目錄 Contents

互聯網每天都在改變，相信今天的互聯網世界跟 10 年後將會完全不一樣，未來互聯網的世界如何發展，將由新一代年輕人主導。先培養良好素質，才能把互聯網推向一個新境界。

安全上網
智能時代的風險與自我保護

Chapter 1 :

互聯網應用及網絡安全概要

1.1 網絡足跡

如果你在沙灘上漫步，回頭一看，相信你會看到不少屬於你的腳印。腳踏在沙上留下腳印看來是一件平凡事，你又有沒有想過，我們在互聯網亦會留下不少網絡腳印？

網絡足跡（online footprint），又稱數碼足跡（digital footprint），是指所有互聯網使用者在使用互聯網應用時所留下或產生的訊息，包括你的網上帳號、在論壇或社交平台所發表的文章、利用即時通訊軟件發出的訊息等。這一切一切，都是你的網絡足跡。

互聯網發展得越成熟，我們在參與所有互聯網活動時留下的足跡便越多。原因很簡單，要發展互聯網，就需要了解所有互聯網使用者的背景、喜好、習慣，甚至期望。我們都在不知不覺間透露了這些資訊或想法給互聯網應用提供者，因為資訊交換才是發明互聯網的主要原因。

在 Web 1.0 時代，互聯網使用者只可在互聯網上瀏覽網站，而網站提供者都是單向地為瀏覽者提供資訊。既然是單向，用家不能在網站留下訊息。當時幾乎沒有人提及網絡足跡這回事，因為對那些網站提供者來說，瀏覽量高已經是一個大成就，還未有想過要作進一步的資料收集。

到了 Web 2.0 時代，世界變得不一樣。大部分網站不再單一地向用家提供資訊，而是變得可讀及可寫，讓用家作為互聯網應用一部分並參與其中。我們可以在網上隨心所欲地留言，大膽分享意見及看法，亦可跟身邊朋友分享日常點滴。而且模式亦非常多元化，除了文字，還有圖片、聲音及影片。就是這種多元化模式，讓 Web 2.0 為世界帶來一個新熱潮，一眾網民一步一步墮進互聯網世界而不能自拔。這熱潮當然令我們留下不少網絡足跡，而這些腳印亦令我們看見互聯網未來的發展方向。

過了一段時間，互聯網服務提供者在想，是不是可以把大量用家的數據收集起來並進行分析？而且網絡世界充斥著各式各樣的資訊，如何做到精準搜尋，並把用家跟他們所喜愛的，在互聯網世界連在一起？近年，隨著人工智能及大數據技術發展越趨成熟，成就了 Web 3.0 時代。有不少互聯網平台加入這些元素去提升用家體驗，例如平台已經猜到你在找尋什麼，或者你需要什麼，它們會直接在平台顯示出來，讓你不用再花時間四處搜尋資料。這些功能，除了技術成分之外，沒有了你的網絡足跡，絕對成不了事。

在互聯網上進行任何活動都會留下數碼紀錄，有些是我們主動提供的，另一些是被動地給收集的。網絡足跡主要分為兩個類別，分別為主動式和被動式。

主動式網絡足跡（active online footprint）

這個類別包括所有由你提供並在網絡公開共享的訊息，包括：

- Facebook、Instagram 帖文
- YouTube 影片
- 即時訊息及電郵
- 網絡表格所輸入的資料等

以上一切內容都是你在互聯網透過某個平台主動提供的。可能你會說這些訊息都是跟身邊朋友共享為主，但是一旦在互聯網世界公開發布，除了你所想的對象會看到外，也有不少個人或組織看到的。例如你在 Facebook 讚好了某個專頁或發文，原來你的朋友亦有機會看到。雖然可以在 Facebook 修改個人私隱相關設定，但是很多用家都不會或不懂如何更改這些設定，結果其他人都知道你的一舉一動。

別輕視這個情況，後果可能非常嚴重。試想想，他日當你投身社會尋找工作時，所有未來僱主都可以在網上查找你的主動式網絡足跡，從而了解你的人品、喜好，甚至對國家大事的立場等。有點驚嚇，對吧？從今天起，你在發帖文時會否謹慎一點？

被動式網絡足跡（passive online footprint）

這個類別則包括互聯網服務提供者在後台所收集的數據，包括：

- 網站或手機應用程式偵測你的位置
- 手機應用程式收集你電話中的其他資料（例如瀏覽紀錄）
- 各服務提供者收集你的網絡行為（例如讚好及留言）作分析，再向你推送合適的廣告等

這些「被動」資料都是各個部門或機構在後台「主動」收集的，目的是在你不知情（或不被打擾）的情況下，靜悄悄地記錄你的網絡行為，從而對所有服務使用者，甚至每一位服務使用者作多一點了解。

值得慶幸的是，暫時這些數據仍未能在公共場所被其他人作搜尋或瀏覽，因此在日常生活中不會出現很大問題。但是近年私隱問題被全球熱烈關注及討論，在世界各地，甚至部分地區已為此進行修改法例討論，期望為各大互聯網使用者帶來多一分保障。

1.2 網上帳號及保護

回到家門前，要進入屋內，必須用門匙或密碼才能將門打開。要使用各種互聯網服務，很多時都需要使用者先登記帳號，除了輸入基本個人資料，使用者需要想好在平台上一個獨一無二的使用者名稱及屬於這帳號的密碼。你所設定的密碼，在每個平台上都是一樣，還是各有不同？

根據網絡安全公司 Nordpass 早前自行統計並發布的「2021 年最常被使用的密碼排行榜」，公布了前 200 個最常被用家選為密碼的英文字及數字組合。這排行榜亦說明了密碼被他人公開、使用次數和破解所需的時間。按 Nordpass 所述，在 2.75 億個常用密碼中，只有少於一半的密碼具有獨特的特徵，其餘則由容易記住的組合組成。Nordpass 強調，如果你正在使用的密碼，在這排行榜中排行前 200 名，這個帳號有可能在「不到一秒內」被駭客攻陷。建議你立即去看看，如果發現這個情況，應立即更改該密碼。

前 10 名排名如下：

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567

破解密碼

我們不時會看到帳號遭盜用的新聞，其中一個主要原因就是該帳號密碼被破解。雖然現時已經出現很多保護使用者帳戶及密碼的方法，但是「道高一尺，魔高一丈」，很多不良網絡攻擊者借助一些簡單的工具就可破解使用者的密碼。

破解密碼方法主要分為以下兩個類別：

1. **暴力破解法：**因為大部分密碼都是由數字、英文字母及符號組成，所以破解者可以利用一組伺服器群組，把所有密碼組合逐一測試，直至成功為止。由於現時很方便就可以用上網絡雲端伺服器資源，所有互聯網使用者不用花時間去構建伺服器群組，只需支付相關費用便可使用由第三方提供的伺服器資源。坊間有研究指出，利用伺服器群組每秒可以嘗試 3,500 億個組合。以這個破解速度來計算，要破解一組 6 位密碼不用 5 秒，7 位密碼不用 7 分鐘，8 位密碼約 10 小時，9 位密碼約 40 天，而 10 位密碼則需要超過 10 年時間。說到這裡，你應該會好好想一個最少有 10 個位的密碼了吧！

2. **密碼清單破解法：**雖然暴力破解方法好像成功率頗高，但是有個嚴重問題，就是密碼越長，所需測試的組合越多，破解時間就越長。一旦密碼超過了某個長度（例如10個位），相信你不會等待10年時間來破解一個密碼。其實有個較為簡單的方法，就是使用「密碼清單」。密碼清單上存放著各種常見的密碼，同時亦會整合一些常用的日期和詞彙。如果破解者一直在使用自己的密碼清單作密碼破解，隨著破解的密碼量不斷增加，密碼清單所記載的組合量亦相對提升。一般來說，密碼清單越豐富，所涵蓋的常用密碼越多，快速破解的成功機會便越高。

由此可見，要創建一個安全密碼，長度是一個基本考慮因素，而且盡量避免使用常見詞彙。大家有否留意，在很多網站建立帳號時，有些系統會檢查你的密碼是「強密碼」或是「弱密碼」？原來密碼亦有強弱之分。

密碼強度

當大家了解密碼強度之定義及規則後，你亦可以創建屬於自己的強密碼。

先討論「弱密碼」，如果你正在使用以下規則創建密碼，即使是一部分，亦已經有一定風險，建議更改該密碼：

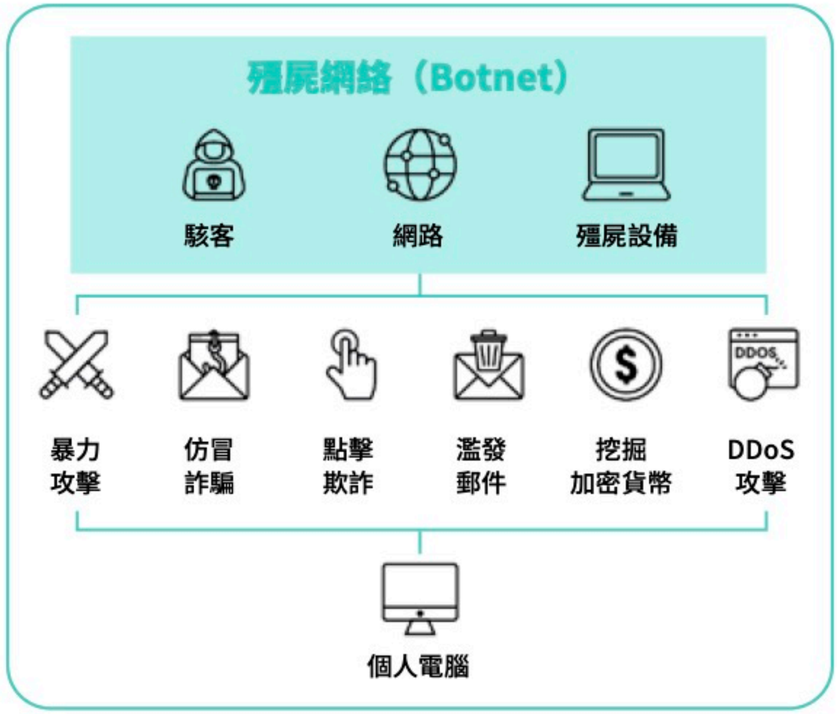
- ☒ 你自己、家人、朋友，甚至寵物的名字
- ☒ 整個或部分帳號使用者名稱
- ☒ 個人資料，包括電話號碼、出生日期、紀念日、車牌號碼等
- ☒ 常見英文詞彙
- ☒ 純數字組合
- ☒ 空白密碼（whitespace）
- ☒ 順序數字（1234）、順連英文字母（abcde）、鍵盤順序組合（qwerty）

2.7 殭屍網絡（Botnet）

殭屍是中國民間傳說的一種復活死屍，它全身僵硬，指甲發黑兼鋒利，牙齒亦銳利。它常躲於黑暗地方，並靠吸食活人或動物血液來維持行動力。要停止它們的行動，其中一個方法是把符咒貼在它們的額頭上，便可令殭屍站著不動。

殭屍網絡一詞，當然跟殭屍亦有一點關係。殭屍網絡（Botnet），是「bot」跟「net」組合而成的。「bot」是「robot」（機械人）的簡稱，加上「net」（網絡）即是「機械人連成的網絡」。在殭屍網絡中，一方是被惡意軟件感染的設備（例如你的電腦、網絡攝影機，甚至家中所有連上互聯網的設備），另一方是負責操控的機構（或自動化機械人）。犯罪分子透過發布惡意軟件來建立殭屍網絡，他們一般都希望把這些受感染的設備組合起來，利用較強之運算能力來發動大規模網絡攻擊。

利用這些被操控設備的資源，犯罪分子可發動具破壞力的攻擊。攻擊可以有多厲害？例如發送以億計的垃圾電郵、通過巨型殭屍網絡伺服器強迫挖掘加密貨幣及癱瘓大型網站等。攻擊力及影響實在令人不容忽視，下列為一些常見的殭屍網絡攻擊：



- **分散式阻斷服務（distributed denial-of-service，簡稱 DDoS）攻擊：**為了使某個互聯網服務超出負荷，攻擊者可利用殭屍網絡中的大量受感染裝置（殭屍裝置）通過向目標伺服器發送指令來發動攻擊，令伺服器超出可負擔水平而倒下來。

- **濫發電郵攻擊：**攻擊者將大量垃圾郵件無差別地發送至大量收件人。為了防止濫發電郵的發送者被列入黑名單，殭屍網絡可持續地改變發送者的電郵地址，好讓這攻勢能維持一段時間。這些電郵內容大多數為一些商業廣告，亦有些為身份偽冒的詐騙攻擊。

- **挖掘加密貨幣：**殭屍網絡中的殭屍裝置可為攻擊者提供電力、電腦運算能力及頻寬，攻擊者便可免費使用殭屍裝置來挖掘加密貨幣（例如比特幣（bitcoin）等之虛擬貨幣，屬於區塊鏈（blockchain）技術上的其中一種應用），從中獲取收入。

- **仿冒詐騙攻擊：**這類攻擊大部分透過電郵來發送詐騙連結。一旦受害者按下了這些連結，將會把受害者帶到一些虛假或惡意網站，並收集個人及其他敏感資料，例如銀行帳戶或信用卡資料等。

- **點擊欺詐：**攻擊者可控制殭屍裝置來進行點擊欺詐，利用殭屍裝置假冒成為正常裝置來瀏覽網頁，並點擊網頁內之連結（例如點擊付費線上廣告）來創造收入。

- **暴力攻擊：**暴力是指通過不斷的嘗試及錯誤中，希望把所有可組成你的密碼的組合試出來，從而強行登入你的帳戶。別使用弱密碼，設定高強度密碼是非常重要的。

如果你的裝置出現以下特徵，裝置有可能已被殭屍網絡感染而成為殭屍裝置：

- ⚠ 網絡連線變慢。
- ⚠ 裝置操作系統或應用程式常常無故終止執行。
- ⚠ 裝置經常出現異常情況，例如電池電量急跌或網絡連線中斷。
- ⚠ 裝置可用記憶體或磁碟空間突然減少。
- ⚠ 在未有使用網頁瀏覽器時突然彈出廣告。
- ⚠ 在不知情的情況下從你的電郵帳戶發送郵件等。

假若你的裝置被殭屍網絡感染成為殭屍裝置，先不用怕，因為應對殭屍網絡相比之前提及的惡意軟件較為簡單。

1. 必須切斷裝置與互聯網之連線，攻擊者便不能操控該裝置。
2. 使用防毒軟件掃瞄整個系統，以確認是否遭殭屍網絡感染。

3.1 大數據時代

根據 IDC（International Data Corporation，國際數據資訊有限公司）在 2018 年 11 月發表的《數據時代 2025》研究報告顯示，全球每年所產生的數據量將從 2018 年的 33ZB 增長至 2025 年的 175ZB，每天約產生 491EB 的數據。

ZB 及 EB 是指多少的數據量？以下列出由小至大的數據單位給大家參考：

1B（Byte，字節）＝ 8b（bit，位）

1KB（Kilobyte，千字節）＝ 1,024B

1MB（Megabyte，兆字節）＝ 1,024KB

1GB（Gigabyte，千兆字節或吉字節）＝ 1,024MB

1TB（Terabyte，萬億字節或太字節）＝ 1,024GB

1PB（Petabyte，千萬億字節或拍字節）＝ 1,024TB

1EB（Exabyte，百億億字節或艾字節）＝ 1,024PB

1ZB（Zettabyte，十萬億億字節或澤字節）＝ 1,024EB

1YB（Yottabyte，一億億億字節或堯字節）＝ 1,024ZB

對 1EB 完全沒有概念嗎？讓我們以影片做例子。一段一分鐘、1080p、30fps 的影片，檔案大小約 1GB。十億段一分鐘影片約等於 0.93EB。換言之，假若在 2025 年全球每天真的產生 491EB 的數據，這比十億段一分鐘影片的檔案大小總和還要多很多。真的很誇張，對吧？

IDC 還預測，在 2025 年，全世界的互聯網使用者每天平均有超過 4,900 次的數據互動，包括刊登一個 Facebook 帖子、上載一段 YouTube 影片、發送一封電郵、在討論區留下一條回應，甚至只是在社交平台的一個「讚好」，這些行為都屬於數據互動之列。如果把這個數字跟 2015 年的調查結果相比，在 2025 年互聯網使用者每天的數據互動將為 2015 年的 8 倍以上，大約每 18 秒便發生一次數據互動。

網上一直流傳一個網絡諺語：「Google knows everything !」（Google 知道所有事情！）在互聯網上尋找資訊，比起到圖書館找參考書方便得多。利用搜尋引擎去尋找日常生活解決方案已經成為我們生活一部分，無論大

事小事，遇到問題都會第一時間到網上逛逛。隨著智能手機及移動網絡越來越普及，我們能隨時隨地在網上尋找資訊，而在同一時間，亦在互聯網產生搜尋數據。

Smart Insight 在 2019 年估計，全球每天有 50 億次網絡搜尋，而其中 35 億次是利用 Google 搜尋引擎，約佔全球的 70%，相當於每秒處理逾 4 萬次搜尋。相比 2000 年，Google 那時一年的總搜尋次數只有 140 億次。如果想了解本日 Google 的全球總搜尋量，可瀏覽以下網頁：

數字上升速度非常快，因為全世界每一刻都有人在使用 Google 搜尋引擎。

Facebook 早前亦向外公布一些統計數字，整個 Facebook 平台每天產生超過 4PB 數據，內裡包含超過 100 億個帖子、3.5 億張照片及 1 億小時的影片。而在 Instagram 平台上發現，全球用戶每天會分享約 1 億張照片及影片。Twitter 亦表示用戶每天共發超過 5 億條訊息。

相信你亦同意我們正身處大數據時代，我們每一刻都在產生各種互聯網數據，而且數據量比你所想還要多。雖然以上分享的都是全球性數字，你或許會認為我們日常生活產生的數據量微不足道，但是如果這些平台及服務供應商從你每日所產生的微小數據中作出分析，繼而向你作出比你自己更了解你的推薦和選擇，你會否對此小事另眼相看？