。這裡推薦一個可以在手機或平板下載的 Firefox Focus，它是延伸自 Firefox 的瀏覽器，它不只阻擋追蹤，每次關閉軟體之後都會刪除 Cookie 跟瀏覽紀錄，很適合用來在手機或平板開啟網頁，看完之後就關掉，毫無負擔地甩掉大部分的追蹤行為。

4. 不要將密碼交給瀏覽器管理

最後，無論使用哪一款瀏覽器，在輸入帳號密碼時都會被詢問是否將密碼交給瀏覽器管理，這樣下次輸入時可以直接由瀏覽器貼上。注重安全或隱私的人，最好別這麼做，因為一旦瀏覽器的防線被駭客突破，那就可以一次打包你所有帳號密碼。如果需要管理眾多帳號密碼，建議另外使用密碼管理器軟體，可參考本手冊接下來介紹的 KeePassXC 與 Bitwarden。

5. 官方下載最安全

若使用電腦，前述注重隱私的 Firefox、Brave、LibreWolf、Tor 四種軟體都只建議從官方網站下載；如果使用的是手機或平板等行動裝置，只建議 Android 裝置從 Google Play 商店或 iOS 裝置的 App Store 直接搜尋瀏覽器軟體名稱並下載安裝。這些由官方管理的商店會定期檢查檔案的安全，絕對不建議從其他地方下載安裝檔案再移入裝置裡面使用（除非…，不！沒有除非！）。

6. 分散風險：用兩個瀏覽器來讓公私生活分開

當然，只要你願意多花一些時間，前述的每個瀏覽器都有加裝外掛、提升保護能力的空間，成為萬用的瀏覽器。不過，如果都用同一個瀏覽器進行生活娛樂、日常工作、機密通訊等所有事情，那就仍有可能因為被駭客發現漏洞而導致全盤皆輸。

真正能分散風險的作法，是將不同性質的事項交由不同的數位裝置處理，但一般人在經費有限的情況下，很難分別為了生活娛樂、日常工作、機密通訊購買三個不同的設備。即使買得起，也很難帶著它們移動。

因此，我們建議一個折衷作法 —— 依據事務性質分別使用不同的瀏覽器。例如，最無關緊要的生活娛樂交給瀏覽器 A、日常工作業務只在瀏覽器 B 進行、僅在需要進行機密通訊時開啟瀏覽器 C。這樣你在網路上的足跡就能被簡單分割，不會累積在同一個瀏覽器裡，也不會輕易被同時監視多個網站的追蹤器將你的娛樂帳號、工作帳號、機密帳號辨識為同一個人。

簡單來說，別將雞蛋放在同一個籃子裡，瀏覽器就是那個籃子。

如果對本文的介紹有任何疑義，也可以聯繫 hi@ocf.tw 開放文化基金會。

單元課程

一次保管所有的密碼

密　碼　管　理　器

02 一次保管所有的密碼：密碼管理器

案例

小明在了解瀏覽器重要性和重新檢視自己的上網行為後，發現他的資安問題還是沒解決，隔壁的技術人員看了看，指著捲軸的第二頁，告知是因為他的「密碼被偷了」！你知道在個案故事裡，小明的哪些風險是因為密碼管理不當而造成的嗎？想好後，再往下對答案喔！

答案：

★ **小明用同樣的帳號與密碼申請各式各樣的服務，這代表只要任何一處外洩他的資訊，其他帳號的安全性也極有可能被攻破。**

★ **在〈風險評估〉章節，組織 A 發生員工怕忘記密碼，用便利貼寫下帳號密碼貼在桌上的狀況。**

★ **小明讓瀏覽器記憶自己的帳號密碼，把自己的密碼交給瀏覽器保管，如果瀏覽器外洩他的帳密，他的資料也會跟著曝光。**

概論

又忘記密碼了？在社交平台、購物網站、遊戲使用同一個密碼？還是，太多密碼要記反而手忙腳亂？在數位時代，密碼如同鑰匙，保障你的社交帳號、購物紀錄、遊戲資料，它因此成為駭客覬覦目標，因為只要取得密碼，就能冒用身分、盜刷信用卡、竊取線上遊戲內的虛擬寶物，對受害者造成各種損害。

更進一步看，對捍衛人權的公民團體而言，電子郵件信箱、會議文件、捐款者資料，皆是組織的重要資產，如果帳號密碼為駭客所知，恐怕不只組織員工的個人生活遭殃，更有可能使組織名譽受損、重要的行動資訊洩露，甚至組織員工或合作對象被極權國家鎖定，有生命安全之虞。

密碼紀錄方式有哪些？

你仍用紙本記錄密碼，壓在抽屜中，或用便條紙將帳密貼在電腦上嗎？紙本不失為記錄密碼的辦法，然而紙本容易暴露資訊，也容易遭竊、遺失，許多人開始改用網路瀏覽器自動記錄所有密碼。但前面也提到用網路瀏覽器記錄帳密會產生的疑慮，那麼，除了紙本和瀏覽器，還有其他更好的方式嗎？

目前常見的密碼記錄方式包括：紙本紀錄、瀏覽器自動儲存、密碼管理器、Security token 等，下表介紹其優缺點：

	使用方式	優點	缺點
紙本紀錄	使用紙筆記錄密碼。	隨手隨記錄，可直接貼在裝置上。	易被竊取實體、遺失及暴露資訊。
瀏覽器自動儲存	將帳號密碼紀錄在瀏覽器中，並自動帶入。	需要登入時會直接帶入帳號密碼。	可透過瀏覽器漏洞竊取帳號密碼；任何能存取電腦使用者設定檔的人，可看到或偷走密碼。
密碼管理器（本地儲存版） * 如：KeePassXC、Bitwarden 離線使用	將密碼儲存在密碼管理器中，登錄管理器取用密碼。	• 只要記住一組密碼開啟管理器，就可以管理所有密碼。 • 離線版本可以在網路環境不安全、不連線情況下使用。	離線版本密碼庫檔案遺失就全部不見，且電腦、手機不互通。
密碼管理器（雲端版本） * 如：1Password、Bitwarden 雲端		• 只要記住一組密碼開啟管理器，就可以管理所有密碼。 • 雲端版本可跨裝置同步密碼庫，方便取用。	雲端版本密碼庫加密儲存在服務商的伺服器，有可能被駭客入侵竊取。
Security token * 如：YubiKey	使用實體安全金鑰認證登錄。	提供主要密碼以外的保護措施，兩階段認證可為物理保護。	裝置須額外購買，裝置若遺失，就沒有機會打開密碼（庫）。

使用密碼管理器是一項重要、卻常遭輕忽的基礎工作。除了 KeePassXC 與 Bitwarden 之外，市面上還有其他開源、商業的密碼管理器，可依照自己的使用習慣來做選擇，Privacy Guides 網站所挑選出的幾款密碼管理器[10]，亦可作為挑選時的參考。

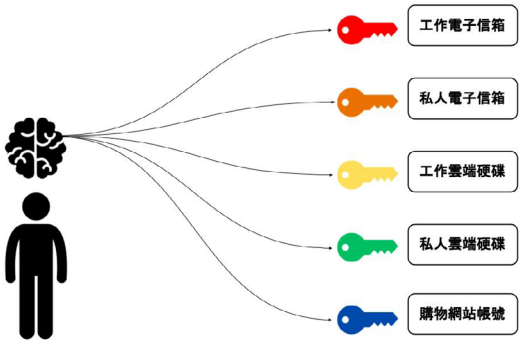
10 數款密碼管理器介紹：https://www.privacyguides.org/zh-Hant/passwords/

如果你希望在主要密碼之外再加一道保護措施，確保即使整台電腦被盜走，對手也無法開啟密碼資料庫，那麼可以考慮使用 YubiKey[11] 這樣的物理保護措施當作第二層鎖 (也就是「二階段驗證」的概念)，它如同實體鑰匙，外觀像 USB 隨身碟，只能在實體插入、手動接上電腦時解鎖打開 KeePassXC 密碼庫。但是，使用者須負擔購買此裝置的費用，且若裝置遺失，就沒有任何機會可打開密碼庫了。

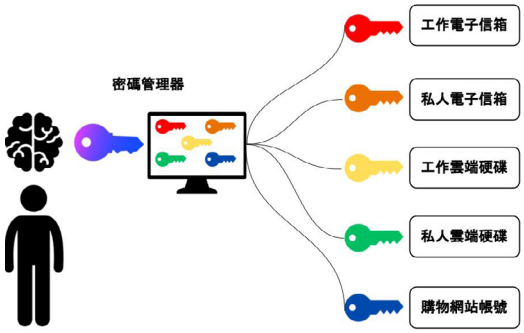
整體而言，我們推薦「一加一大於二」的作法，密碼管理器搭配亂數密碼作為主要工具，並以 Security token 實體金鑰做二階段認證為輔助，更完善地保護密碼。

密碼管理器的原理是什麼？

人的記憶力有限，對於複雜的密碼更有限。如果你的密碼很多，也許你曾考慮將所有密碼都寫在同一張紙上，鎖進櫃子裡，但因為使用上很不方便，而且要是紙張遺失，後果不堪設想，因此作罷。密碼管理器可說是為此而生，將複雜的思考與記憶工作交給軟體，「人」只要記住一組最關鍵的主要密碼 (也可以再加上雙重驗證)，就可以完成儲存、記憶眾多密碼的艱巨任務。



圖左： 人腦記住所有密碼



圖右： 由密碼管理器管理密碼

具體而言，密碼管理器可以協助你從圖左一個大腦記憶不同帳密的情形，改善到僅須記得管理器入口密碼，再由管理器告訴你哪些帳號分別對應哪些密碼。每當你要輸入、登入時，只要五個步驟：

1. 打開管理器並輸入密碼，解鎖資料庫。 → 2. 點選你要登入的帳號。
3. 複製密碼。 → 4. 在欲登入的頁面貼上密碼。 → 5. 關閉管理器。

11 YubiKey：https://www.yubico.com/products/yubikey-5-overview/

你只須在第一個步驟動腦解鎖，不必費心從記憶深處召喚複雜的密碼。在本手冊撰寫過程中，我們多次與資安專家及數位科技愛好者討論，最終大家認為最好上手、最推薦的，是兩套以開源技術為基底的密碼管理器：KeePassXC 與 Bitwarden。以下將介紹這兩個好用的密碼管理工具：

KeePassXC

KeePassXC 是開放原始碼軟體 KeePass 家族的一員，它的程式碼透明、為任何人所知且可供檢驗，由網路社群的志願工程師集體開發與維護，降低了它隱藏惡意功能以竊取資料的可能性。
與市面上商業密碼管理器不同的是，KeePassXC 不僅免費提供所有人使用，保護功能更不會因營利考量而打折，其密碼儲存與管理的位置並非在商業公司經營的伺服器裡，而是在你所擁有的電腦裝置中，大大降低潛在的密碼洩露、或是因網路斷線而無法同步下載使用的風險。
KeePassXC 功能多樣，可跨裝置在手機、平板共用，網路上有相關教學，例如：開源密碼管理軟體：KeePass[12] 或 KeePassXC 免費密碼管理軟體圖解教學，信用卡、瀏覽器、手機都能快速輸入[13]，於此不再贅述。不過，跨裝置使用意謂你要四處搬遷密碼資料庫，甚至將資料庫上傳到雲端硬碟，如果擔心搬遷過程遺失、出現無法預料的問題，或是存放密碼資料庫的網路空間遭竊，請慎選跨平台的功能。

想知道如何第一次安裝 KeePassXC 就上手嗎？ 請見〈附錄二：KeePassXC 使用方式〉。

Bitwarden

Bitwarden 是一款自由且開源的密碼管理服務，它的程式碼公開且可供檢驗，提供多種跨平台應用程式，包含網頁與命令列介面、桌面應用、瀏覽器擴充套件、行動裝置應用程式。Bitwarden 有提供雲端代管服務，如有資安考量或資料保存規範，亦可自己架設密碼儲存伺服器，支援自行部署解決方案，自己管理密碼又可保有不同裝置同步密碼的便利性。
Bitwarden 主要分為「Personal」跟「Business」兩個方案。個人方案內又區分為「Free」、「Premium」和「Families」三種方案，如果需要讓多人存取相同密碼庫，必須選擇「Families」才有多用戶功能，單人使用選「Free」即可。免費、付費在功能上差異不大，主要差別為一些進階功能，對一般用戶而言，免費方案其實足以勝任大部分工作，包括無限制的密碼儲存數量、在所有裝置同步密碼、密碼產生器等等。

KeePassXC 跟 Bitwarden 在使用上與其他密碼管理器相同，卻更加安全。它可以幫助你輕鬆保管多組帳號密碼，或使用亂數自動產生更難破解的密碼，讓你再也無須為創造新密碼想破頭。

12 開源密碼管理軟體：KeePass：https://ithelp.ithome.com.tw/articles/10226300
13 KeePassXC 免費密碼管理軟體圖解教學，信用卡、瀏覽器、手機都能快速輸入：https://www.playpcesor.com/2020/07/keepassxc.html

小撇步

1. 使用獨立運作的密碼管理器，而非讓瀏覽器記憶你的密碼

瀏覽器本身承載了很多使用者的網路瀏覽紀錄、使用習慣，已經是相當容易被駭客盯上的目標，因此，建議密碼只交給獨立運作的密碼管理器，避免與瀏覽器有直接關聯。如同將不同功能事務交由不同瀏覽器處理的分隔原則，減少雞蛋集中在同一個籃子裡的風險，密碼只交給獨立運作的密碼管理器雖然沒那麼便利，但是密碼管理器大多已提供直接複製帳號名稱、密碼的功能，仍可省下使用者輸入帳密的時間，且密碼管理器還可以在市面上絕大多數的電腦作業系統 Windows、蘋果作業系統 MacOS，或開源作業系統 Linux 跨平台使用，甚至也適用 Android、iOS 手機或平板，協助你做到跨裝置的密碼管理。

2. 使用不同帳號及密碼，更妥善保護重要資訊

大多數的人會在不同的網路服務、帳號使用同樣或相似的密碼，以確保自己不會忘記。然而，使用相同密碼，意謂一旦某一個網路服務商被竊取資料，惡意人士可以僅靠取得其中一次外洩事件中的密碼，就盜取你所有不同服務的帳號。例如，檢測個資是否遭外洩的線上服務 Have I Been Pwned 或 Firefox Monitor 每隔一段時間發布某些知名服務外洩事故，範圍包含雲端硬碟 Dropbox、健身服務、線上設計軟體 Canva 的帳號密碼。只要你使用過的服務其中一種遭駭，其他帳號也可能會遭殃，導致損害範圍擴大。

為了保障基本的帳號使用安全，大多數人都知道要設定複雜密碼、經常更換密碼、不要四處使用同一組密碼，但實際執行極其困難。畢竟，每想一套複雜的密碼，都要需要花時間與心力去記憶，而且也不見得能夠及時更換所有帳號的密碼。密碼管理的成本會隨著工作內容的敏感程度而增加，這也是本章節特別要介紹密碼管理器的原因，讓一套系統為你記得這些分散的帳號密碼，既不怕忘記，更可降低帳號外洩的可能性。

3. 別偷懶讓全組織共用一組密碼

全組織共用一組密碼不是好作法，因為無法完全掌握組織裡每個人保護密碼的程度，所以若密碼外洩，無法有效找出外洩原因，也難以提出修正或提升安全防護的對策。組織不僅不該共用同一組帳號，也應針對業務需求給組織成員不同程度的權限帳號，以提升整體的安全等級。

4. 設定「好密碼」

- 長度足夠：通常建議至少包含 12 個字符以上。
- 複雜性：密碼應包含不同類型的字符，如大寫字母、小寫字母、數字和特殊符號，或選擇一個容易記住但不容易猜測的句子，或結合多個句子來建立更長的密碼。避免使用易於猜測的常用單詞或簡單的數字序列。
- 不易猜測與被社交工程攻擊：密碼應該避免使用與個人資訊相關的單詞、日期或其他易於猜測的模式，因為這樣的密碼遭社交工程攻擊、破解的風險較高。最好採用隨機生成的密碼。
- 不重複使用：每個帳戶都應該使用獨特的密碼，避免多個帳戶共用同一個密碼。
- 定期更新：密碼應該定期更改，以降低被破解的風險。建議每 3~6 個月更換一次密碼。

如果對本文的介紹有任何疑義，可以閱讀我們以前寫過的 如何：使用 KeePassXC | 監控自我防衛[14]，或是聯繫 hi@ocf.tw 開放文化基金會詢問。

14 如何：使用 KeePassXC | 監控自我防衛：https://ocftw.github.io/ssd.eff.org/zh_TW/module/how-use-keepassx.html

單元課程

保障公民團體自建網站的安全

03 保障公民團體自建網站的安全

案例 小明搞好了密碼之後，發現網站仍然還沒恢復……他又拿出了捲軸，前後翻看著到底該如何是好。你知道在前面的個案故事一章當中，哪些是與網站安全 / 網站管理相關嗎？

沒錯，答案就是：

★ 同事小美用 Woodless 與網路上搜到的免費外掛，自己架設組織 A 的網站，但她不具備檢視程式碼是否有安全漏洞的能力，難以應付駭客攻擊。

★ 網站遇到分散式阻斷服務攻擊 (DDoS)，組織 A 沒有防禦手段。

公民團體往往忙於第一線的工作，難有時間與量能去維護自架的網站，更遑論精進相關的技術能力。但無奈的是，個案故事中的情境在現實生活屢見不鮮。首先，在數位時代，架設網站進行倡議，不僅能有效率地增進觸及廣度，也是組織長期工作的依據，有了網站上建檔的資料與成果，有助倡議工作長遠推展。

公民團體有自架網站的需求，然而，來自公民團體對立面的威脅也是存在的，具敵意且受政府資助的駭客 (此為舉例，這類型的駭客具有較高的針對性並具備持續攻擊的量能)，攻擊、入侵這類自行架設的網站輕而易舉，輕則癱瘓網站 (例如反覆提及的 DDoS)，阻止訊息傳播；重則植入惡意外掛程式以盜取使用者的重要資訊。

面對針對公民團體的網路攻擊，我們應該優先考量什麼？我們可以從威脅建模，也就是風險評估的角度，依序思考「要防護什麼、為什麼要防護、威脅或風險從哪裡來、形式是什麼」這幾個層次來釐清。

概論 威脅或風險樣態概覽

以下介紹幾種威脅樣態，這些敘述不會深入細節，旨在提供簡單的名詞解釋及可能的風險後果：

DoS & DDoS

阻斷服務 (DoS) 攻擊目的在於讓系統資源短缺，使其無法回應正當的服務請求。分散式阻斷服務 (DDoS) 攻擊也類似，只是 DDoS 是多系統針對單一系統的攻擊，比起一對一的 DoS，它的規模往往較大。兩者都會試圖耗盡目標系統的資源，讓受害網站無法提供服務給使用者，這經常導致受害網站完全關閉。甚至，在網站關閉重啟的過程中，又可能受到其他攻擊傷害。

域名系統 (Domain Name System, DNS) 的相關攻擊

DNS 就像電話簿，在一般情境中，它透過分層向下委任，一層層把人類可讀的域名 (例如：ocf.tw) 比對、轉換為以數值呈現的網際網路協定 (Internet Protocol, IP) 位址 (例如：192.68.1.1)。在此不細述 DNS 攻擊的技術細節，但我們必須知道，針對 DNS 的攻擊可能導致網站停擺、進入網站時被轉址到其他網站 (粗製濫造的網頁，或更糟的惡意網站)，也可能導致資料外洩。不僅對組織聲譽及營運有害，也可能傷害使用者，甚至觸犯法律。

未經 HTTPS 加密的風險網站

沒有 HTTPS 協定加密的網站，相當於把網站內過手的資料全都攤在陽光下供人檢視，不僅網站方有資料外洩的危險，同時也置瀏覽網站的使用者於風險之中。

Brute Force Attack

正如字面上所說，蠻力攻擊、暴力攻擊，或稱暴力破解。駭客針對目標網站準備了認為有機率存取網站管理人員的帳號密碼清單，然後讓機器人 (程式) 一個個嘗試，直到成功侵入網站管理層為止。這可能導致資料外洩、網站被綁架或刪除等。

專業的事交給專業的來

但是，千萬不要因為潛在風險而對在數位世界倡議卻步！說白了，就像現實生活，你需要注意自己的人身安全、確保辦公室不會有陌生人闖入或偷聽 / 偷窺。在數位世界的維護、營運也需要成本，若這些成本不是金錢或時間，代價很可能就是你的安全或隱私。那麼，沒有足夠技術能力的公民團體 / 倡議者，該怎麼保護自己呢？

很簡單，交給專業的來！

全球有許多支持公民團體或人權工作者的非營利組織、商業公司提供資訊安全相關服務，以下將介紹 eQualitie 提供的 Deflect 和 eQPress 網站保護服務，以及 Cloudflare 提供給公益團體網站的 Galileo 計畫，透過申請，目標網站可受 Cloudflare 保護。這幾個選項目前都屬於申請後免費提供，聚焦在協助公民 / 公益團體，甚至有些提供中文客服，我們認為這些都是適合本手冊讀者用來應對網站威脅的好選項。

自己的責任切莫心存僥倖

在應對外來威脅時，有很多基礎的概念、行為需要自己理解、內化、實踐。舉例來說，將工作帳號的管理權限分層、登入採多階段驗證、設定高強度密碼、運用端對端加密軟體或使用 VPN 等，都能強化自身資安體質，可有效降低曝險。而關於個人或組織內部如何應對可能的風險、如何與專家對接，還是需要親自面對。建立個人紀律、組織守則是比較好的實踐方式，包括：

管理權限分層	高強度密碼	多階段 / 兩階段驗證
有加密意識、多用加密通訊	對釣魚信件保有警覺	

總而言之，把技術含量高的資訊安全實踐交付專家處理後，個人 / 組織還有很多需要加強、努力之處。這些知識與行為層面的改善將大大助益個人 / 組織的資訊安全，讓風險顯著下降。好比總不能在門上加了很多道鎖和生物辨識後，屋主卻連關門鎖門的原理都不懂吧？

可用工具

以下我們介紹兩類服務：Deflect 與 eQPress、Galileo project

Deflect 與 eQPress

總部在加拿大的 eQualitie 提供讓公民團體免費申請的保護措施。eQualitie[15] 是一家目標提高人們在數位世界的言論自由、規避審查、強化匿名、避免監視等基本權利的公益企業，與跨國、跨領域成員在全球提供服務。

本文要介紹它在網站防護的 Deflect 服務，以及其中專門給公民團體免費申請使用的 WordPress 系統網站維護服務 eQPress。鑑於公民團體遭受攻擊的風險高、通常缺乏技術團隊，很容易因為網站沒有更新、外掛功能(plug-in)而產生安全漏洞，eQualitie 團隊因此開發了 Deflect 與 eQPress，協助公民團體保護網站。

公民團體若將網站架設在由專業團隊維護的空間，就能降低特定攻擊入侵的機率，例如 2016 年，一個烏克蘭獨立媒體網站就因此免於來自俄羅斯、越南等境外的流量超載攻擊 [16]，使網站不至於中斷，能繼續揭露政府弊案。只要是公民團體，以捍衛人權為目標，例如獨立媒體、或支持從事人權工作的人，在同意使用條款並接受隱私規範後，就能申請協助保護網站服務 [17]。

15 https://equalit.ie/values/
16 https://www.vice.com/en/article/qv5xwq/the-activists-on-the-forefront-of-ukraines-cyberwar
17 https://deflect.ca/non-profits/

使用情境

若你符合以下兩點情境，為了倡議工作的安全、持續性，敬請認真考慮申請 Deflect 與 eQPress：

1. 你的網站有被攻擊的疑慮

公民團體在網路上發表的內容經常會觸犯既得利益者 (通常是政府或是有能力雇用駭客的有力人士)，進而引來惡意攻擊。如果有駭客打算讓你的意見從網路上消失、或是減損你的社會信任，可能會使用俗稱 DDoS 的流量超載攻擊來癱瘓你的網站 —— 攻擊者會在短時間內製造數以百萬計的讀取要求，讓網站所在的伺服器沒有足夠頻寬可讓其他人造訪。

另外，公民團體的網站也可能成為異議人士的隱私漏洞，如果極權國家想透過駭客來威脅網站使用者的安全，會監控公民團體的網站，並在網路資料傳輸的過程攔截、辨識、竊取有關人士的個資。

2. 已經使用或打算使用 WordPress 系統架設網站

WordPress 是一種常見的架設網站軟體，世界上有超過 40%的網站使用這個系統。同時，因為軟體免費、易上手、開放程式原始碼給所有人使用，公民團體為了與社會大眾溝通，經常會另外租賃網域、伺服器，以 WordPress 自行架設網路平台，尤其 WordPress 安裝各式外掛容易，能提供捐款、訂閱、購買義賣品的功能。

然而，即使它彈性大、讓使用者有自主權、不會受限於網站架設廠商，但自行架設的 WordPress 網站若沒有專業技術團隊維護，可能會產生許多安全漏洞。如果你擁有 WordPress 系統的網站，或考慮使用 WordPress 建置網站，就能申請由 eQPress 平台維護網站，讓專業技術團隊進行管理，使你的網站可以在攻擊中屹立不搖、繼續倡議工作，並且加密所有傳輸資料過程，確保使用者的隱私及安全，除了擁有 Deflect 的保護，該服務還有以下功能：

- 防止病毒
- 遠端備份
- 提供佈景(theme)及外掛(plugin)之編輯介面供客戶自行操作
- 客服技術支援
- WordPress 及 Deflect 的更多細部選項及服務

如果你的網站非 WordPress 系統，可以只申請 Deflect 服務協助你的網站抵禦攻擊。

如果你需要申請這些服務，可繼續閱讀下文認識這些服務的使用方式、申請流程。如果你不確定相關的技術資訊意義，建議在組織內協調適合人選，或尋求顧問協助。

開始使用之前

當你的組織有架設網站的需求，又可能是駭客針對的攻擊目標時，可選擇結合 WordPress 這項工具並搭配 eQPress 的服務。簡單說，Deflect 服務可以保護網站，若網站是以 WordPress 系統建置，加掛 eQPress 框架會更安全。

如果你的組織網站不是 Wordpress 系統，只需要 Deflect 的防護功能保護網站，請直接跳到申請流程的段落繼續閱讀。

WordPress 是一套開放原始程式碼的網站系統，使用者可以自訂外觀與內容，並增加各式外掛功能。經由 WordPress 架設網站並搭配 eQPress 的服務，可以想成在網路世界租辦公室開始倡議工作，可粗略分為三大步驟：

1. 決定並租用網址

決定網址的名稱，例如 https:// 你的網站名字 .tw ，讓所有人都能記住並找到你的網站。想好網址名稱後，就要尋找租賃網域的服務商，例如 Gandi、Cloudflare、GoDaddy 這類服務商如同購物平台，整合各類網址提供租借，你可以基於組織對網站網址年費的預算決定不同結尾的網址。決定後，你的網址就登記在網路世界中了。

2. 租用適合的空間

現實中的辦公室，除了地址之外，還得有一個具體的建築空間。在數位世界，網站的「建築空間」，就是存放網站資料的伺服器主機，其如同建築的大小、規格，會影響能探訪網站的訪客人數以及他們的行為限制。eQPress 擔任伺服器主機，並提供 WordPress 網站強健且具彈性的保護；任何想要造訪網站的訪客，都必須經由 eQPress 的伺服器才能進入網站。

3. 網頁外觀設計

你可以按照倡議需要，使用 WordPress 的軟體系統來設置網站外觀、功能、內容。不過，網頁設計不屬於 eQPress 的保障範圍，因此你得自行挑選或設計好看的網頁。當然，你也可以外包給專業的網頁設計師，再將網頁設計師的成果搬移到 eQPress 裡。

申請流程

eQPress 是一項基於 Deflect 的免費服務，不須下載或安裝程式到電腦中。經由線上申請，就可取得 Deflect 的網站保護以及 eQPress 的網站維護服務。欲申請這項服務的組織，須符合以下條件：

捍衛人權；公民組織；經營獨立或非盈利媒體；支持人權工作者。	**工作內容不違反《世界人權宣言》中的原則。**	**工作過程不宣揚仇恨言論或鼓勵歧視。**	**同意使用條款並接受隱私規範。**[18]

18 https://deflect.ca/privacy-notice/

若你符合上述條件並同意規範，便可到 https://deflect.ca/non-profits/ 註冊申請。
在申請之前請先準備好：

- 網站的網址(網域及伺服器的 IP)、聯絡人的 e-mail。
- 如果不需要使用eQPress保管Wordpress網站，在此步驟可僅申請Deflect的網站保護功能即可。

流程中有任何申請問題，都可聯繫客服人員。

申請通過後，就能在 Deflect Dashboard 的選擇介面(Hosting tab)決定要使用的 eQPress 方案，有三種類型：

1. 建立空白的 WordPress 網站
   如果你未曾架設，或想重新開始一個網站，那就可以選擇這個方案，透過 WordPress 的管理工具設計網站內容。如果不知道如何開始，可以上網搜尋「WordPress」、「佈景主題」等關鍵字組合，可找到相當多網站設計流程教學文章，本文不再贅述。
2. 建立空白的 WordPress 並預載指定主題
   如果你已經有選定的、設計完成的網站佈景主題，就可以載入你設計好的網站。
3. 遷移已架設的 WordPress 網站到 eQPress 平台內
   如果你之前已在其他地方使用 WordPress 架設網站，並且想原封不動搬遷既有的網站內容，請聯絡之前協助你管理網站的伺服器供應商，請他們提供 WordPress 的原始檔案、程式碼及資料庫備份檔，再交給 eQPress 的技術人員。

技術支援／求救方法

當你註冊 Deflect 的帳號之後，即使你不是資訊科技相關的技術人員，或不熟悉 WordPress 的軟體、租賃網址過程，都沒關係。在使用流程上有疑問，或是網站經營期間有其他問題，都可以從 https://support.deflect.ca/ 登入你的帳號，請求客服協助。還沒註冊帳號的話，則可填寫官網表單：https://deflect.ca/contact-us/。eQualitie 團隊是為了協助全世界的公民團體適應、強化數位世界的生存能力而生，只要你的組織工作目標是促進公平、自由、人權，他們願意協助你。

Galileo project

若你的組織是從事藝術、人權、公民社會、新聞工作或民主工作的組織，只要通過申請[19]，你的組織網站就有機會加入 Galileo 計畫，接受 Cloudflare 商業等級客戶的服務支援。
Cloudflare 是美國一家提供 CDN (Content Delivery Network，內容傳遞網路)、雲端資安、DDoS 緩解，以及網域註冊服務的公司。 截至 2022 年，全球已有超過 20%的網路用戶使用 Cloudflare 服務。 換言之，Cloudflare 的使用者社群已有相當規模，其服務也有一定的可信度。
Galileo 計畫為其保護的網站提供了許多服務，對應先前提及的常見攻擊，我們節錄以下幾個重點項目：

- DDoS 保護：提供 DDoS 警示，並保護網站和應用程式，同時確保合法流量的效能不受影響。
- DNS：提供 Cloudflare 的 DNS 服務，具備緩解針對 DNS 之 DDoS 攻擊的能力，也具備 DNSSEC 功能，能夠協助確保 DNS 的完整性和真實性，降低針對 DNS 的攻擊。
- 通用 SSL 憑證：可與現存的 SSL 設定相容。網站需要 SSL 憑證，以確保使用者資料的安全，驗證網站的擁有權，防止攻擊者建立網站的虛假版本，並且獲得使用者信任。如果當前沒有使用 SSL，無須進一步操作，Cloudflare 即可提供 SSL 功能。SSL 憑證為架設網站、建立 HTTPS 連線時需要的加密憑證檔案。
- 機器人緩解：有效減少蠻力攻擊的影響。
- Web 應用程式防火牆 (WAF)：針對 WAF 的每個請求都將根據規則引擎進行檢查，並設計威脅情報以保護網站。可以根據使用者的需求封鎖、質詢或記錄可疑請求。

Galileo 計畫提供的諸多服務中，也包含來自 Cloudflare 自身效能提升、降低風險的改善服務，例如 Cloudflare Gateway、Cloudflare 的 DNS、CDN、快取效率提升或完整清除等等。這些服務都仰賴 Cloudflare 龐大的使用者社群，以資訊安全為例，龐大的使用者社群意味靈活且豐富的威脅情報，因此 Cloudflare 有條件可以去經營好攻擊緩解與遏止。

Galileo 計畫的申請表填寫完畢後，對方會回覆，溝通流程可能是非制式的，本手冊不在此作預測及贅述，若有需求或疑惑，歡迎聯繫開放文化基金會。

19 https://www.cloudflare.com/zh-tw/galileo/

小撇步

除了我們前面所撰寫的數位安全內容，台灣的 Civil Society Cyber Shield (CSCS) 資安社群所翻譯的教材[20] 有對密碼相關、兩階段驗證的介紹，想多認識資安概念與工具的話，也非常推薦上 Surveillance Self-Defense 網站[21]，該網站還有記者出差、參與抗議等情境題可參考，非常易懂。以下為 Deflect / eQPress 的官方說明文件：

- **eQPress — 由 Deflect 安全託管網站：**
  eQPress - secure hosting with Deflect - Deflect (https://equalit.ie/eqpress-secure-hosting-with-deflect/)
- **Deflect / eQPress for non-profits 服務與申請方式簡介：**
  Deflect_eQPress_Intro_zh_TW_May_8.pdf (https://drive.google.com/file/d/1ciHbLpKA34HxRv811-E8KqdzXs2-qt9e/view)

如果對本文的介紹有任何疑義，也可以聯繫 hi@ocf.tw 開放文化基金會詢問。

20 https://ocf.tw/p/cscs/SEC%20%E6%95%B4%E4%BD%B5%E7%89%88_+%E9%A0%81%E7%A2%BC.pdf
21 https://ssd.eff.org/

單 元 課 程

做好備份 321
不再擔心資料遺失案例

04 做好備份 321，不再擔心資料遺失

案例

看著網站重新開站，小明不由得鬆了一口氣。正想著要把報告重新放上去，猛然想起「天啊！我們的資料都不在了……」，小明想著以後的資料該怎麼辦時，一陣風吹起捲軸，翻開了第四章。你知道在個案故事裡，小明是因哪些行為而導致檔案喪失又毫無備份可用的窘境嗎？想好後，再往下對答案喔！

答案：

★ **小明在自己的筆電存放所有報告的素材（訪談、研究材料）和第一版報告檔案，這些資料沒有在他的筆電以外的地方備份。如果筆電遺失或中毒，組織 A 數月以來投注的心血便化為烏有。**

★ **小明將第一版報告上傳到 Woodless 以便跟同事線上協作，不過修訂過程中的每個版本，以及發布前的最後一版檔案，都只存在 Woodless 系統上。當線上檔案遺失，這段時間的編修進度也就跟著消失。**

「在自己的筆電做事，需要團隊討論時上傳到雲端」這是許多人熟悉的工作方式，Google 文件可以輕鬆做到版本管理，回溯到某個大家編修改動的時間點；有些人會細心地為不同版本另開檔案，仔細分類與保管。然而，在鍵入最後一個句號後，大家通常只記得慶祝報告完工、專案執行完畢，不會記得將這些檔案備份。

換言之，你我都可能遭遇小明與組織 A 的慘劇。

概論

資料意外消失的機率比你想像得高

組織 A 遭遇的狀況並非特例，根據資料保護供應商 Veeam 發布的《 2023 年資料保護趨勢報告》[22]，在受訪的 4200 個組織中，有 85%的組織在 2022 年遭受至少一次勒索軟體的攻擊，其中的 39%組織生產數據在攻擊中被加密或銷毀，受害者平均僅能搶救回受影響數據中的 55%。

22 https://www.veeam.com/blog/air-gap-vs-immutable-backups-key-differences.html

就算組織沒被任何駭客盯上，我們也可能因為各種人為、機器故障或天災意外等原因遺失資料。以人為因素來說，工作忙碌時免不了出錯，例如誤刪文件、不小心格式化檔案、重灌電腦前沒備份資料，甚至在意外發生後覆寫檔案，救回檔案的機率更渺茫；有時我們會遇到 USB、光碟或 NAS[23] 之類的儲存裝置故障；也可能因為遭遇地震、淹水等天災導致儲存裝置損壞，或是像在組織 A 的情境裡，若辦公室與救援地點都曝光，對手竊取資料的風險也大幅提升。

為什麼要備份？為了不要經歷失去的遺憾啊！

2021 發生高中生學習歷程檔案資料遺失事件[24]，就是一個警世案例。由於政府委外處理的廠商在將資料搬遷至新機房的過程中，套用錯誤的設定樣板，又恰巧因時程匆促而未完備資料備份機制，導致這段時間所上傳的檔案全部消失，沒有挽救餘地。這件事一共影響 81 所學校，抹去 7854 名學生嘔心瀝血之作。對廠商來說，失去合作單位的信任、額外付出於搶救資料的金錢與時間成本，代價慘重。

對公民團體來說，專案文件、服務對象個資、捐款人資料等各種檔案，都攸關組織守護的價值，更是組織維持運作的基礎。建立完善的資料備份機制，能確保面對任何緊急狀況，組織的核心資產和運作能力不會受到致命打擊，這對組織持續推動倡議、救援個案的工作，至關重要。

如何建立完善的資料備份機制？熟記 321 口訣

只要把資料多存在幾個地方就好了嗎？還是要在電腦和 NAS 上放幾包綠色乖乖，祈禱資料不遺失？雞蛋不可放在同一個籃子裡，但要把雞蛋分散放在什麼地方最安全？資訊界的「備份 321」機制便是這些問題的解答。

- 將資料分別儲存至少在 3 個地方。
- 至少其中 2 個檔案須儲存在不同媒介中，例如在電腦裡存一份，用 USB、外接硬碟等可外接儲存裝置再存一份，或是在雲端上儲存檔案。至少讓一份檔案處於離線狀態，如此可防止病毒攻擊、安全漏洞等風險導致資料遺失；使用雲端備份時，記得考慮該雲端儲存服務是否足夠安全、有無從雲端外洩資料的風險。[25]
- 至少 1 份檔案完成異地備援的儲存方式，亦即把這份檔案保存在和上述 2 個檔案不同的地方，例如可將儲存這份檔案的外接硬碟放在銀行保險箱、辦公室以外的空間。此舉可避免將全部的離線檔案都放在同一個地點，若一個儲存地點遭遇偷竊、天災等意外，仍有儲存在其他地點的資料可備援。

23 NAS 全名是 Network Attached Storage，網路儲存裝置。使用者可透過設定 IP 位址、FTP、網路芳鄰等方式取得存放在 NAS 內的檔案。許多組織使用 NAS 作為辦公室內共用、儲存和備份資料的地方。

24 https://www.ithome.com.tw/news/147155

25 正如〈風險評估〉章節所述，沒有百分之百的安全。使用雲端備份可以降低實體備份因故障、被竊取而遺失資料的風險，還有方便協作等優點，但也有伴隨而來的資安風險。建議組織可以使用威脅建模的流程，辨識出組織保護的資料價值、願付出的成本，找到組織最能承受且可實踐的備份方式。

「備份 321」做起來其實不難，舉例來說，每當完成一個版本的文件，你可以在辦公室電腦、USB 和雲端空間各儲存一份， 並將 USB 保持在離線狀態，存放在另一處 (但如何限制組織的資料外洩到其他地方，是另一個須考量的問題)，這樣即符合備份 321 的原則。如果辦公室遭遇意外、線上備份因人為疏失而遺失檔案，你還有離線且儲存在別處的 USB 裡的檔案可恢復使用。

要注意的是，如果是儲存在同一台電腦的不同硬碟、資料夾，並不符合「將檔案儲存在不同媒介」的原則喔！想想看，如果這台電腦被病毒感染或意外損壞，資料也會跟著消失，在這個情況下，雞蛋仍然放在同一個籃子裡，風險並未分散。

備份時，別忘了要確認檔案可否打開，確保在有需要時能正確還原檔案，若可做到版本管理會更好。以小明的案例來說，如果在每次修正報告內容時都儲存並備份一個版本的檔案，便能找回特定時間點的報告版本，以備不時之需。

可用工具 常見的外接儲存裝置

備份 321 實行不難，最難的是保持這個好習慣。以下介紹常見的外接儲存裝置的差異，可作為讀者選擇最符合需求備份裝置的參考。

儲存裝置 / 性能	CD	DVD	USB	NAS	外接硬碟
容量	700 MB	4.7 ～ 17GB	2GB ～ 2TB	依據 CPU 架構不同而異，可多達數 TB	500 GB ～ 8TB
耐用性	低	低	中	高	高
便攜性	高	高	高	低	中
數據傳輸速度[25]	低	低	高	高	高
取得成本	低	低	低	高	中
故障示警	無。 通常肇因於劃傷、保存環境的溫度與濕度變化，使用者難以提前得知。		無。僅可從頻繁的讀取錯誤、傳輸速度變慢等跡象來推測可能即將故障。	有。 透過硬碟自我監測、分析及報告技術，即時掌握故障前兆。	
建議用途	小檔案、音樂	大檔案、影片	外出攜帶的備用檔案	辦公室集中備份檔案	數量多又大的檔案

如表格，每種裝置的性能不同，組織應視自己須儲存的資料性質、便利性、可負擔成本等不同面向來評估，選擇最適合自己的備份裝置。

25 數據傳輸速度與資料備份和復原時的效率有關，包括將檔案從電腦複製到儲存裝置（寫入速度），以及從儲存裝置存取或還原檔案到電腦上時（讀取速度）所需的時間。速度越快，完成備份和復原的時間就越短，這對於需要頻繁備份大量資料的使用者尤其重要。

雲端備份的選擇

若組織將雲端列為備份的選項，你可以就組織資源與安全性尋找適合的雲端空間。常見的雲端儲存服務有 Google Drive、Mircrosoft One Drive 和 Dropbox，它們皆提供一些免費儲存容量，組織選擇時可評估預算、團隊的工作習慣等，選擇最適合自己的服務商。這些廠商都有提供詳盡的使用教學，本手冊不再花篇幅介紹。

如果你跟組織 A 一樣，判斷某資料屬於應極力保護的資產，那麼你選擇雲端備份廠商時就該將「資料自主性」納入考量。上傳資料到雲端，意謂將自己的資料透過網路上傳，存放到別人的電腦，當你需要存取資料時，再透過網路連線取用 —— 而這代表資料貯存地（也就是機房）的所在國家，可能有權力命令執法單位扣押主機、取走檔案，就如同個案故事裡，政府 C 命令 Nono 集團交出組織 A 的數位足跡紀錄。

因此，對於重視資料的公民團體來說，最好充分了解自己存放在雲端的資料究竟是被誰管理、誰有權限取得。不過，就如同〈風險評估〉章節裡強調的，選擇自己可負擔的安全措施才是最重要的。如下表，開源方案的優點是對資料的掌握度高，有利把關資料流向，堅守隱私。相對的，自行架設的技術門檻是一道挑戰，若你沒有技術能力，也無法委託專業團隊協助架設和維護開源的雲端備份方案的話，非開源方案依舊是可考慮的選擇，以免因缺乏維護而導致資安漏洞。

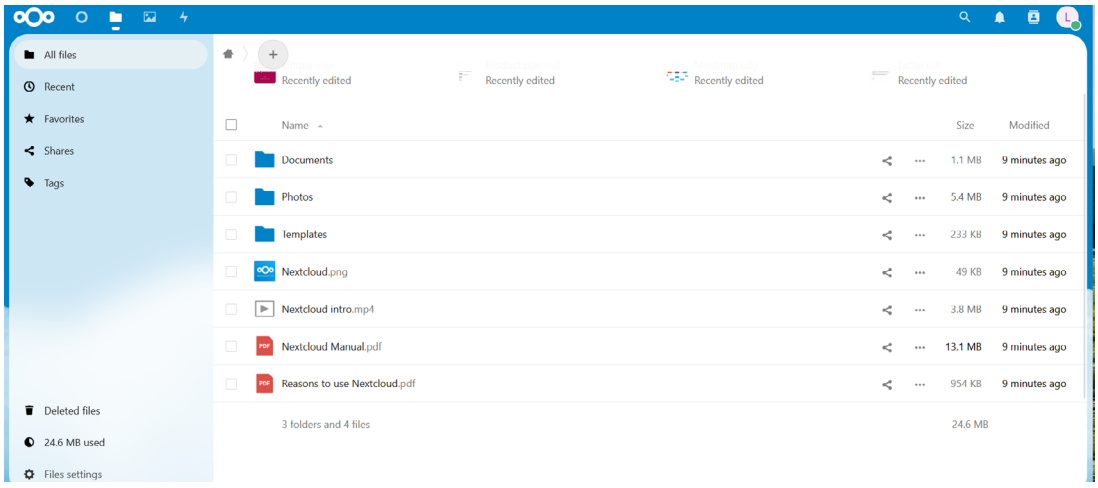
雲端備份	開源方案	非開源方案
資料自主性	高。可掌握資料儲存在哪裡、誰可以拿到資料，因此有較高的安全與隱私。	低。 僅能在供應商提供的選項裡選擇。
服務安全性	可控度高。所有人檢視軟體運作的原始碼，確認是否有安全漏洞。	可控度低。仰賴供應商把關。
成本	架設與維護成本。包括購買主機、租用機房，或是委外維護運作的費用。	每月訂閱費用。

開源方案有許多資料備份的服務，本手冊僅介紹 Nextcloud，因為這套服務的介面與 Google Drive 高度相似，易用性較高，轉換工具的成本較低。我們先來看 Nextcloud 的使用方法，如果你覺得還算好操作，再往下看架設方式，以評估是否要使用開源方案做雲端備份。

Nextcloud 有三種使用方式：

圖： Nextcloud 登入介面

1. 使用網頁備份、處理資料
   打開瀏覽器，在網址列輸入已架設好的 Nextcloud 網址。進入登入畫面，接著輸入自己的帳號與密碼。
2. 開啟電腦的檔案同步功能
   到 Nextcloud 的官方網站下載並安裝程式（ https://nextcloud.com/install/ ）。接著如第一種方式，先輸入已架設好的 Nextcloud 網址，再登入帳號，即可與電腦裡的檔案自動同步。
3. 使用手機或平板的應用程式
   若你使用 iPhone，請到 App Store 搜尋 Nextcloud (https://apps.apple.com/us/app/nextcloud/id1125420102)；若你使用 Android，請到 Google Play 上搜尋 Nextcloud (https://play.google.com/store/apps/details?id=com.nextcloud.client)。安裝 Nextcloud 的應用程式之後，就可以如第一種方式登入雲端硬碟介面。



圖： Nextcloud 使用介面

如果你覺得 Nextcloud 的介面看起來與 Google Drive 相差無幾，上手不成問題的話，不妨參考以下架設方法，考慮組織是否有能力使用 Nextcloud 作為雲端備份方案。

1. 建立儲存空間：有兩種作法。
   - 自行購買電腦主機當作伺服器，優點是較安全，能完全掌握自己儲存檔案的位置，缺點是需要負擔購買及維修電腦、存放電腦主機的機房租金等費用。
   - 將租賃電腦與機房的需求委外給服務商，優點是方便，缺點是對資料的自主性降低，因此建議須再三確認服務商以客戶的安全與隱私為首要目標。
2. 決定雲端硬碟的網址

   如同 Google Drive 有自己的網址 (https://drive.google.com/)，你架設的 Nextcloud 也需要網址。你需要租賃一個網域，例如建立這種網址 —— https://nextcloud. 你的組織 .tw/；若你的組織已經有自己的網域，可直接沿用。

如果架設過程超過組織的技術能力，或是你希望有專業團隊協助你維護雲端空間的安全，避免外界攻擊，可洽詢網路主機供應商 Greenhost[27]、GreenNet[28]，或聯繫開放文化基金會 (hi@ocf.tw) 詢問相關建議。

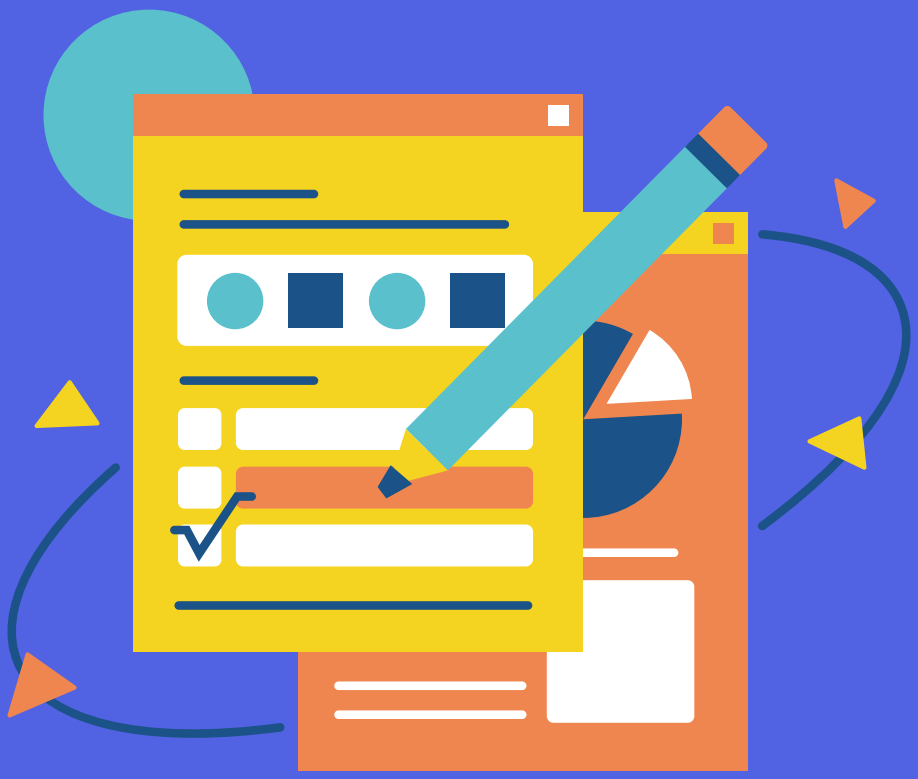
小撇步

資料備份是重要卻又時常被忽略的基礎工作，就像是我們會注意運動的姿勢和技巧，卻常忘了運動後應該要收操，幫助我們放鬆肌肉，避免發生運動傷害，如此才能更安全、持久地運動。同樣地，我們需要將資料備份視為日常工作的必備環節，以建立組織應對危機時刻的韌性。

建議讀者參照〈風險評估〉章節，審視組織對不同資料的保護程度與可負擔的成本，訂立一套組織成員真的可以落實的備份機制。為了養成定期備份的習慣，或許可先從設定幾個檢核點做備份檢查開始 (例如報告寫到一定程度、專案在結案歸檔之前)，避免大家遺漏這個重要步驟。

如果對本文的介紹有任何疑義，也可以聯繫 hi@ocf.tw 開放文化基金會詢問。

27 https://greenhost.net/
28 https://www.greennet.org.uk/



後　　測

後測

借鑑小明和組織 A 的案例，希望你已經和小明一樣，充分了解在工作與生活中應如何落實良好的數位安全習慣。為了不再重蹈覆轍，四個章節之後，捲軸尾端赫然出現了一個整理清單，我們邀請你和小明一起定期檢查，檢視自身與組織落實了哪些項目。最後，小明謹記著神明臨行前的一句忠告，建立良好的數位安全習慣並非一蹴可幾，所以要持續努力，就算無法第一次就全部做到，記得還是要定期檢視，逐漸改善喔！

	檢查項目	是否做到
瀏覽器管理	當網站詢問我是否接受 Cookies，我會拒絕，或僅允許盡可能少的被追蹤項目。	
	我會定期清除瀏覽器的 Cookies 和歷史紀錄，降低我的資訊外洩機率。	
	在大部分情況下，我不會瀏覽沒有加密連線的 HTTP 網站。若不得以為之，會避免在該網頁輸入個人資訊，也會再三確認並核實網頁上的內容是否正確，因 HTTP 網頁是未加密頁面，也有遭竄改內容的風險。	
	我將個人與工作用的瀏覽器分開。	
	在挑選瀏覽器時，我會以保護隱私與安全性為主要考量。	
	安裝瀏覽器時，我只從官方網站下載安裝檔，避免從來路不明的地方下載。	
	我會將瀏覽器更新到最新版本，以免瀏覽器出現安全漏洞。	
密碼管理	我為所有帳戶設置了長度至少 12 個字符，且包含字母、數字和特殊符號的高強度密碼。	
	我避免重複使用密碼，為每個帳戶設置不同密碼。	
	對於支援啟動二階段認證的帳號，我全部啟用二階段認證 (例如：Google、 Facebook、 LINE、 Dcard 等服務)	
	我使用密碼管理器來生成、儲存和管理所有密碼。	
網站管理與維護	公司自己架設的網站有使用 HTTPS 來保護資料傳輸的安全性。	
	網站伺服器、網站平台定期更新，並注意有無重大安全性公告釋出。	
	公司有設定權限分級制度，嚴格控管哪些人能存取雲端空間、進入網站後台，以區分不同員工與合作團隊的資料取得權限。	
	公司有使用以下其一的網站管理措施： ・使用網站託管服務 (例如本手冊介紹的 eQPress)，積極保護網站。 ・自聘或委託外部可信任的資安專家，定期掃描網站和所有第三方外掛程式，確保沒有安全漏洞。	
資料備份	我會按照資料備份 321 ，定期將重要文件和資料做好至少三個地方的備份。	
	我會定期檢查備份資料是否處於可使用狀態。	
整體	公司有按照風險評估 (威脅建模) 的流程，建立自身的組織安全政策。	
	向所有員工布達組織安全政策。若外部合作團隊會接觸到組織所保護的資產，公司會向外部團隊告知並落實相關的安全政策。	
	公司會定期重新檢視組織安全政策，調整至可因應最新情況。	

日期： **填表者：**

危機來了，怎麼辦？

危機來了，怎麼辦？[29]

數位安全防禦是預防威脅發生，但當數位攻擊真的發生時若不知所措，反而功虧一簣。透過閱讀前面幾章理解了這麼多風險及應對方式後，現在的你已有足夠的基礎資安知識和防禦工具。然而，當在數位攻擊發生時的那一刻，該如何在第一時間應對止損，保護自己關心的人、物和使命呢？

答案是 —— 你需要建立一套「緊急因應機制」。

「啊！又要建立緊急因應『機制』，太累、太麻煩了吧！」你是不是冒出這樣的念頭呢？雖然「緊急因應機制」聽起來厚重又複雜，但形式上只是一份短短的文字檔（電子或其他方式），記載相關資訊、施行步驟，它將是你面對緊急狀況時的指引，幫助你快速反應。下面我們分成三個面向：準則、制定緊急因應計畫、資安求助資源，幫助你建置「緊急因應機制」。

準則

面對數位攻擊時，即使感到恐懼，也必須把握「主動回報」、「安全至上」這兩個準則。「主動回報」數位攻擊的狀況，除了能讓組織全體能及早發現、介入之外，更能確保組織及員工的福祉。同時，以同理心看待資安狀況造成的損失（如手機遭竊、使用網站遭受釣魚攻擊、社交帳號被駭等），避免組織或個人因擔心報復或究責，反而隱瞞受損狀況。更重要的是，透過獎勵帶動「安全至上」風氣，從根本打造注重資訊安全的文化。

制定緊急因應計畫

制定緊急因應計畫是為了應對危機時能有所「行動」，而如同風險評估會因組織、個人而異，緊急因應計畫也需要綜合自身狀況和資源以客製化。畢竟，不同規模的機構所能處理危機的資源不同，不同性質的組織所遭受的數位攻擊和頻率大相逕庭。個人與組織都有能力規畫、制定因應計畫，因為自己就是行動的主體。當然！若有資安專家把關，這份計畫會更完善。

---

29 參考資料：https://www.ndi.org/sites/default/files/%5BEnglish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf

危機來了，怎麼辦？

若你不知道從何開始，以下是幾個最常見的資安緊急狀況，先從以下幾個問題開始構思緊急因應措施吧！在此要先提醒，發生資安事件，我們需要可能不只是技術、資安專家，更可能需要法律專業、警察、心理諮商、其他公民團體等資源來修復資安攻擊導致的傷害。

- 如果帳號或網站遭到駭客攻擊，我們該怎麼辦？
- 如果有人點擊網路釣魚電子郵件或他的裝置行為可疑 (例如半夜上傳資料出去或下載一大堆東西)，我們該怎麼辦？
- 如果組織的電子郵件或最機敏的檔案被盜或洩露，我們該怎麼辦？
- 如果組織成員面臨人身安全危險或被逮捕，我們該怎麼辦？
- 組織成員因此產生人身安全危險或被逮補類型的威脅，而產生壓力和焦慮時，我們該怎麼辦？
- 如果組織辦公室因自然災害而受損，我們該怎麼辦？
- 如果組織成員的電腦或電話等裝置遺失或被盜，我們該怎麼辦？

透過這些提問，相信你腦海已經浮現一份資源聯絡清單和一些作法了！將這些資訊寫入「緊急因應」機制文件檔時，須確保這些資源都是「可聯絡的」，並且依序列出求救的聯繫流程。經過幾次演練 (或真的使用！) 和排除執行障礙，並搭配定期的檢核與操演，如此一來，有效的資訊安全因應機制就成形了。

危機來了，怎麼辦？

資安求助資源

資安攻擊所導致的傷害，除了在線上發生，有時也會延續到線下。若攻擊發生的當下，直接威脅到個人生命和資產安全，務必以生命安全為最高保全概念，其次才是資產。

在台灣，若在地的警局、醫院都還是值得信賴的情況下，撥打 119 (醫療救護專線) 或 110 (警察專線) 來獲得第一時間保護為最佳。記得事先備妥醫療、人身安全的資源清單，且讓組織內的其他人都知道放在哪裡。

若就數位空間內的受損，如帳號遭駭、資料竊取、網路斷網、網站侵占等，雖說人身安全當下沒有可見危機，但仍須立即向資安專家求援，以確認到底是什麼攻擊、如何止損、後續如何因應及防禦，以確保傷害不會進一步擴大，甚至威脅現實生活中的人身及資產安全。

國際上，應對緊急資安狀況有 AccessNow 的 Helpline 資安專線 [30] 提供全球 24 小時的緊急因應服務。他們提供多語服務，但目前沒有中文，台灣人若求助，仍以英文通報為主。在台灣，我們推薦求助者直接與 Civil Society Cyber Shield (CSCS) 聯繫。CSCS 這個資安社群以「扮演科技人士和公民社會的橋樑，提升公民團體使用資訊科技的安全」為目標，由一群資訊和資安背景的志願者組成，透過官方聯絡信箱 contact@cscs.asia，可向他們尋求以下協助：

1. 資安培訓：

   培訓組織人員資安知識，包含基礎概念、網路原理、電腦安全、手機安全、線上帳號安全等等。亦可依不同團體實際需要提供客製化的進階主題，例如 CSCS 曾設計並提供「 駭客網路監控技術的實際演示 」。建議培訓與健檢要一起執行，否則成效有限。

2. 設備健檢：

   講師帶領組織人員檢視電腦、手機、組織公用設備 (WiFi 基地台、印表機、網路硬碟等) 的安全性設定，並給予調整建議及教學。

3. 資安事件諮詢：

   提供緊急或非緊急事件處理的建議，例如網站被入侵、帳號盜用等等。但不提供維運管理的服務，這需要由組織自行處理或是聘僱專業的外包廠商負責。

CSCS 是志願者團體，其回覆依照緊急程度，將在 1~2 週內回應。若你有更緊急或是其他更多想尋求協助的事項，請直接與本書作者 —— 開放文化基金會 (hi@ocf.tw) 聯繫，以銜接求助者與更多可用資源的窗口。

---

30 AccessNow 資安專線 (Digital Security Helpline) : https://www.accessnow.org/help/

結　　語

結語

從了解數位安全是什麼，到風險評估、四大單元課程：瀏覽器選擇、密碼管理、網站安全、備份 321，最後匯聚成數位安全的緊急因應機制。本手冊所提的概念和建議，除了數位安全的技術知識、基礎概念之外，我們反覆提及組織成員的溝通和定期訓練。組織裡的每個人都是構成安全的一份子，就像砌成屋頂的瓦片，不用最高級的材質也可以遮風避雨，但只要少了一片瓦，就如同組織遺漏了一名成員，雨水就可能灌入屋內並造成損失。

最後，本手冊整理了六個關鍵要點，為讀者做最後的複習：

1. 數位安全能保護的，不只是網站、資料、信譽，更能保護組織中的「人」和使命。
2. 面對數位安全防禦及因應，首先，要先了解組織或個人主要想保護的是什麼？
3. 制定組織的四大數位安全守則和緊急應變計畫
   - 針對瀏覽器選擇、密碼管理、網站安全、備份 321 這四個層面，蒐集在組織與個人日常生活中能完善的事項，並記錄在文件檔中。
   - 集體討論可能發生的事件，並在事件發生前做好「事發 / 事後」的應對方案。
   - 將應對方案寫下來，連同緊急聯絡清單都要記錄在文件檔中 (可以是同一份檔案或不同檔案)。
4. 定期檢視，但更重要的是時常演練。
5. 確保每位成員都知道組織在事件發生後如何聯繫，不同角色該做什麼事。
6. 緊急聯絡清單是一個列表，內容包含數位安全資源、人身安全資源之外，更有可能是法律、情緒或社會支持等資源。

附錄一：開源瀏覽器下載／安裝流程

若使用電腦，前述注重隱私的 Firefox、 Brave、 LibreWolf、 Tor 四種軟體都只建議從官方網站下載，即

https://www.mozilla.org/zh-TW/firefox/new/

https://brave.com/zh/download/

https://librewolf.net/installation/

https://www.torproject.org/

記得選擇符合自己作業系統 (Windows、MacOS) 的版本下載，直接點擊就可開始安裝。千萬不要從任何免費軟體介紹網站下載，因為無法保證這些安裝檔案在官方網站之外是安全的。

如果使用的是手機或平板等行動裝置，只建議 Android 裝置從 Google Play 商店或 iOS 裝置從 App Store 直接搜尋瀏覽器軟體名稱並下載安裝。這些由官方管理的商店會定期檢查檔案的安全性，絕不建議從其他地方下載安裝檔案再移入裝置使用。

技術支援／求救方法

以上介紹的開源與安全瀏覽器，都有繁體中文版可使用，只是各家瀏覽器的官方疑難解答平台的中文化程度各異，例如 Firefox 的中文化發展較久，有相對豐富的中文志工在官方的疑難解答平台上回應各式問題。不過，自動翻譯功能日漸進步，使用者可以放心嘗試有隱私與安全保護功能的其他瀏覽器。

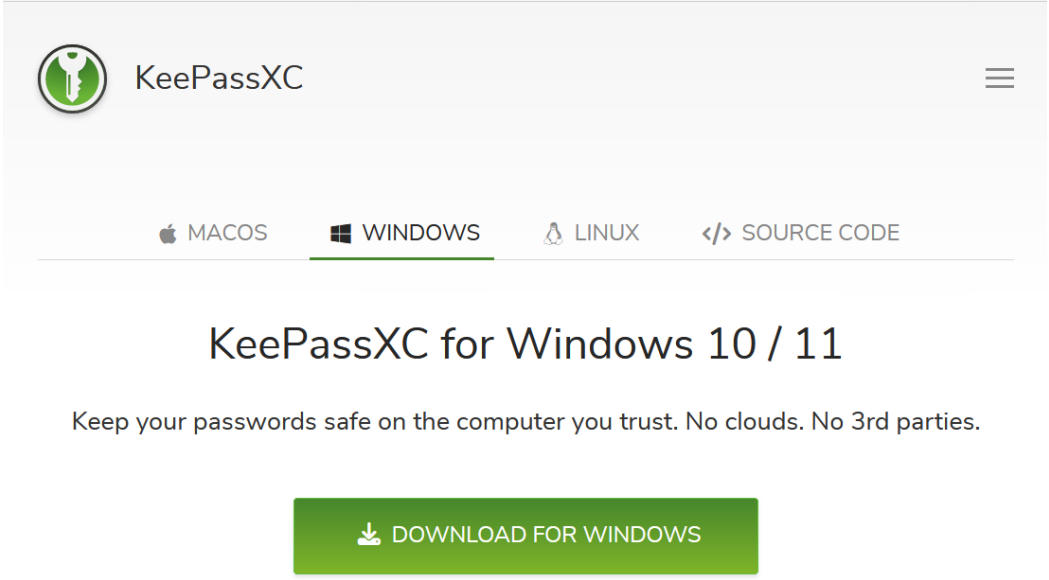
	疑難解答平台	語言
Firefox	https://support.mozilla.org/zh-TW/products/firefox	繁體中文
Brave	https://support.brave.com/hc/en-us/	英文
LibreWolf	https://librewolf.net/docs/faq/	英文
Tor	https://support.torproject.org/zh-CN/	簡體中文

附錄二：KeePassXC 使用方式

KeePassXC 是一個嚴格加密的密碼管理器，有繁體中文版本，使用者可以輕易上手。請跟著我們花 5 分鐘進行設定吧！

下載／安裝流程　在電腦安裝

切記，下載工具程式務必要從官方網站下載，以避免下載到來路不明、被暗藏後門的軟體。進入 KeePassXC 的官方網站（https://keepassxc.org/），在首頁就可以看見下載連結，依你的電腦作業系統下載即可。記住，KeePassXC 與其他商業密碼管理器不同，是免費提供下載的，如果你發現要註冊、付費，那肯定是搞錯軟體了。



圖： KeePassXC 下載

下載後，就可以直接點擊安裝檔案，按照軟體提示依序進行。安裝完成後，就可進入使用環節。

附錄二：KeePassXC 使用方式

在手機或平板安裝

如果你想安裝 Android 或 iOS（蘋果）的版本，它們與電腦版本的名稱不同。官方網站的指引（https://keepassxc.org/docs/）建議在 Android 使用 KeePassDX[31] 與 KeePass2Android[32]，在 iOS 則是 Strongbox[33] 與 KeePassium[34]。他們都是 KeePass 家族的成員，可以互通使用，管理密碼的方式也相近。本文後續以介紹電腦裝置上的 KeePassXC 為主。

首次設定

KeePassXC 的運作方式是，經由這個軟體產生一個加密的文件檔案，稱為資料庫（副檔名會是 .kdbx），只能由使用者設定的主要密碼解鎖。當你首次打開它，軟體會詢問你是否「建立新資料庫」或「開啟現有資料庫」，或是從其他的密碼管理器匯入資料庫。如果你是第一次使用，還未存入任何帳密，或是要設定另外一組帳密儲存，以下為「建立新資料庫」的流程：

1. 為新的密碼資料庫命名，可以加上描述，以免自己遺忘內容。

圖：建立新的 KeePassXC 資料庫

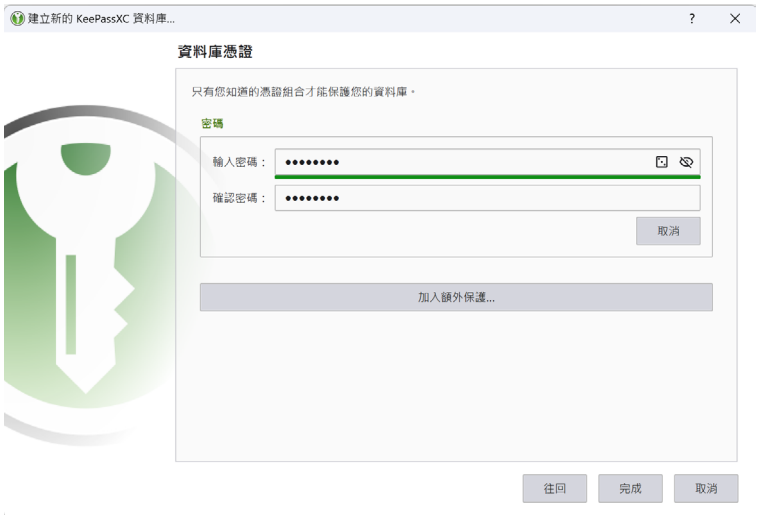
31 https://play.google.com/store/apps/details?id=com.kunzisoft.keepass.free
32 https://play.google.com/store/apps/details?id=keepass2android.keepass2android
33 https://apps.apple.com/us/app/strongbox-password-manager/id897283731
34 https://apps.apple.com/us/app/keepassium-keepass-passwords/id1435127111

附錄二：KeePassXC 使用方式

2. 為這個資料庫提高加密層級，這可以阻礙有人將資料庫檔案盜走後的解密工作，提高他們需要解鎖的時間成本。

圖：建立新的 KeePassXC 資料庫的加密設定

3. 為這個資料庫設定「主要密碼」，可以說是最重要的事情，如果遺忘主要密碼，裡面的東西就再也無法取出。



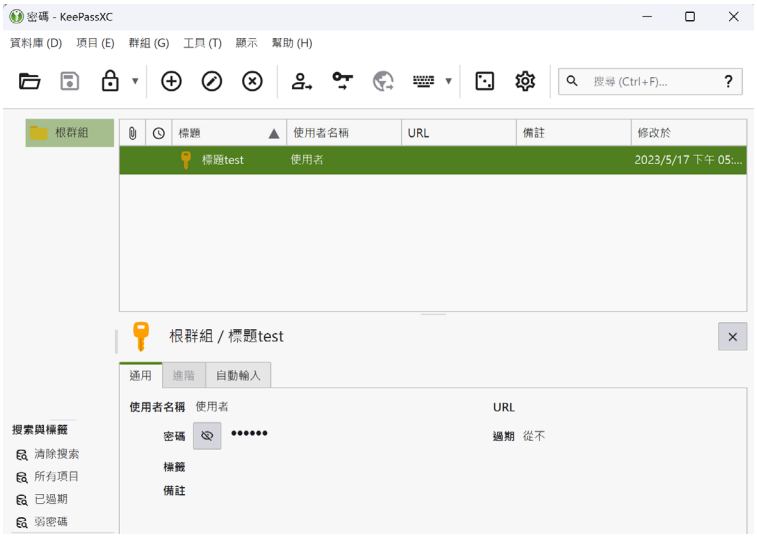
圖：為新的 KeePassXC 資料庫設定主要密碼

附錄二：KeePassXC 使用方式

開始使用

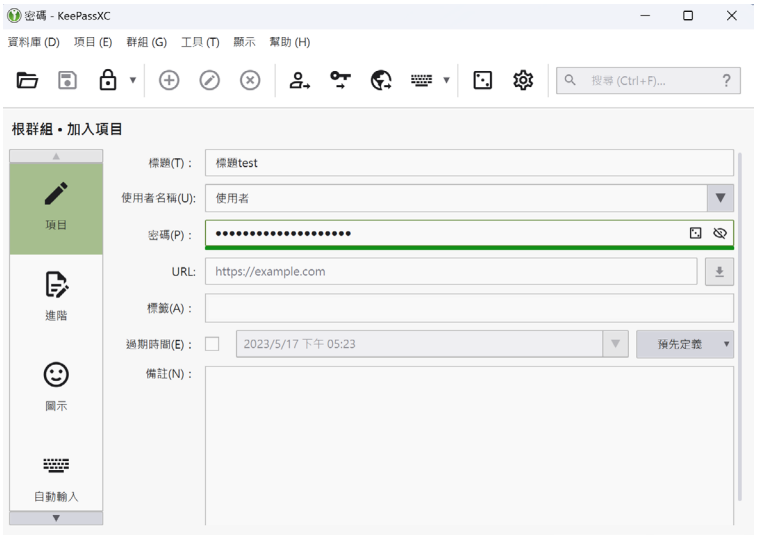
每次打開 KeePassXC，你要以主要密碼解鎖資料庫。解鎖之後，可進行以下動作：

1. 首頁裡條列各個帳號的管理項目，點擊要尋找密碼的帳號，就可以檢視或準備複製貼上密碼。



圖：在 KeePassXC 資料庫中尋找帳戶密碼

2. 如果要新增某個網站或服務的帳號、密碼，就要到工具列「新建項目」



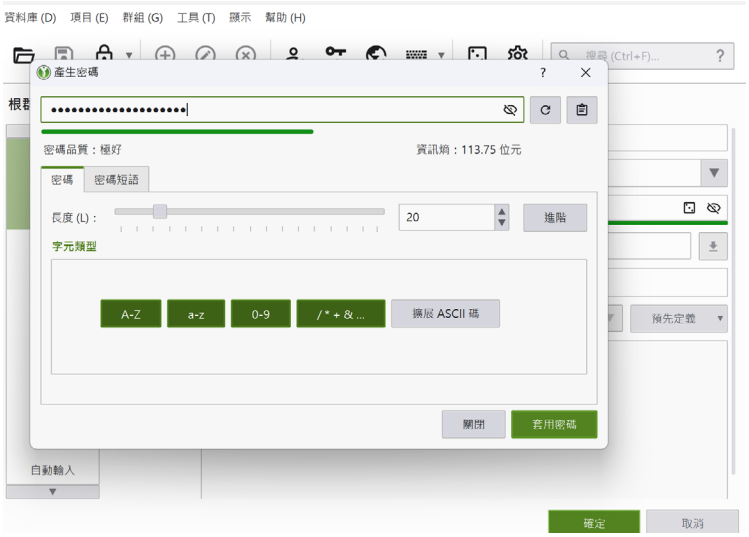
圖：在 KeePassXC 資料庫中新增帳戶密碼

a. 輸入標題
（例如某購物網站）

b. 使用者名稱
（也就是你在該服務註冊的帳號）

c. 產生新的密碼。
可以自行輸入，也可以隨機產生。

附錄二：KeePassXC 使用方式



圖：在 KeePassXC 資料庫中產生隨機密碼

3. 在工具列的「編輯項目」：可以更改項目的標題、使用者名稱、修改密碼。
4. 在工具列的「刪除項目」：可以將所選的項目刪去。
5. 如果需要修改 KeePassXC 的設定，可以到工具列的最後一個「設定」進行：
   - 例如，在「通用」的地方，可以設定開機後啟動管理器。
   - 或是在「安全」的地方，設定複製密碼之後自動消除的時間，以避免使用者不慎在公開的聊天訊息貼上自己的密碼。
   - 想在瀏覽器裡直接連結密碼管理器，可以到「瀏覽器整合」為 Firefox、Google Chrome、Brave、Edge 等主流的瀏覽器下載並安裝外掛，讓你可以直接在瀏覽器裡面複製貼上密碼。

當你使用過前述 1~4 的步驟，就已經掌握密碼管理器的主要功能，可以讓你的生活及工作更輕鬆也更安全。

在新電腦或是其他裝置上設定

1. 換了新的電腦，要繼續用 KeePassXC，就要記得搬遷資料庫到新電腦裡面，也就是那個副檔名為 .kdbx 的檔案。
2. 在新的電腦安裝 KeePassXC 之後，初次開啟時選擇「 開啟現有資料庫 」。
3. 輸入你原先為這個資料庫設定的主要密碼，即可開啟使用。

密碼管理器讓你可以再也不需要記住所有服務的帳號密碼，但是請千萬要記得 KeePassXC 的主要密碼，並且保管好電腦裡的密碼庫檔案 (也就是 .kdbx 檔)。你可以在不同地方備份它，或是使用前文提及的 Android 或 iOS 版本的 KeePass 家族成員來開啟它。

切記，一旦忘記主要密碼，或遺失了資料庫檔案，你的諸多密碼就會消失，戒之慎之！

CSOs 數位防禦手冊 — 注重隱私與安全的開放原始碼工具

作者： 財團法人開放文化基金會

編輯：林倚安

美編設計：張文蘊

發行人：財團法人開放文化基金會

信箱：hi@ocf.tw

網址：https://ocf.tw/p/csodefense/

2023 年 五月 初版

2024 年 七月 二版一刷

ISBN : 9789869570862

OCF_

2024 / 7 月