NFT防盜指南丨如何保護自己的NFT資產安全？

原文：
https://www.btcc.com/zh-TW/academy/crypto-basics/nft-anti-theft-guide

隨著幾個熱門 NFT 項目獲得相當不錯的成績，NFT開始獲得越來越多的曝光率。但由於 NFT 的特性，不少駭客和不法分子也盯上了這一塊巨大的蛋糕。

但我們不需要太過擔心，NFT 等數字資產在區塊鏈級別中非常安全，很少會出現因為區塊鏈被駭客攻擊而失去資產的情況。通常，絕大部分的 NFT 盜竊和損失是由於持有者對資產的保護不夠充分造成的。

如果你對 NFT 感興趣，想要買入 NFT，或現在已經持有 NFT，那麼花時間來了解如何保護自己的NFT資產安全是十分必要的。

本文總結了幾種 NFT 防盜方法，一起來看看吧！

保護NFT安全的方法

1. 使用冷錢包（硬體錢包）儲存NFT

如果你現在正將自己的 NFT 資產儲存在託管錢包中，那麼需要盡快將它取出來，因為集中式的平台有時會被駭客入侵，從而造成 NFT 資產損失。

較好的選擇是將 NFT 放在冷*錢包*（硬體錢包）中。冷錢包通常是小型的物理設備，用於把你的數字資產與互聯網以及其他潛在危險隔離開來。通常你需要手動簽署每一筆交易，以防止其他人遠程竊取你的資產。

在冷錢包中，你可以完全控制你的資產安全性，但你需要存儲好自己的助記詞/私鑰，否則將無法取出自己的資產。

現在市場上有大量的冷錢包，且提供不同預算的選項，被認為是精明的加密投資者必備的工具。

不同硬體錢包的形式、功能以及整體的安全性可能會有較大的差異，但總的來說，冷錢包通常能比絕大多數集中式錢包提供更好的安全性。

此外，你還需要確保自己選擇的錢包支援你打算存儲 NFT 的區塊鏈，並且支援該 NFT 的代幣標準。

2. 選擇合適的 NFT 交易平台

在大多數情況下，NFT 交易平台是非託管平台，這意味著你可以始終控制自己的 NFT 資產。但是，NFT 交易平台會要求用戶授權他們的智能合約與平台上的資產進行交互。一旦這些智能合約存在錯誤，你的資產就很可能會受到攻擊。

因此，在選擇交易平台時，建議選擇高度安全又知名的 NFT 交易平台，檢查是否安全可以透過查看平台的公共審計——本質上是檢查平台的智能合約不包括任何錯誤和漏洞，且總體上對公眾使用是安全的。

對於尚未提供公共審計的一些新平台，如 LooksRare 等，可能就會具有挑戰性。但是有時風險與收益並存，如果平台提供豐厚的激勵措施和機會，你可以平衡機會與風險，決定是否嘗試新的平台。

最後，我們需要記住，並非市場上所有的 NFT 平台都是安全可靠的，在選擇自己想要交易的平台前，建議做好詳盡的調查，新平台尤其是如此。

3. 保護計算機免受病毒侵害

對於 NFT 持有者來說，計算機受到病毒侵害造成的影響可能是毀滅性的，因為攻擊者可以透過各種方式從你的計算機中竊取數據（包括你的私鑰），甚至可能遠程接管你的系統。

聽起來很恐怖，但是實際上保護計算機免受病毒侵害對你來說並不難。

首先，我們需要知道如何避開可能會在你的計算機安裝病毒代碼的地方。一些常見的攜帶病毒的場所包括山寨網站、提供可疑/非法訊息的網站、種子和其他P2P文件共享服務，有時候一些聊天室也會帶有病毒代碼。

要記住的是，任何情況下我們都不能安裝可疑程式或打開可疑來源給你發開的附件，大多數病毒代碼都需要你手動打開文件才能安裝。

此外，你可以考慮在你的計算機中配備強大的防病毒軟體，在日常使用中確保防火墻已經打開。這將有助於你的計算機避開偷渡式的攻擊，並且這些軟體還會提醒你計算機中存在的可以文檔。

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） <<<<

如何有效避免NFT詐騙

加密貨幣行業充斥著騙子和欺詐者，他們會利用各種手段將你的數字資產從錢包中提取出來。

避免這些騙局對很多 NFT 持有者來說是一個挑戰，尤其是對新手而言。但是，只要你能做到以下三點，你就能很大程度上避開 NFT 詐騙。

交易前仔細檢查URL：在遇到需要你登錄並訪問你的NFT的情況時，請仔細檢查你是否擁有正確的 URL，並在他們的社交媒體上交叉引用此連結，將連結添加為書籤，以防止陷入虛假連結中，丟失自己的數字資產。

警惕釣魚連結：NFT 持有者被騙的最常見方式之一就是相信了虛假的釣魚連結。通常詐騙者會冒充有信譽的個人、實體和組織發布帶有虛假連結的帖子，誤導 NFT 持有者點入錯誤錢包或開放自己的錢包權限。

因此，我們在看到感興趣的 NFT 訊息時，要確定是否為官方發布，其次確定消息是否可靠，不能因為一時之利讓自己產生更大的損失。

小心未知的電子郵件和消息：Telegram、Discord、Twitter 甚至您的電子郵件收件箱都可能出現垃圾郵件。這些郵件可能成為詐騙者盜取數據的工具——尤其是當您陷入數據庫洩漏時。如果您在以上這些（或其他）平台中的任何一個收到來自陌生人的未知訊息，那麼很可能這是一個騙局。切記，永遠不要將你的私鑰交給任何人，無論他們的原因或狀態如何，絕對不要授權你不熟悉的智能合約。

透過以上這些方法，相信你也可以避開 NFT 中大多數詐騙和盜竊，保護自己的 NFT 資產。