[PDF Database Document] - BTCC Cryptocurrency Exchange

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/telegram-honeypot-explained-tips-for-spotting-scammers

Telegram HoneyPot是什麼？如何避開蜜罐詐騙？

隨著透過 Telegram 變得更容易存取 Web3 世界，安全問題也隨之升級。 騙子信任廣大的社區，利用他們的蜜罐技巧滲透進來。 但是，不要成為受害者！ 了解如何發現並防範這些騙局。

蜜罐計畫透過承諾以最少的投資獲得高回報來吸引毫無戒心的投資者。 這些騙子創造虛假的投資機會，通常偽裝成合法的加密貨幣項目，並誘騙用戶發送資金。 一旦收到資金，詐騙者就會消失，讓投資者空手而歸。

- 蜜罐定義

蜜罐定義

攻擊者精心設計項目，以巨大的經濟收益為誘餌來吸引受害者。 一旦獲得信任，這些騙子就會帶著資金消失，讓投資人陷入困境。 關鍵在於該專案機制的簡單性，這通常會吸引新手用戶。 然而，經驗豐富的投資者在投入資金之前會仔細審查基本面並進行徹底的分析。

揭露隱藏的蜜罐詐騙

詐騙者巧妙地偽裝這些有缺陷的智能合約和 dApp，使其顯得真實，並承諾高利潤來吸引用戶。 然而，真正的目的在於利用這些弱點在不被發現的情況下耗盡用戶的資金。 這些漏洞充當詐騙者的後門出口，使他們能夠竊取加密貨幣而不受懲罰。

此外，詐騙者也建立模仿合法交易所和基金的虛假投資平台。 這些平台可以合法運作一段時間，以真實的服務和回報吸引投資者。 透過培養信任感，攻擊者為毀滅性的退出騙局奠定了基礎，捲走投資者辛苦賺來的資金。

那麼，這些蜜罐計畫到底藏在哪裡呢？ 他們可以滲透到加密生態系統的任何角落，從去中心化金融（defi）平台到遊戲 dApp，甚至主流投資交易所。 對於投資者來說，在將資金委託給任何平台之前保持警惕並進行徹底的盡職調查至關重要。

加密貨幣空投已成為區塊鏈和數位資產領域的主要內容，為新項目吸引用戶和建立勢頭提供了獨特的機會。然而，在免費代幣的興奮和承諾中，詐騙者設計了複雜的蜜罐計劃，潛伏在暗處，準備利用毫無戒心的投資者。

空投的吸引力在於它們能夠提供經濟激勵，向用戶承諾分享項目代幣以換取他們的參與。 不幸的是，同樣的原則已被詐騙者利用，他們使用蜜罐計劃來引誘受害者向虛假項目發送資金。 這些計劃依賴欺騙和誤導，因此投資者在參與空投活動時必須保持謹慎和盡職調查。

詐騙者最常見的策略之一是創建虛假項目代幣並向毫無戒心的用戶宣布空投。 這些詐騙者利用人們對新代幣發布的預期，利用炒作來吸引用戶連接錢包並發送資金。 一旦收到資金，詐騙者就會消失，讓受害者空手而歸。 為了避免成為此類騙局的受害者，用戶必須保持警惕，透過關注該項目的官方社交媒體管道並仔細檢查所提供的任何連結地址，仔細驗證空投事件的真實性。

此外，網路釣魚攻擊是加密貨幣領域蜜罐計畫的另一個常見組成部分。 詐騙者創建模仿合法交易所和平台外觀的虛假網站，使用電子郵件通訊或其他通訊管道鼓勵用戶點擊惡意連結並連接他們的錢包。 透過這樣做，攻擊者可以存取用戶的錢包並竊取他們的資金。 投資者必須警惕來自陌生來源的鏈接，並在連接錢包之前始終驗證網站的真實性。

眾所周知，詐騙者還透過使用不存在的代幣創建交易對來利用去中心化交易所（DEX）。 這種策略特別危險，因為它允許用戶在不知不覺中將真實代幣兌換成假代幣，從而導致重大的財務損失。 為了保護自己免受此類詐騙，投資者在去中心化交易所交易時應謹慎行事，並僅參與經過徹底審查和驗證的信譽良好的項目和代幣。

電報詐騙：實施蜜罐技術

首先，騙子建立一個專門為吸引特定受眾而設計的主題電報頻道。 他們利用平台內建的廣告功能積極推廣自己的頻道，迅速累積了數萬名訂閱者。 最初，他們發布真實且引人入勝的內容，以建立信譽並與追隨者建立信任。

一旦該頻道獲得了大量追隨者，詐騙者就會巧妙地轉移他們的注意力。 在認識到 Telegram 的受歡迎程度和信任度後，他們利用這一點在受眾中製造了一種虛假的安全感。 這為蜜罐騙局的實施奠定了基礎。

詐騙者執行此騙局的主要方式之一是利用 Telegram 上當前的迷你遊戲熱潮。 他們為自己的遊戲做廣告，承諾推出遊戲代幣並鼓勵用戶連接錢包以儘早訪問和分發。 用戶不知道的是，這是一個騙局，旨在獲取他們的錢包並耗盡他們的資金。 重要的是要記住，如果您對某個項目不確定，切勿將錢包連接到該項目。

然而，騙子的策略並沒有就此結束。 他們還採用了蜜罐騙局的更複雜版本，涉及創建一個重複頻道，其中充滿了模仿原始頻道訂閱者數量的機器人。 然後，詐騙者將擁有真實觀眾的直播頻道的用戶名轉移到充滿機器人的虛假頻道。

在這個虛假頻道中，引入了欺詐性代幣或項目，旨在從毫無戒心的受害者那裡引誘資金。 一旦用戶投資，該管道就會迅速被設定為私人或關閉，使他們難以尋求補救或警告其他人。 同時，任何有關該騙局的投訴都會到達充滿機器人的虛擬頻道，在那裡它們可以被忽略而不會產生任何後果。

Telegram 中的這個安全漏洞允許詐騙者切換頻道用戶名，這是一個重大問題。 它強調用戶在使用 Telegram 頻道時需要保持警惕和謹慎，特別是那些宣傳金融機會或要求訪問錢包詳細資訊等敏感資訊的頻道。

為了保護自己免受 Telegram 上的 HoneyPot 詐騙，請遵循以下基本提示：

1。 驗證頻道的真實性：檢查頻道的歷史記錄、參與度以及管理員的可信度。 警惕突然流行的管道或那些宣傳不切實際的金融機會的管道。

2. 避免將您的錢包連接到未知的項目：切勿將您的錢包詳細資訊提供給您不確定的項目或管道。 詐騙者經常利用提前訪問或獨家優惠的承諾來誘騙用戶洩露他們的敏感資訊。

3. 隨時了解 Telegram 的安全功能：Telegram 定期更新其平台，提供新的安全功能和增強功能。 保持您的應用程式更新，以確保您免受最新的詐騙和漏洞的侵害。

4. 回報可疑活動：如果您懷疑某個頻道或使用者正在從事詐欺活動，請立即向 Telegram 報告。 您的報告可以幫助 Telegram 採取行動並保護其他用戶免受詐騙。

詐騙者採用的主要策略之一是創建主題 Telegram 頻道，該頻道最初似乎提供有價值的內容或吸引用戶參與迷你遊戲。 這些頻道利用 Telegram 內建的廣告功能進行大力推廣，迅速累積了數萬名訂閱者。 一旦建立起大量受眾，詐騙者就會開始積極宣傳他們的頻道，在用戶之間培養一種錯誤的安全感和信任感。

然而，真正的陷阱尚未出現。 詐騙者經常利用當前 Telegram 中小遊戲的流行，承諾推出自己的遊戲代幣並鼓勵用戶連接錢包以儘早分發。 一旦用戶連接了他們的錢包，詐騙者就會獲得訪問權限並耗盡所有資金，使受害者的帳戶空空如也。

在 HoneyPot 騙局的另一種變體中，詐騙者會創建一個重複頻道，其中充滿了機器人，模仿原始頻道並有現場觀眾。 然後，他們切換兩個頻道的用戶名，有效地將真正的詐騙頻道隱藏在機器人的外表後面。 這使得詐騙者可以在「即時」頻道上推出虛假代幣或項目，從而吸引毫無戒心的用戶的資金。 由於有關詐

騙的投訴會直接發送到帶有機器人的管道，因此支援人員可以忽略它們，從而給詐騙者帶來一種有罪不罰的感覺。

Telegram 中的這個安全漏洞正被駭客利用進行大規模詐騙，使用者必須保持警惕。 以下是一些保護自己免受 Telegram 上的 HoneyPot 詐騙的提示：

1. 將錢包連接到任何 Telegram 頻道或項目時請務必小心。 在採取任何行動之前，請務必進行研究並驗證管道或項目的合法性。

2. 尋找危險訊號，例如激進的廣告、不切實際的承諾或敏感資訊的請求。 這些通常是詐騙的跡象。

3. 避免點擊可疑連結或從 Telegram 頻道下載未知檔案。 這些可能包含惡意軟體或網路釣魚詐騙。

4. 如果您認為自己可能成為詐騙的受害者，請向 Telegram 支援報告任何可疑活動，並向社群尋求協助。

保護自己免受蜜罐攻擊

開始嚴格的驗證流程，仔細檢視管道、帳戶及其互動的真實性。 避開參與度低的管道，例如缺乏貼文反應或禁用評論，因為這些可能是欺騙的跡象。 此外，新建立的頻道及其管理頁面應該發出警報，促使進一步調查。

透過在信譽良好的第三方論壇和社群上驗證專案的合法性，利用群眾的智慧。 真正的努力通常會擁有概述其願景和機制的技術文件，智慧合約經過嚴格的安全審計以確保透明度和安全性。 在減輕與蜜罐計畫相關的風險方面，這種盡職調查是不容談判的。

在瀏覽可疑連結時要小心謹慎，無論它們是潛伏在頻道內容中還是以無辜評論的形式偽裝。 避免揭露敏感資訊的衝動，並在您的 Telegram 帳戶上啟用雙重認證 (2FA)，以加強您對網路釣魚嘗試的防禦。 對那些承諾在短期內獲得不切實際回報的項目保持警惕，因為它們可能是旨在利用你的貪婪的誘人陷阱。