Google 釣魚詐騙事件頻傳，用戶該如何防範？

原文：
https://www.btcc.com/zh-TW/academy/research-analysis/google-phishing-scam

最近 Google 釣魚事件頻傳，不少受害者因為誤點了 Google 搜尋廣告或 Gmail 郵件，進而進入惡意網站，並不慎簽署惡意簽名，最終導致錢包資產丟失。Web3 反詐騙平台 Scam Sniffer 報告顯示，目前已經有超過 3 千人遭遇 Google 搜尋廣告釣魚，損失資產超 400 萬美元。

那麼，我們應該如何避開這些釣魚詐騙呢？最近頻發的 Google 釣魚詐騙事件有哪些呢？

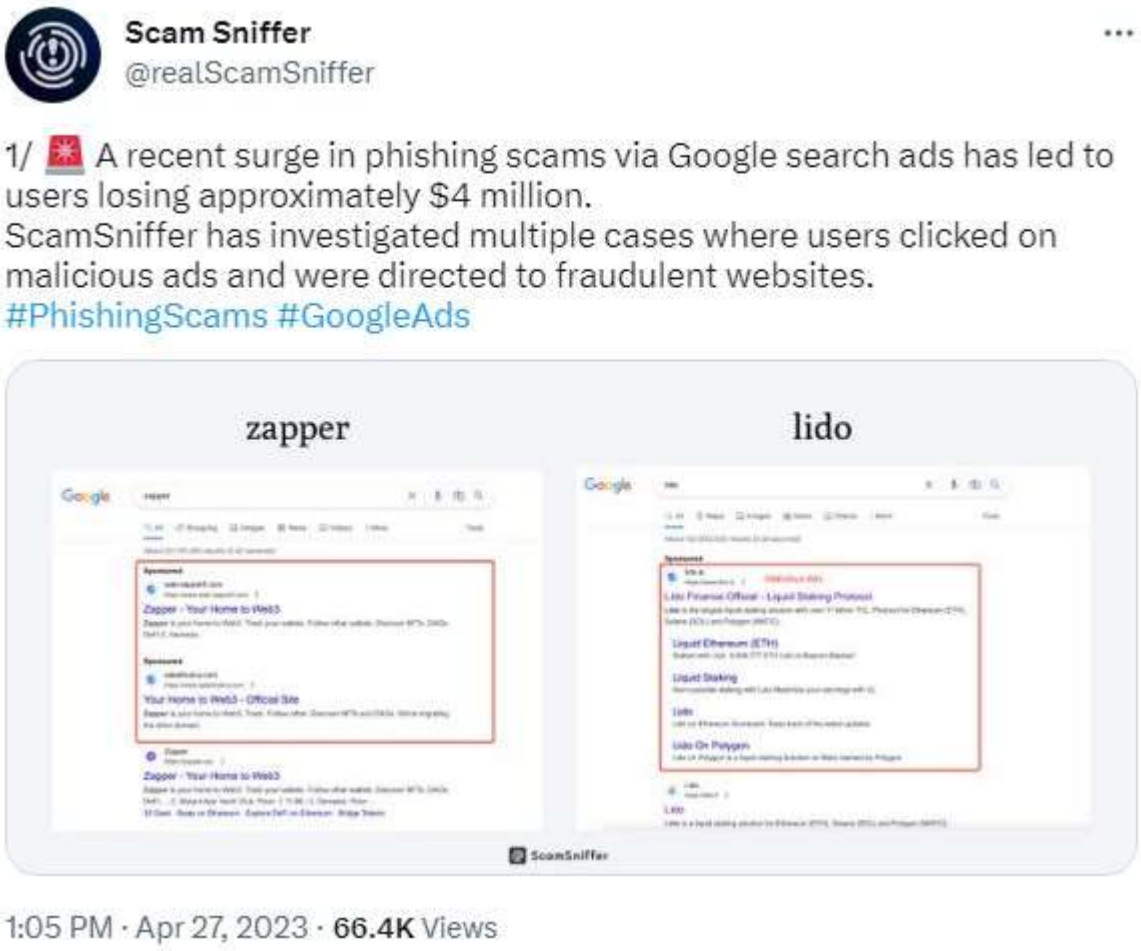
網路釣魚詐騙是什麼？

網路釣魚是是一種欺詐形式，一種網路犯罪。

攻擊者會偽裝成信譽良好的實體或個人通過電子郵件或其他通信渠道，使用網路釣魚電子郵件分發可執行各種功能的惡意鏈接或附件，從受害者中提取登錄憑據或帳戶信息；或者自動下載惡意軟件，讓受害者使用惡意軟件感染自己的計算機。

Google 搜尋廣告釣魚

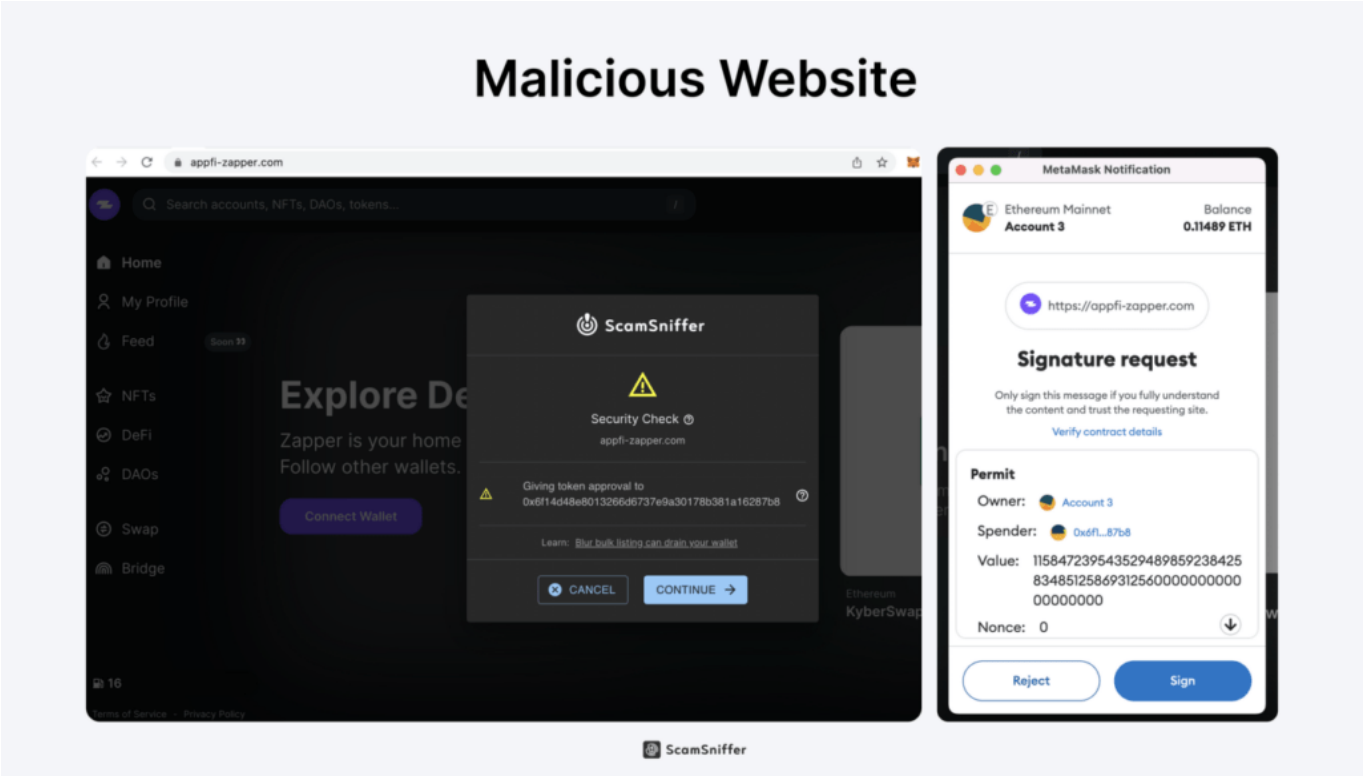
Web3 反詐騙平台 Scam Sniffer 發布的研究報告顯示，最近透過 Google 搜索引擎下廣告進行網路釣魚詐騙的活動大增，Zapper、Lido、Stargate、Defillama 等項目都成為詐騙目標。



1、Google 廣告釣魚的手法分析

Scam Sniffer 指出，惡意份子會鎖定 Zapper、Lido、Stargate、Defillama 等關鍵字，並向 Google 下廣告，使其惡意網站或廣告的搜尋結果能夠被排在搜尋結果的首位，誘騙不知情的用戶點擊並引導入惡意網站。

進入惡意網站後，一但用戶在過程中會跳出簽署授權花費代幣的交易，普通用戶很可能以為是普通的登陸簽名順手就簽了，最終結果就是資產在簽名之後就被立即轉走，一掃而空。



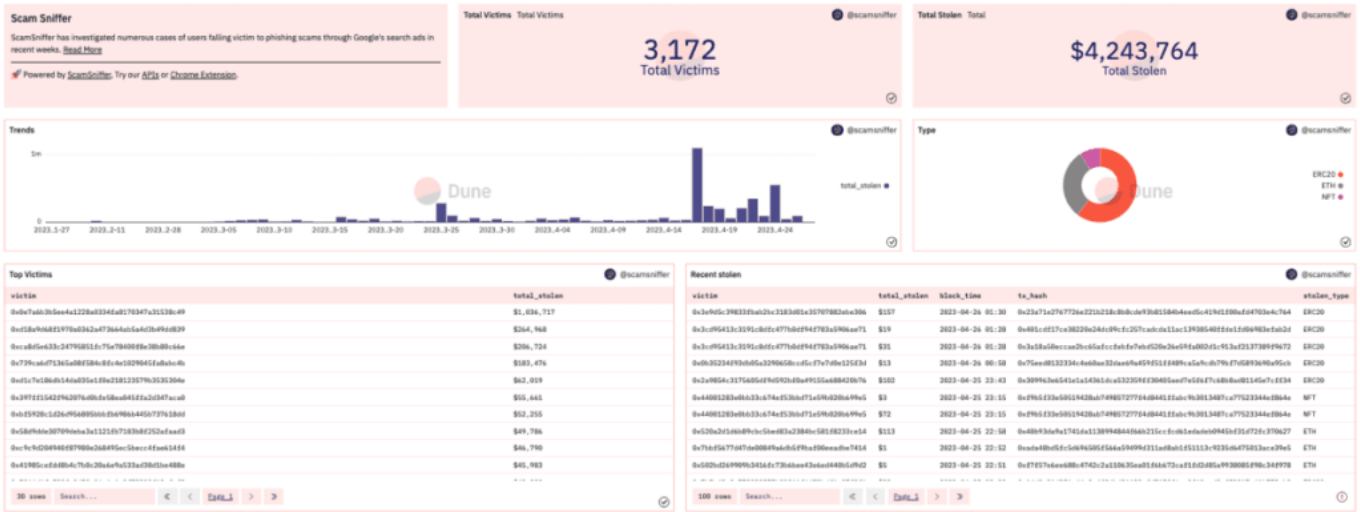
通過分析這些惡意廣告資訊，Scam Sniffer 發現，這些惡意廣告來自於以下廣告主的投放：

- 來自烏克蘭的 ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «РОМУС-ПОЛІГРАФ»
- 來自加拿大的 TRACY ANN MCLEISH

Scam Sniffer 指出，大部分的釣魚廣告的投放成本極低，之所以人們會看到這些惡意廣告，並不是 Google 不審查廣告內容，而是這些惡意的詐騙份子會採用「參數區分」或「防止調試」等方式繞過 Google 的審查流程，進而對使用者造成嚴重的傷害。

2、Google 搜尋惡意廣告受害者已達 3 千多人

據 Dune 數據顯示，目前這些 Google 惡意廣告網站已導致約 4,200 萬美金資產被盜， 3,172 人受害，且攻擊主要發生在近一個月左右。在所有受害者中，金額最大的是開頭 0x0e7 的地址，個人受害金額就超過 100 萬美金。



3、如何防範 Google 搜尋廣告釣魚？

面對這樣的釣魚活動，用戶務必在每次打開網站時再三確認網址是否有異狀，甚至直接忽視搜尋結果中廣

告區域的內容，最好的做法則是將常用的網站直接存入瀏覽器書籤，避免用搜尋的方式進入。另一方面，簽署交易時也必須了解簽署的內容與當前的操作是否吻合，以免在無意間將代幣授權給他人而毫不自知。

工具方面，用戶可以下載 Scam Sniffer 或 Defillama 開發的瀏覽器插件，能夠在誤入釣魚網站或跳出簽署高風險交易的請求時發出警示。

Scam Sniffer 也建議，使用者在使用 Google 搜尋的時候，應該多加留意，同時希望 Google 廣告能加強對 Web3 惡意廣告的審查，來保護使用者。

虛假 Google 郵件

除了 Google 惡意廣告釣魚外，近期也有用戶在Gmail信箱當中，收到來自Google的郵件，請小心這封看似是官方寄來的郵件，極有可能是詐騙的手法，一不小心將失去自己的帳戶及錢財。

1、Google 郵件釣魚手法

據外媒《每日鏡報》報導，Google遭到釣魚詐騙簡訊的冒名利用，以「在線獎勵計畫」為主題的信件，寄到用戶的Gmail信箱裡，並詐騙內容寫到「您剛剛在Google上進行了第182.5億次搜尋，全球每達1千萬次搜尋，我們就會挑選一名幸運用戶送出感謝禮，而你就是那位幸運兒！」，若當其受騙，點擊以後會遭到駭客竊取個資，甚至會竊取個人帳戶的錢財。

此外，國外資安廠商Avanan 發布的最新報告也指出，旗下研究人員發現一項以假冒Google文檔分享連結的網路釣魚攻擊活動，一旦點擊信件內附的網址連結後，會先連結到偽裝成官方的文檔分享網頁，並要求用戶需輸入帳號密碼，完成登入後，即可下載該份文檔檔案，以用於離線觀看。

然而，實際上，連結的惡意釣魚網頁卻暗藏有可竊取用戶帳號密碼的程式碼，利用偽裝的登入頁面要求用戶輸入帳號密碼，只要用戶按下「登入」按鈕後，駭客就能從遠端存取用戶的Google帳密資料。

2、如何防範虛假 Google 郵件？

Avanan 指出，這類新型惡意網路釣魚攻擊活動，主要是利用Google文檔分享檔案所生成的網址連結，可繞過電子郵件用於掃描檢測網址安全防護的機制漏洞。提醒用戶，在收到附有Google文檔分享的網址連結時，若發現該連結導向需登入帳號密碼的頁面時，務必要格外謹慎，以免陷入惡意釣魚陷阱，導致個人帳密遭竊的資安危機。

此外，收到附有Google文檔的網址連結時，若要判別是否為惡意釣魚郵件，可掌握兩個原則，其一，就是透過Email發送含有Google文檔檔案的分享連結信件時，並不會要求用戶在查看之前需先下載文檔。其二，若不確定電子郵件的寄信人來源時，建議不要點擊郵件內附的網址連結、也不要下載檔案，以免裝置遭惡意軟體入侵感染。另，若不慎點擊假冒為Google文檔的網址連結時，務必盡快更新Google帳號密碼。

Google官方也注意到近期詐騙釣魚訊息的嚴重性，呼籲用戶，注意在手機或電腦網頁上遇到彈跳式廣告，內容聲稱贏得Google一份禮物，並要求回答問題個人資料或電子信箱等，以領取禮物，皆屬於詐騙，Google官方強調並不會提供這類形式的獎勵。

Google也表示，詐騙集團為了騙取用戶的信任，通常會製造「要在幾分鐘內回覆」的急迫性，且為了研究需要用戶，會要求填寫更詳細的個資，因此用戶要提高警覺、切勿流出重要個人資訊。

如何防範 Goolge 網路釣魚？

雖然駭客不斷提出新技術，但我們可以採取一些措施來保護自己：

1、使用垃圾郵件過濾器

可以使用垃圾郵件過濾器。來防止垃圾郵件的出現。通常，過濾器會評估郵件的來源，用於發送郵件的軟件以及郵件的外觀，以確定郵件是否為垃圾郵件。有時，垃圾郵件過濾器甚至可能阻止來自合法來源的電子郵件，因此它並不總是100％準確。

2、更改瀏覽器設定

瀏覽器建議設定為只允許可靠的網站打開。瀏覽器會保留一個虛假網站列表，當您嘗試訪問該網站時，該地址將被阻止或顯示警告消息。

3、安裝防網路釣魚工具欄

您可以使用反網路釣魚工具欄自定義最流行的Internet瀏覽器。此類工具欄會對我們訪問的站點進行快速檢查，並將其與已知網路釣魚站點列表進行比較。

4、定期檢查帳戶

養成定期更改密碼的習慣，不要對多個帳戶使用相同的密碼。

5、檢查郵件連結

在單擊或輸入敏感信息之前，需要檢查電子郵件鏈接中URL的拼寫，保證安全；永遠不要從可疑電子郵件或網站下載文檔。

6、驗證站點安全

在提交任何資訊之前，請確保網站的URL以“https”開頭，並且地址欄附近應該有一個關閉的鎖定圖標。檢查網站的安全證書。

7、使用防病毒軟件

防病毒軟件附帶的特殊簽名可防範已知技術的變通方法和漏洞。

8、使用防火牆

高質量的防火牆充當計算機和外部入侵者之間的緩衝區。我們應該使用兩種不同的類型：桌面防火牆和網路防火牆。第一種選擇是一種軟體，第二種選擇是一種硬體。當它們一起使用時，它們可以大大降低駭客和網路釣魚者滲透您的計算機或網路的機率。

9、不要洩露個資

作為一般規則，絕不應通過互聯網分享個人或財務敏感信息。

10、了解網路釣魚的知識

新的網路釣魚詐騙正在不斷發展。如果不掌握這些新的網路釣魚技術，我們可能會無意中陷入其中。

如何在加密釣魚詐騙中保護自己的資產安全？

隨著加密貨幣行業的發展，詐欺集團也開始以虛擬貨幣為號召，吸引投資人加入。而由於目前很多投資者對加密貨幣/虛擬貨幣行業不太熟悉，不少被害人在投入大筆資金後才有可能發現自己遭騙。

此外，為了讓投資者放鬆警惕，詐騙團夥使用的方式更是層出不窮，不少民眾防不勝防，成為了其中的受害者。

想要避開詐騙，就**需要提高自己對虛擬貨幣的認識，掌握有關虛擬貨幣詐騙的相關知識**，同時，不要輕易相信任何可以短期獲取暴利的謊言，就是守住荷包的最好方法。

虛擬貨幣最全介紹，加密貨幣是什麼？種類有哪些？交易所、風險一次看

6種常見數字貨幣詐騙 新手應該如何防範？

加密投資者是真的嗎？一文教你避開90%的虛擬貨幣詐騙！

NFT防盜指南丨如何保護自己的NFT資產安全？

加密安全丨預防加密貨幣所被駭指南

Pi 幣是詐騙嗎？該項目存在什麼風險？

派網（Pionex）安全嗎？是詐騙嗎？PTT網友如何說？

新網路釣魚詐騙！錢包出現異常USDT交易記錄怎麼辦？一招教你識別它！

新詐騙手法！傳送「Telegram截圖」帳戶被偷走？如何提高自己的帳戶安全性？

更多相關加密詐騙新聞：

台灣加密詐騙丨女外送員誤信虛擬貨幣詐騙群組，遭詐85萬，恐再跑1萬單

實體店「假投資真詐騙」，以投資虛擬幣USDT泰達幣違法吸金2億元

泰達幣詐騙案丨9人狂刷BUG爽撈2500萬ETH、USDT！刑事判決已出爐

警惕！詐騙集團騙取民眾信用卡盜刷購買 USDT

涉及多宗虛擬貨幣詐騙的MBI創辦人落網，將移交中國受審

「TeddyDoge」拉地毯騙局（Rug Pull），捲款超 425 萬美元

T-SET事件詳解，我們應該如何避開加密貨幣騙局

高鐵左營站驚傳虛擬貨幣搶案 2匪得手「900萬泰達幣」後逃逸

想了解更多有關區塊鏈和金融的資訊，可以進入 BTCC **學院** 及 **資訊** 頁面進行查看。

?BTCC 註冊優惠活動

註冊後即可獲得 10 USDT 贈金，再加入官方 LINE 參加活動可獲得額外 10 USDT 贈金。新用戶註冊後 7 天內入金，贈金最高 10,055 USDT！趕快開始註冊吧！

更多優惠內容：關注 BTCC 活動中心

註冊 BTCC 贏10,055U豐厚贈金（入金活動）

關於 BTCC

- 安全性高，已獲得美國、歐洲、加拿大等地監管牌照
- 無資金費率
- 1到150倍靈活槓桿
- 交易費低至 0.03%
- 行業領先的市場流動性，交易深度大
- 提供通證化代幣（貴金屬、美股、台股）
- 24 小時線上真人客服
- 每月提供大量福利活動

立即註冊 BTCC 帳戶