教育訓練文件——Google Safe Browsing 與釣魚網站

Google Safe Browsing 簡介

Google Safe Browsing 是 Google 開發的一個網路安全服務，旨在保護用戶免受釣魚網站、惡意軟件、社交工程攻擊等網路威脅的侵害。此服務可用於 Google Chrome 和其他支持的瀏覽器中，同時也通過 API 提供給開發者，以便和網站或其他應用整合。這項服務於 2007 年推出，隨後成為網路安全領域的重要防護工具之一。

什麼是釣魚網站？

手法

「網路釣魚」是指透過假冒或偽裝的方式，騙取受害人信任並提供個人資訊，常通過電子郵件與社群媒體等媒介進行。而「釣魚網站」是其中的分類之一，攻擊者通常會製作出以假亂真的網頁介面，以此來假冒真正的網頁服務，進而騙取使用者的個人資訊。

例如有一段時間相當常見的釣魚手法，就是假冒 Facebook 發送安全警告通知給使用者，誘導受害者點進幾乎和真正 Facebook 一模一樣的釣魚網頁介面。而受害者在該介面輸入當前的帳號與密碼意圖進行修改時，其目前正在使用的 Facebook 帳密就會被傳送到攻擊者手中加以利用。

危害

除了上述提及的特定網站帳號密碼之外，根據釣魚網站仿冒的對象，使用者還可能被騙取身份證等證件、甚至是信用卡資訊。攻擊者可以利用這些資訊偽裝成受害者進行非法活動、進一步將連結傳送給受害者好友以擴大範圍、或是直接盜用受害者的可用資金。

此外，若是企業或組織內部有人誤信釣魚網站，可能會導致更嚴重的後果。那些遭受模仿的原始網站（如上述提到的 Facebook）也有機率因此而蒙受聲譽上的損失。

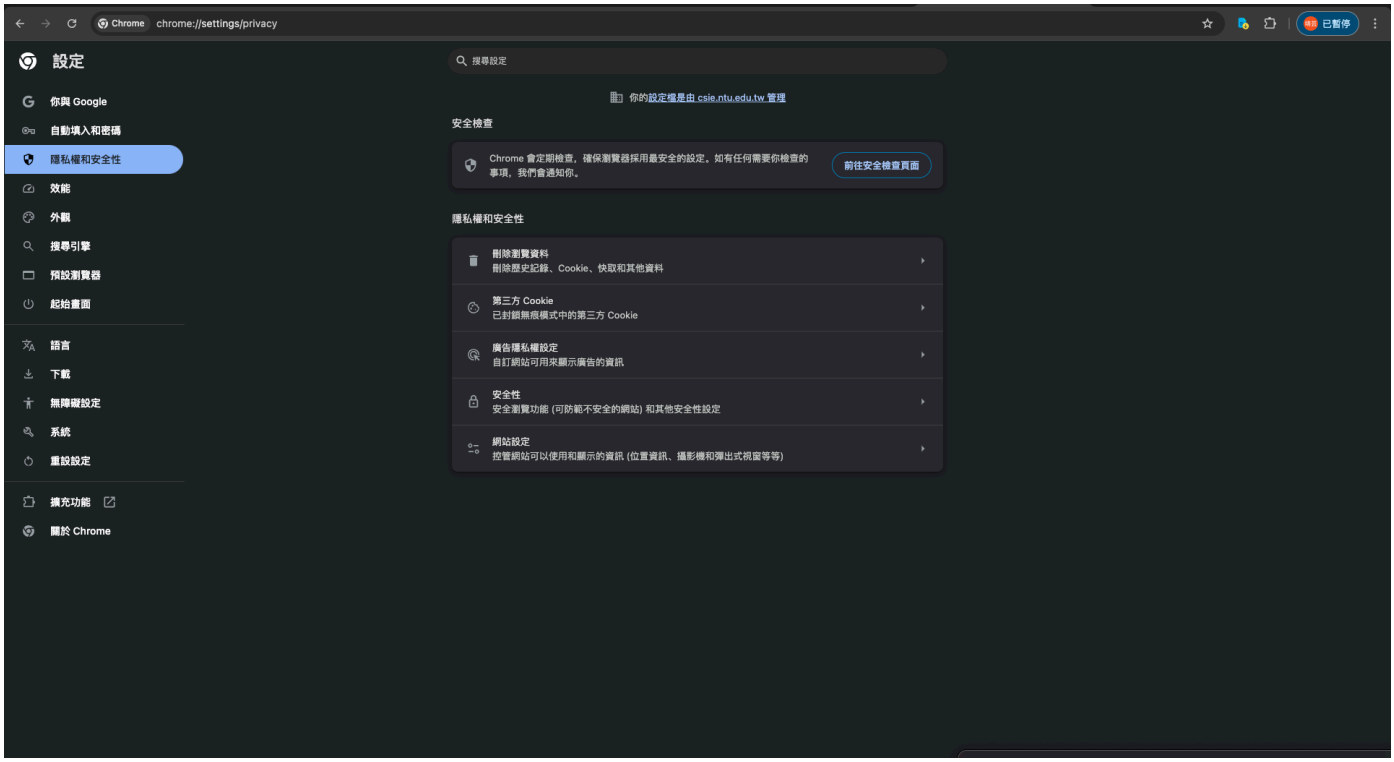
Google Safe Browsing 如何辨識釣魚網站？

此服務除了將目標網址和現有的所有釣魚網站網址做對照之外，對於沒有在資料庫裡的網站， google safe browsing 也會透過爬蟲獲知網頁資訊，並結合機器學習模型來判別是否為釣魚網頁。

Google Safe Browsing 使用說明

Chrome 瀏覽器設定

進入 Chrome 瀏覽器設定 > 隱私權和安全性 > 安全性



選擇強化防護：

此設定會對進入的網站進行一定程度的分析，以判斷是否為釣魚網站或包含惡意下載內容。

若是選擇一般防護，則只會確認當前的網站是否有在已知的釣魚網站列表內，並適時發出警告，而不會一一確認當前使用的網頁服務。

回報

由於架設釣魚網站的成本低廉，在新的網站源源不絕出現的前提下， google safe browsing 可能無法涵蓋所有最新的網址。此外，使用爬蟲及機器學習協助進行釣魚網站的標記也可能會有判斷上的謬誤。因此 google 也提供了回報新網站及標記謬誤的頁面，讓使用者也可以一同協助完善資料庫。

回報未包含於當前 data 中的釣魚網站：https://safebrowsing.google.com/safebrowsing/report_general/

回報誤認的釣魚網站：https://safebrowsing.google.com/safebrowsing/report_error/?hl=en

API

上述為沒有 IT 背景的使用者也可以簡單加強安全方護的方式。

若是具有相關背景，並且希望將其他服務和 google safe browsing 進行整合，則可以利用 google 提供的免費 API：

https://developers.google.com/safe-browsing/reference?hl=zh-tw

API 不僅提供網址的比對，也有即時對網頁進行檢測的方式，可以根據需求自由使用。