2024 年應避免的 8 種加密詐騙類型

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/8-types-of-crypto-scams-to-avoid-in-2024-2

您是否成為加密貨幣騙局的受害者？ 如果是這樣，那麼您並不孤單——加密貨幣用戶在 2023 年因詐騙、詐騙和駭客攻擊損失了近 20 億美元，2024 年上半年損失超過 14 億美元。

保護自己的一個關鍵步驟是全面了解現有的各種類型的加密貨幣詐騙。 這些範圍從網路釣魚嘗試到精心設計的龐氏騙局，詐騙者不斷設計新策略來利用毫無戒心的個人。 透過保持警惕和充分了解情況，您可以顯著降低風險。
我們的綜合指南概述了八種常見的加密貨幣投資詐騙類型。 讓我們深入研究一下細節。

- 冒充與贈品詐騙
- 加密貨幣投資詐騙
- 勒索和勒索計劃
- 雲挖礦方案
- 假加密貨幣交易所和錢包
- SIM 交換詐騙

什麼是加密詐騙？

從本質上講，加密貨幣詐騙是一種利用加密貨幣從個人非法獲取金錢、個人資料或數位資產的非法嘗試。　加密貨幣的去中心化和通常是假名的性質助長了此類詐欺活動，使得追蹤和追回被盜資金變得困難。　不幸的是，一旦在加密騙局中損失了錢，找回它通常是一項艱鉅且不太可能的任務。
詐騙的多樣性和複雜性可能會令人困惑，因此很難從詐騙中辨別出真正的機會。　詐騙者採用的常見策略是向投資者承諾不切實際的回報，風險極低甚至沒有風險，以巨額經濟收益的前景來吸引個人。　這些騙局一視同仁，不僅針對新手，也針對經驗豐富的投資人甚至大公司。

八種最常見的加密貨幣詐騙是什麼？

正如我們上面提到的，加密貨幣用戶在2023 年因詐騙、詐騙和黑客行為損失了近20 億美元，2024 年上半年損失超過14 億美元。看看它們是如何運作的，以及如何防止成為它們的受害者。

網路釣魚詐騙

網路釣魚詐騙是詐騙者採用的一種欺騙策略，他們會創建虛假網站、社交媒體資料或發送虛假電子郵件來誘騙您洩露個人信息，包括您的身份、密碼和加密貨幣錢包密鑰。 這些騙局狡猾地模仿合法的加密貨幣平台，例如交易所，以向毫無戒心的受害者灌輸信任。 您收到的電子郵件或訊息可能看起來可信，通常包含誘人的報價或對您的敏感資訊（例如您的私鑰或登入憑證）的緊急請求。

一旦您無意中向詐騙者透露了這些信息，他們就可以利用它來竊取您的數位資產。 這可能涉及使用您提供的詳細資訊在正版平台上存取和清空您的加密貨幣帳戶。 因此，警惕任何主動要求您提供個人或財務資訊的通訊至關重要，尤其是當它承諾好得令人難以置信的交易或造成緊迫感時。

浪漫詐騙

另一個需要警惕的危險騙局涉及情緒操縱，特別是加密浪漫騙局的形式。 在這些騙局中，詐騙者會在約會網站或流行的社交媒體平台上建立虛構的個人資料，以透過精心設計的、通常是漫長的關係來獲得您的信任。 在幾週甚至幾個月的時間裡，他們會與你建立聯繫，利用情感連結來發揮自己的優勢。

一旦詐騙者贏得了您的信任，他們就會介紹投資加密貨幣計劃的想法或要求直接進行加密貨幣轉帳。然而，這些資金並沒有用於承諾的投資，而是立即被轉移到他們自己的口袋裡。 這些騙局造成的經濟損失可能是驚人的，達到天文數字。 據 AARP 稱，2023 年 11 月，美國司法部和特勤局從針對 70 多名受害者的詐騙者手中追回了價值 900 萬美元的 Tether。 其中很大一部分是透過浪漫計劃而成為目標的。

冒充與贈品詐騙

詐騙者越來越多地採用欺騙手段，冒充名人、有影響力的人和信譽良好的公司，以推銷虛假的投資機會和虛假的贈品。 以下是這些騙局如何展開的詳細分析：
假名人代言：詐騙者創造虛假的社群媒體資料或滲透真實的、經過驗證的帳號。 他們利用這些平台宣傳欺詐性加密貨幣計劃，承諾豐厚的贈品或保證高回報的投資前景。 受害者被誘騙將加密貨幣發送到指定地址，以未來收到巨額回報為幌子。
社群媒體詐騙 ：詐騙者在 Facebook 和 Instagram 等平台上建立虛假的個人資料、頁面或群組。 然後，他們將利用這些頁面來宣傳詐騙投資計畫或網路釣魚連結——到 2024 年，虛假社群媒體詐騙（有時稱為 Deepfakes）的金額已超過 250 億美元。 詐騙者透過發布虛假推薦、成功故事和巨額利潤截圖來引誘受害者，從而達到這一目的。 這些貼文上的連結將引導用戶造訪擷取登入憑證或私鑰的網站。

加密貨幣投資詐騙

騙子有時會設計誘人的加密貨幣投資計劃，承諾高回報，幾乎沒有風險。 他們通常會採用複雜的方式來讓您相信他們的投資是安全且有利可圖的。 最常見的類型包括龐氏騙局、拉高拋售計劃以及欺詐性 ICO 和 NFT。

它們的工作原理如下：

龐氏騙局
龐氏騙局利用新投資者的資金來償還早期投資者，從而助長了投資機會蓬勃發展的誤解。 這項策略吸引了更多投資者的湧入，但隨著新投資者數量的減少，該計劃不可避免地會崩潰，導致大多數參與者遭受重大損失。 儘管這些計劃至今仍然存在，但它們在 2017/2018 年加密貨幣繁榮期間激增，主要表現為高收益投資計劃 (HYIP)。
拉高和轉儲方案
拉高拋售計畫涉及詐騙者透過欺騙性索賠人為抬高加密貨幣的價格。 他們累積了大量低價、小批量的加密貨幣，隨後透過社群媒體和其他行銷管道開展積極的促銷活動。 這種策略吸引了毫無戒心的投資者，進一步提升了加密貨幣的價值。 在價格飆升的頂峰，騙子會清算其持有的資產，引發價格急劇下跌，並給其他投資者留下貶值或一文不值的資產。
ICO 和 NFT 詐騙
首次代幣發行 (ICO) 和不可替代代幣 (NFT) 是專案的合法募款管道。 然而，詐騙者經常利用這些機制為虛假的活動籌集資金，例如承諾的革命性技術或獨家數位資產。 他們用虛假的宣傳資料吸引投資者，但一旦累積了足夠的資金，他們就突然消失，給投資者留下空洞的承諾和經濟損失。

勒索和勒索計劃

這些騙局的作案手法與傳統的貨幣詐騙相似，儘管以加密貨幣作為交換媒介。 加密貨幣詐騙者採用勒索或勒索策略，利用他們擁有的個人照片、影片或財務記錄等敏感資訊來強迫受害者進行加密貨幣付款。 由於擔心這些敏感資料被揭露會產生後果，受害者通常會以迫在眉睫的最後期限為威脅而默許。 因此，詐騙者成功地從受恐嚇的受害者那裡提取了加密貨幣付款。

雲挖礦方案

這些騙局的受害者成為冒充加密貨幣挖礦承包商的假冒公司所採用的欺騙策略的受害者。 這些合約承諾從加密貨幣挖礦中獲得利潤，而無需擁有昂貴的設備。 然而，事實是，這些公司只是由騙子設立的幌子，他們既沒有採礦設備，也沒有財務手段來兌現對投資者承諾的回報。 在某些情況下，這些挖礦騙局最初是龐氏騙局，即使用新投資者的資金向初始投資者支付費用，從而進一步延續了詐騙循環。

假加密貨幣交易所和錢包

為了竊取資金，詐騙者設計了模仿合法平台的假加密貨幣交易所和錢包，使毫無戒心的人幾乎無法區分它們。 這些假冒網站以誘人的優惠來吸引受害者，包括降低費用、增強安全性和專有功能。 然而，一旦受害者創建帳戶並存入資金，詐騙者就會迅速攜款潛逃，讓受害者空手而歸。

今年 5 月，英國兩名男子從受害者那裡竊取了價值近 600 萬英鎊的加密貨幣。 他們複製了 Blockchain.com 的網站，以便存取受害者的線上錢包。

SIM 交換詐騙

這些加密貨幣詐欺策略異常複雜，利用受害者的手機號碼作為其線上帳戶（包括加密錢包）的網關。 詐騙者利用這些資訊攔截驗證碼，甚至重置密碼，從而直接存取數位資產。 他們可以透過各種方式取得手機號碼，例如社群媒體資料、資料外洩或網路釣魚電子郵件。

詐騙者通常可以透過社群媒體、資料外洩或網路釣魚電子郵件得知您的手機號碼。 有了這些訊息，詐騙者就可以聯繫您的行動供應商並要求 SIM 卡交換，這樣他們就可以讀取您的訊息並繞過您在加密貨幣交易所或錢包上設定的任何雙重認證。