

數位足跡建構數位身分- 便利? 風險? 如何避免?

社團法人台灣 E 化資安分析管理協會
(ESAM, <https://www.esam.io/>)

中央警察大學-資訊密碼暨建構實驗室(ICCL)

<本文作者:

1. 社團法人台灣 E 化資安分析管理協會(ESAM, <https://www.esam.io/>);
 2. 中央警察大學資訊密碼暨建構實驗室 (ICCL)，1998 年 12 月成立，目前由王旭正教授領軍，並致力於資訊安全、情資安全與鑑識科學，資料隱藏與資料快速搜尋之研究，以為人們於網際網路(Internet)世界探索的安全保障 (<https://sites.google.com/site/iccltogether/>)。>
-

摘要

隨數位應用科技發展與 Covid-19 疫情的陰影下，生活大小事不可避免地轉移到數位世界中。然而隨著數位應用擴展，特別是在社群應用快速成長下，使用者在數位環境所留下的足跡，包含帳號密碼、瀏覽記錄、訂閱推播及交易資料等等，也更加頻繁且多元。使用者於網路世界留下的足跡積累所形成的數位身分，讓網路應用更加了解使用者，讓使用者能更精準地找到想要的資料，減少了使用數位產品的障礙，更讓網路購物行銷與社群媒體興起，成為社會了解潮流脈動的來源。然而數位足跡也承擔著風險，有心人士一旦將資訊足跡被蒐集完整，個人或是組織的資訊安全就受到高度威脅。本文介紹檢視自我網路資訊足跡的網路資源，供讀者保護自身的數位資訊的選擇，減少不必要的數位資訊暴露，提升使用網路科技的安全性。

壹、前言

數位生活已經漸漸取代傳統生活模式，每個人起床的第一件事已經是拿起手機，確認天氣概況、今日行程及無止盡的文字訊息，特別是在 Covid-19 疫情爆發後，減少傳統社交的生活模式直接衝擊所有人的生活節奏，數位科技應用加速發展，各類數位資訊直接強制進入生活，例如：採用餐飲外送數位平台處理三餐、居家上班上課機制成為主流趨勢，更有各類無止盡的視訊會議。以往已經習慣網路生活模式的人更加沉浸其中，以往排斥網路生活的人則必須認真面對加入現況，數位生活的比例直接爆炸性增長。

而數位生活留下的數位足跡也隨著這樣的模式更加頻繁且多元，進而累積使用者的數位身分，隨之而來的便利生活運用也越來越廣泛，而如何讓個人的數位足跡避免過度暴露或是適時地減少也變成重要課題，本文首先介紹數位足跡的便利運用及相對的風險，後續介紹檢視自我網路資訊足跡的網路資源，供讀者保護自身的數位資訊，減少不必要的數位資訊暴露，提升使用網路科技的安全性。

貳、數位足跡的定義與應用

舉凡使用者於數位網路世界所做的每一個動作都可稱為數位足跡，不論是註冊網站會員輸入帳號密碼、輸入關鍵字搜尋網頁、瀏覽各項網站、在社群網站分享生活點滴、在直播主的直播平台+1、給 Youtuber 的影片下訂閱按讚留言等等所有現行網路世界的日常行為，都逐漸累積成為使用者在數位世界中的身分累積。

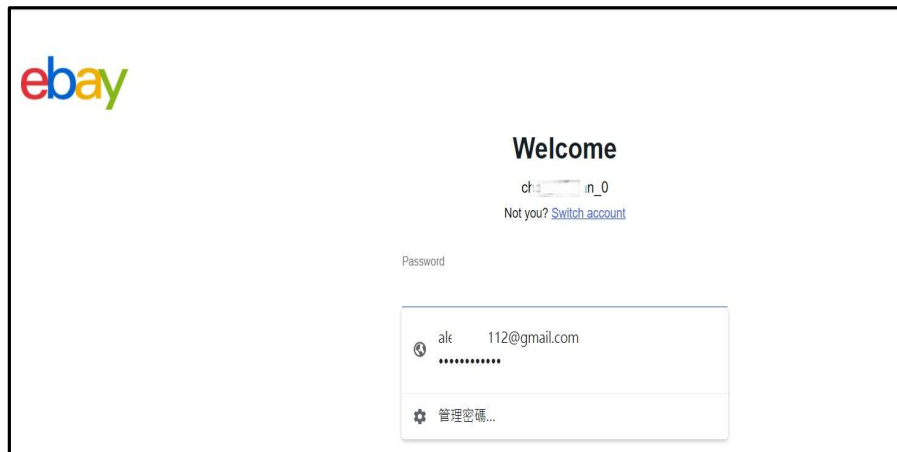
隨著數位人口激增，數位足跡的激增與巨量記錄當然給了許多於數位世界生活的便利性。以個人使用而言，網路資訊量持續激增，使用層面越來用廣泛，如何精準地找到想要的資料，或是減少使用數位產品的障礙變得很重要，舉例來說，各類網頁瀏覽器開始紀錄著個人搜尋過的關鍵字與瀏覽記錄，於下次找資料時就

能節省時間，以圖一為例，即是透過瀏覽器搜尋資料時的瀏覽器足跡，可以發現不需輸入完整的關鍵字，網頁就記錄了近期使用的可能關鍵字與網頁記錄提供點選。



圖一、網頁搜尋記錄 資料來源：chrome 瀏覽器

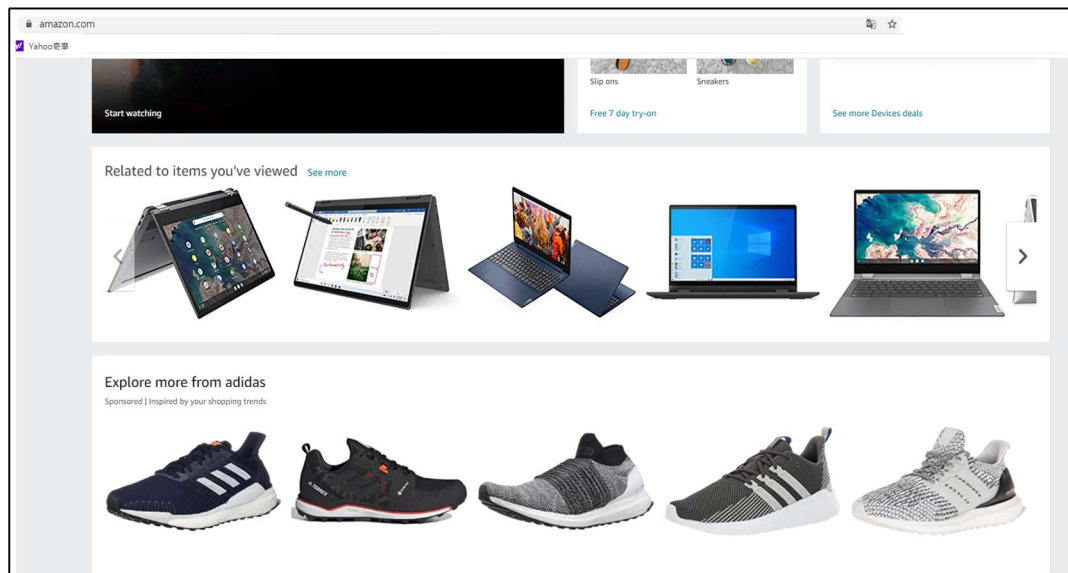
另外瀏覽器也可以幫助使用者記錄各類不同的網站會員的帳號密碼，減少使用上障礙，如圖二，各類需要會員資格的網站，都可以選擇在使用者使用的瀏覽器中記錄使用的帳號密碼，減少記憶與輸入的困擾。



圖二、自動填入帳號密碼 資料來源：chrome 瀏覽器

除了個人使用外，從科技產業發展角度而言，數位足跡的激增更是帶來無限的行銷商機及網路聲量分析產業，網路使用者的每一個操作步驟直接都代表了一個傳統問卷調查的回答，以行銷商機來看，從什麼入口網站過來?使用何種設備?

連入網站後是無目的隨意點擊瀏覽，或是直接到想要的產品購物？最常停留在哪個網頁？最常在某一網頁離開？是從哪個實體地理位置而來？最常被瀏覽的時間段？等等的相關資料，都透過使用者於網路購物過程中完整的記錄，當購物完成後再將你的購物記錄進行分析，如：花了多少錢、是買何種商品類別嗎？等等，有這些資料後，就能更精準地投放給消費者需要的產品推薦，各類購物網站平台比較的就是誰能夠將數位足跡資料分析的更加精準，除了保有既有客群，更能愛廣大網路世界中，找到更多未來的潛在顧客，給其看到自家商品，舉例來說，筆者最近於亞馬遜網站搜尋過筆記型電腦與運動鞋，網站就會在你瀏覽的亞馬遜網站首頁上推播出相關筆記型電腦與球鞋相關訊息。



圖三、購物數位足跡 資料來源：Amazon

而近年討論最為廣泛的網路聲量分析產業，更是數位足跡的最佳受益者，傳統世界中想要知道潮流脈動需要透過報章雜誌媒體，而數位世界中到處都是自媒體，到底誰是網路資訊走向為何？，變得難以辨認。而透過收集巨量數位足跡分析生活潮流脈動的產業已經相當成熟，目前已有許多企業開發出數據分析平臺，以臺灣在地而言，如：Qsearch 的 Trend+ 社群分析與網路聲量工具、i-Buzz 的 i-Buzz VOC+產業口碑數據庫、意藍資訊的 Opview 社群口碑資料庫及 DailyView 網路溫度計等等提供相關分析資訊，提供各項產業走向數位發展有較為精準的數

據依據。



圖四、Opview 社群口碑資料庫 資料來源：意藍資訊

參、數位足跡的風險

當然數位足跡絕非只被正向運用的優勢，當風險較高或是過多的個人資訊暴露於網路世界中，受到駭客或是有心人士進行網路攻擊機會變高度提升，一旦資訊足跡被蒐集完整，個人或是組織的資訊安全就受到高度威脅。

以個人而言，數位資訊需求持續增長，常見的個人數位足跡風險，例如：許多人習慣使用同樣的帳號密碼設定通行於各網站，大型入口網站有基本的安全規範，但對於資安投資不夠的網路平臺一旦被破解後，同樣的帳號資訊就洩漏出去，成為個資於暗網販售；另外，使用社群服務時，時常過度分享個人資訊，且並無進行隱私權設定，限制分享的對象，因此分享的個人資料，包括照片、姓名、生

活大小事等等，都能讓有心人蒐集；近來的各大小購物社團、群組也可能是足跡破口，疫情期間各類便利商店、傳統市場店家成立許多通訊群組辦理送貨到府的服務，無形間個人的住所與金融資訊便流傳於無安全防護的通訊群組。

對於企業組織而言近來常見的資訊暴露風險頻傳，以 KPMG 安侯建業於 2021 提出的臺灣企業資安曝險大調查中便指出台灣許多企業數位足跡廣泛，導致企業內部資訊不當揭露，其中可能是網域混雜錯亂、內部員工有心/無心的資訊洩漏、企業私有雲端協作平臺組態設定錯誤都可能造成企業高度曝險，再者也提出當企業的數位足跡曝露的數目越高，企業網路防護所得到的分數也越低，因此不得不去面對數位足跡防護的重要性。

肆、可運用減少數位足跡網路資源

而以一個面對數位應用持續發展的使用者，使用者要能夠完全沒有數位足跡是不可能的事，而如果有意願嘗試減少不必要的數位足跡，或者是想好好管理自我數位生活，網路上已經有許多在既有的資訊服務網站可以進行隱私操作設定可供使用者參考外，我們將介紹一些網站資源可以檢視或降低數位足跡的選擇。

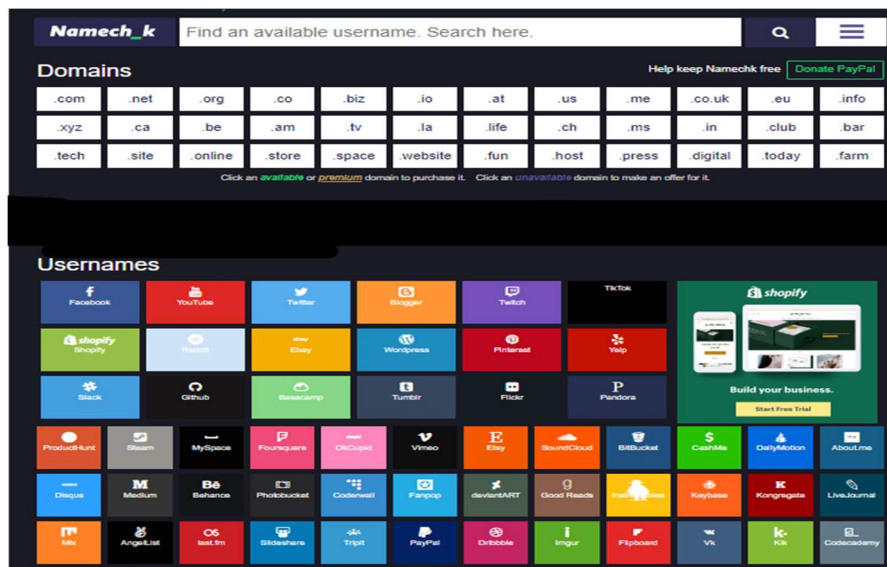
一、增加數位足跡安全性

(一)帳號密碼的暴露檢視

數位足跡中的帳號密碼絕對是使用者最需要萬全掌握的內容，以目前的數位應用來說，雖然很多大型金融服務與購物網站已經導入多因素驗證，例如除了需要需要驗證外，更需要綁定手機號碼或是電子郵件進行一次性驗證

碼的程序等，但多數的網站會員機制仍是以帳號密碼單一驗證為主，因此如何檢視自己的帳號密碼是否有高度暴露風險絕對是最重要的。

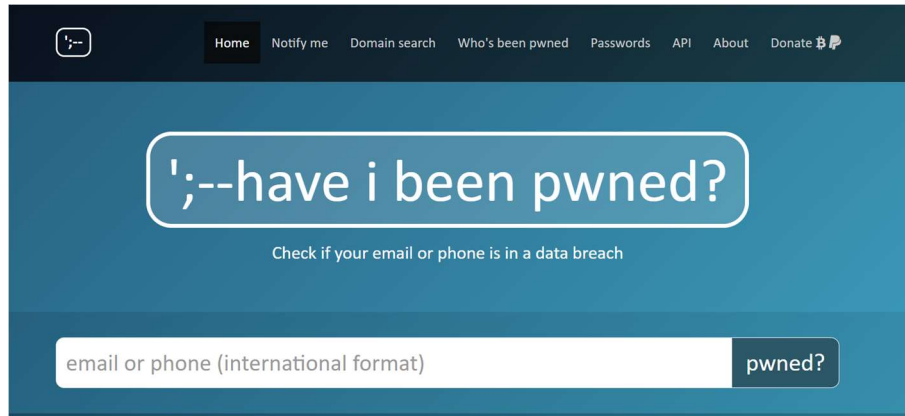
帳號而言，使用者通常都是習慣使用固定的帳戶名稱，會發生最近流行什麼數位應用就去註冊使用，之後喜新厭舊可能就不再使用，但使用者就直接忽略原本的註冊資料，此時可以透過 Namechk 網站(namechk.com)進行使用者帳號的檢視。



圖五、namechk 網站

Namechk 網站原本主要為目的原為商業用途，檢視使用名稱是否已經被註冊，我們可以用來查看自己常用的帳號是否有曾經註冊在哪些社群網站但已經被遺忘了，進而考量是否可將不再使用的閒置帳號移除

而密碼使用部分，除了基本的概念必須減少使用弱密碼的樣態，就是容易被有心人士暴力破解或是容易猜出的密碼設定，例如使用個人的基本資料，包括生日、手機號碼，或是簡易的鍵盤排列或替換符號，例如:lqaz@WSX、p@ssw0rd 等等，使用者可以使用 Have I been pwned? 網站進行測試。

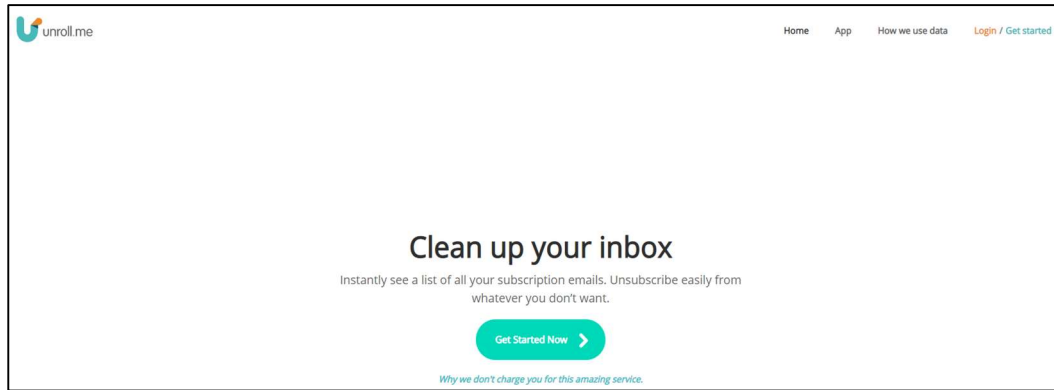


圖六、Have I been pwned?網站

Have I been pwned? 網站主要為蒐集近年被駭客竊取在網路上的使用者清單資料，首頁輸入使用者 e-mail，即比對這些被竊取的資料庫中裡有沒有相對應的資料，其中網站中也有個密碼清單，是曾經暴露於清單資料中的密碼，計有 6 億 1 千多萬個現實世界密碼，可以讓我們進行比對，比對後並非告訴我們的密碼資料洩露了，而是讓我們考量是否還要繼續使用這樣的密碼設定，因為這類曾經暴露過的密碼使用上風險要大很多，考量進行更換以免曝險。

(二)電子郵件訂閱管理檢視

如果說帳號密碼是屬於最重要的隱私性數位資料外，電子郵件則是網路使用者於公開性數位資料最為重要的溝通媒介，就如同一個人在數位世界的數位地址，除了既有收發重要訊息外，常常因為臨時的應用需求而訂閱特定網站服務資訊推播，而使用者的 email 資訊就一直隨著訂閱資訊增長而持續廣泛存在網路世界中，風險自然就增加，此時可以透過 Unroll.me 網站進行 email 帳號清理。



圖七、Unroll.me 網站

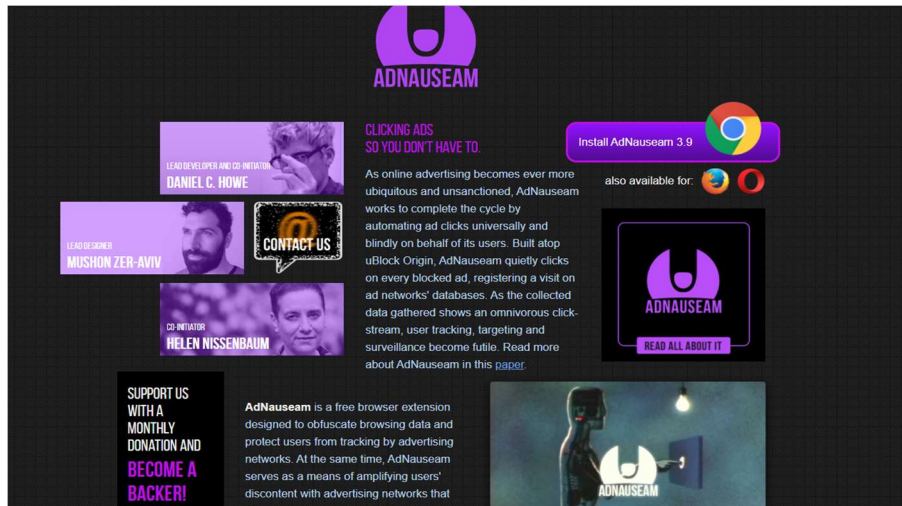
Unroll.me 主要為 email 信箱訂閱整理服務，支援現行常用的 Google、Yahoo 及 Outlook 信箱服務，透過填入 Email，可協助檢查 email 信箱裡現有的網路資訊訂閱，讓使用者快速從清單上移除。

二、混淆數位足跡

除了透過增加數位足跡的安全性外，使用者若想避免數位足跡及隱私被濫用外，有研究者提出可以使用「數據下毒」的策略，透過提供無意義或有害的使用記錄給網路服務平臺，讓網站無法認清使用者的使用記錄；以下可分成被動式與主動式的干擾應用。

(一)被動式干擾追蹤

使用者可於網頁瀏覽器安裝插件，定期發出隨機的搜尋指令，以隱藏使用者真實的搜尋，因此對方要精準地搜集數位足跡轉化或組合成使用者的數位身分定位困難度將大幅提升，常用干擾足跡的瀏覽器插件有 AdNauseam 及 TrackMeNot。



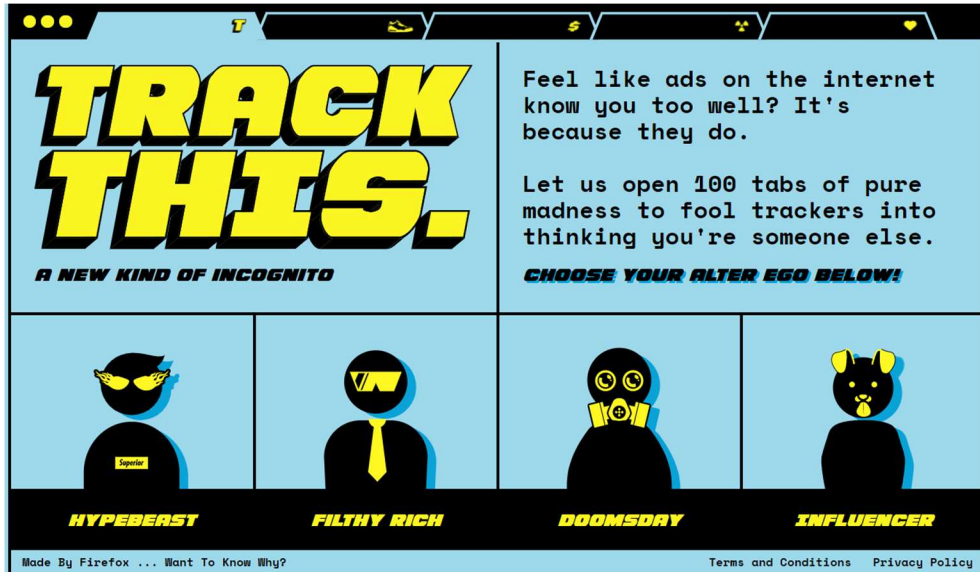
圖八、AdNauseam 網站



圖九、TrackMeNot 網站

(二)主動式干擾追蹤

除了安裝被動插件於瀏覽器，也可考慮使用主動型的網路隱身網站進行混淆網路足跡追蹤，以 Track This 網站為例，以透過一次性開啟 100 個瀏覽分頁方式，假扮為特定的使用者，如此一來可以快速短暫的投放給網路足跡追蹤以混淆網路身分。



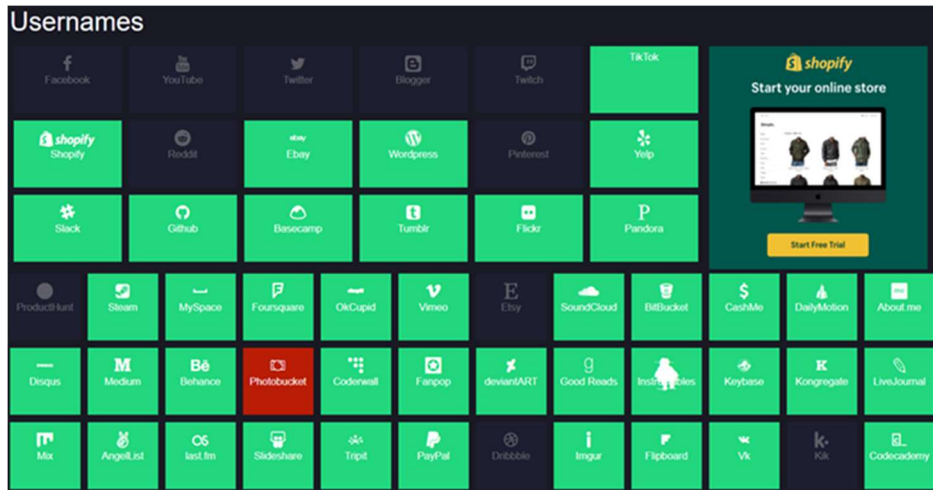
圖十、Track This 網站

伍、情境模擬

華仔一家人近來隨著疫情影響，大人們開始居家辦公，家中小孩也因為疫情關係都在進行居家視訊教學，除了不同的視訊與遠距辦公軟體設定註冊安裝，也為了減少出門，開始嘗試外送、線上採購食物等等，參加了許多從未參加過的社群平台，哪邊特價就往那邊註冊，哪邊有優惠方案就往哪邊去購物，也開始習慣在不同社群平臺討論生活大小事，以解居家不能出門之苦。

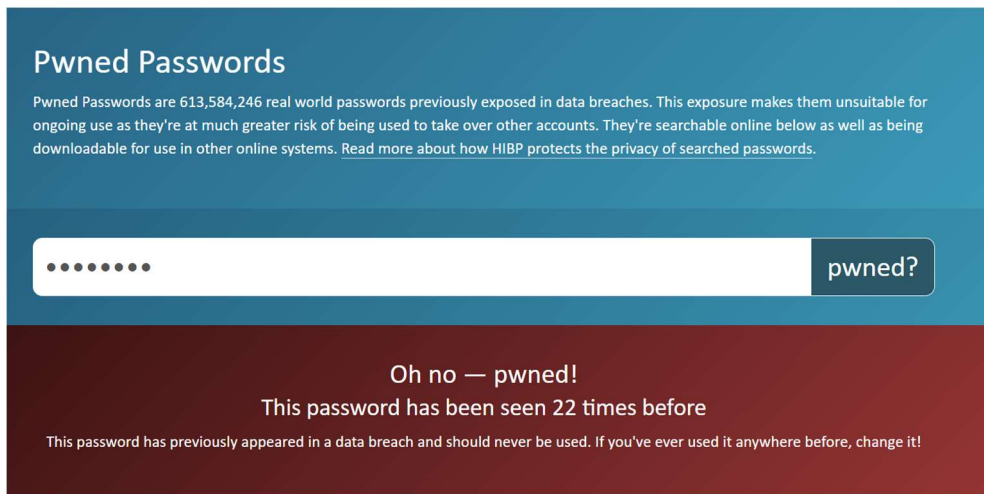
漸漸地，華仔發現，常用的電子郵件信箱開始有無止盡的廣告信，瀏覽社群網站看到的廣告不斷的讓它分心，直到有一天發現一些好久沒用的社群平台開始寄 email 給他詢問她是不是要重新設定密碼，才意識到自己在網路世界裡留下了好多資料，似乎應該要好好整理一下自己的數位足跡了。

華仔首先去了 Namechk 網站，用自己的帳號名稱進行了搜尋(如圖十一)，顯示暗色背景代表該網站帳戶已經有註冊使用，華仔才發現自己曾經註冊了好多社群網站，才慢慢地把一些鮮少使用的帳戶進行關閉。



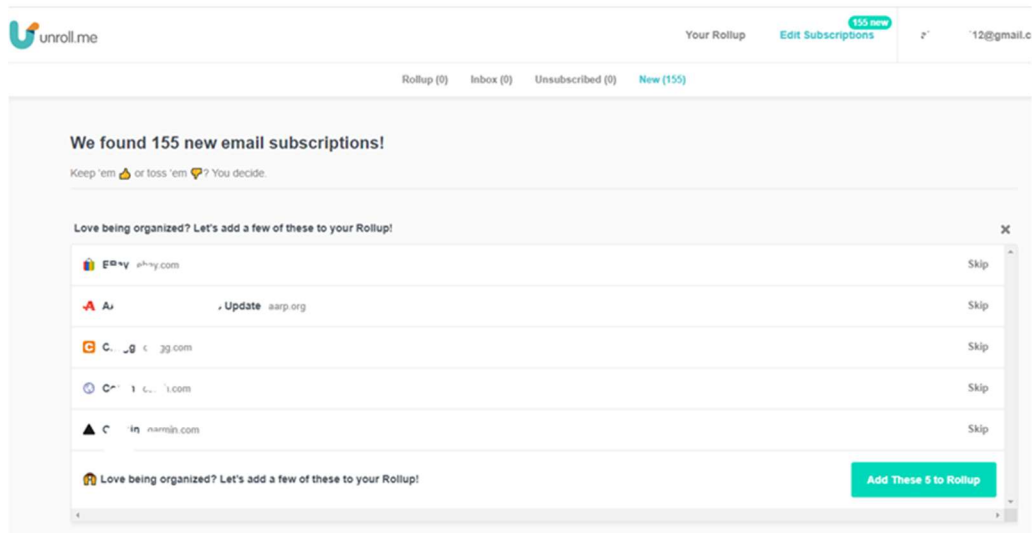
圖十一、Namechk 網站掃描結果

緊接的華仔又去了 Have I been pwned? 網站，把自己常使用的密碼輸入搜尋看看，發現自己最常用的密碼組合已經在曾經被駭走的資料庫中出現了 22 次 (如圖十二)，趕緊修改密碼設定。



圖十二、Pwned Password 畫面

最後華仔去了 Unroll.me 網站，想好好整理一下自己的 email 帳戶訂閱，發現自己的帳號內有 155 種訂閱(如圖十三)，平常常用的也沒幾項，只好認命地慢慢檢視刪除，重新好好整理一下自己的數位資料，也開始慢慢考量是不是應該透過一些瀏覽器插件或是網站來減少被數位追蹤的可能。



圖十三、Unroll.me 網站

陸、結論

數位足跡建構出使用者在網路世界的身分角色，而數位應用已無限延伸至人類的現實生活，此時此刻談論如何完全不使用數位資訊進行生活已經是不可能的事，而應該是使用者要認清要如何妥善管理數位資料，減少暴露的風險，避免遭受有心人士非法利用。本文中介紹了使用者帳號密碼與電子郵件訂閱管理的自我檢視方式，也介紹了主被動避免網路足跡被濫用的策略，藉此能在數位世界中感受便利時，也能在意隱私安全的重要，讓數位科技更能貼近你我生活。