

BTCC “**新手專享**”

註冊並入金 BTCC，領取最高價值**17,500USDT**獎勵。
推薦好友還有更多返佣獎勵。

立即註冊/查看詳情

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！

原文：

<https://www.btcc.com/zh-TW/academy/research-analysis/defi-phishing-scam>

近期加密詐騙案件頻傳，其中「網路釣魚」的手法更是層出不窮。imToken 安全團隊發現，有些用戶的錢包地址會突然出現非本人操作的 **USDT** 操作記錄，這其實很可能是騙子通過釣魚合約偽造的，一旦用戶誤以為帳號被盜，就很可能走進騙局中。

那麼，我們應該如何避開這種新型的 DeFi 釣魚詐騙呢？



網路釣魚是什麼？

我們經常會在新聞中看到「網路釣魚」詐騙，那麼，到底這種詐騙是什麼？其特征有哪些呢？

網路釣魚(phishing)是一種用於獲取有價值的用戶數據的技術，攻擊者可以將這些數據出售或濫用，用於惡意目的，例如敲詐勒索、金錢盜竊或身份盜竊。

進行「網路釣魚」的匪徒會發出一封電郵 / 短訊，誘使對方提供自己的密碼和銀行資料，或者點擊會把惡意軟件植入受害人裝置的內嵌連結、QR碼或檔案附件。此類電郵 / 短訊一般訛稱由銀行、網上付款服務商或網上零售商等合法機構發出，看來亦往往與這些公司發出的真正電郵 / 短訊相似，內含連結或QR碼所通往的網站更與有關機構的真實網站極度相似。

一旦接達仿冒網站，受害人通常會被提示輸入個人保安資料，如戶口號碼、PIN碼、保安編碼或一次性密碼。「網路釣魚」網站會記錄所輸入的一切資料，繼而藉此盜取金錢。

針對DeFi的網路釣魚

近年來，[去中心化金融\(DeFi\)](#)在全球市場中崛起，大量優秀的DeFi應用/產品不斷地被提出，這些應用/產品不受到集中化金融體系的限制，在分散式的區塊鏈上有著更加開放與透明的優點。

雖然這些DeFi應用/產品本質具備去中心化的優點，但是它們仍然需要中心化的入口(例如：官方網站)來介紹服務和導引用戶投資，因此嗅覺敏銳的黑帽駭客們也從中找到了全新的機會。



[下載Android版](#)

[下載iOS版](#)

[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

如何應對新型 Defi 釣魚騙局？

近期，有不少網友發現，自己的 [ETH](#) 錢包地址中，莫名其妙出現了一項非本人操作的 USDT 操作記錄，懷疑自己的帳號是否被盜了。但其實，這很可能是一個釣魚連結。

因此，當你看到ETH 錢包中出現未經你本人許可的USDT 操作記錄時，請先檢查該項記錄中的USDT 是否是真實的。

你可以通過合約地址，來辨別在imToken 應用程序的ETH 錢包中出現的USDT 操作記錄是否是真實的。

- 通常，在真實的操作中，USDT 在ETH 網絡的合約地址

為：0xdAC17F958D2ee523a2206206994597C13D831ec7

當你看到異常操作記錄時，可以進入ETH 錢包的歷史記錄頁面查看合約地址，如果相關合約地址不是前文羅列的地址，你就能確定該項名稱為USDT 的操作為假。

如何辨別 DeFi「網路釣魚」？

在這種新型的DeFi「網路釣魚」中，騙子是如何透過「假USDT 操作」來騙取用戶資產的呢？

首先，**騙子通過在區塊鏈上創造假的USDT 交易記錄**，使其能在Etherscan 和錢包歷史記錄中顯示，這會導致用戶的錢包中出現非本人操作的假的USDT 操作記錄。

然後，用戶的地址被用作發起地址，**用戶可能會誤認為自己的數字資產被轉走了**。偽造的交易記錄來自騙子自己創造的釣魚合約，因此騙子可以隨意偽造合約的交易發起地址與轉出地址。如果用戶沒有點擊進入錢包應用程序的歷史記錄頁面中認真辨別合約地址，就有可能會覺得自己的錢包被盜了。

通常，騙子設定的轉出地址和用戶之前使用過的真實轉出地址，首尾幾個字符通常會是一樣的，其目的是為了誘導用戶在後續的操作中，複製使用錯誤的轉出地址。

如果用戶沒有認真識別地址（比如，僅僅核對首尾幾個字符是否相同），**就可能中了騙子的圈套**，讓騙子竊得你的數字資產。

那麼，在日常生活中，我們應該如何辨別哪些是釣魚連結呢？

imToken 安全團隊給出了這些「假USDT 操作記錄」的特點，透過以下寫著特點，相信你可以很快辨別出哪些是詐騙，哪些不是。

當你發現你的ETH 錢包歷史記錄中，確實出現了一項「假USDT 操作」時，請不要恐慌，**這並不會影響你的資產安全**。這些操作記錄都是騙子通過釣魚合約偽造的。

透過查詢鏈上數據，我們可以發現這些偽造的交易有以下3 個共同點：

- 偽造的交易都發生在一個陌生的，帶有USDT 名稱的操作中。
- 偽造交易的數額為用戶近期操作過的大額交易的數額。
- 轉出帳戶地址的首尾字符與用戶之前使用過的真實轉出地址相似，容易混淆。

A promotional banner for BTCC. The background is green with a subtle pattern of Bitcoin symbols. At the top center is the BTCC logo. Below it, the text reads "VIP等級只升不降！等級越高福利越多" in large, bold, yellow and white characters. Underneath that, it says "讓BTCC成為您的首選加密貨幣合約交易所". At the bottom, there are two download buttons: "現在下載了解更多" with an Apple App Store logo, and "Google Play 立即下載" with a Google Play logo. To the right of the Google Play button, it says "支援臺幣&幣幣入金". There are also some gold coins and a blue coin icon scattered around the text.

[下載Android版](#)

[下載iOS版](#)

[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

加密詐騙方式層出不窮，提高警覺以防資產損失

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](#)

[5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 | 如何保護自己的NFT資產安全？](#)

[加密安全 | 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？](#)

更多相關加密詐騙新聞：

[台灣加密詐騙 | 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 | 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](#)

想學習更多有關區塊鏈和金融的資訊，可以進入 [BTCC 學院](#) 及 [資訊](#) 頁面進行了解。

?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。新用戶註冊儲值&交易限定福利正在舉行，贈金最高 10,055 USDT! 註冊後在活動中心參與。趕快開始註冊吧!

更多優惠內容：[關注 BTCC 活動中心](#)

註冊 BTCC 贏3500U 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