加密反黑客指南：多种措施保护好个人资产

作者：INSIGHTFUL；编译：深潮 TechFlow

### 免责声明

本指南无法保证任何内容，并不是从「加密或网络安全专家」的角度编写的，而是基于多个来源和个人经验的不断学习成果。

例如，我自己在刚进入这个领域时就曾因害怕错过（FOMO）和贪婪而受骗（假直播诈骗和假 MEV 机器人诈骗），因此我花时间认真学习、设置和理解安全性。

不要成为那个因为失去一切或大量资产而被迫学习安全的人。

### 黑客攻击还是用户错误？

所有类型的钱包、代币或 NFT 的「黑客攻击」或妥协大致可分为两类：

滥用先前授予的代币批准。

私钥或助记词泄露（通常发生在热钱包上）。

### 代币批准

代币批准实际上是允许智能合约访问并移动您钱包中特定类型或数量的代币的权限。

例如：

给予 OpenSea 权限以移动您的 NFT，以便您可以出售它。

给予 Uniswap 权限以使用您的代币进行交换。

作为背景信息，基本上以太坊网络上的一切，除了 ETH，都是 ERC-20 代币。

ERC-20 代币的一个特性是能够授予其他智能合约批准权限。

如果您想进行核心 DeFi 交互（如交换或桥接代币），这些批准在某个时候是必需的。

NFT 分别是 ERC-721 和 ERC-1155 代币；它们的批准机制与 ERC-20 类似，但适用于 NFT 市场。

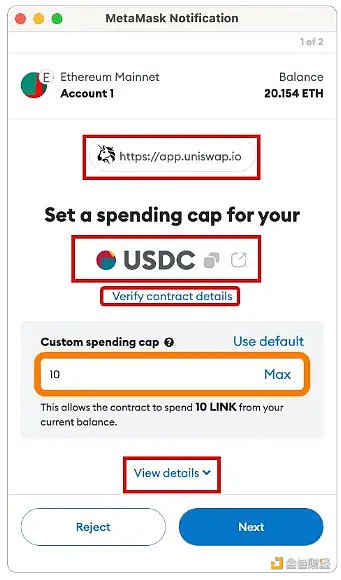
MetaMask (MM) 的初始代币批准提示提供了几条信息，其中最相关的是：

您正在授予批准的代币

您正在与之互动的网站

您正在与之互动的智能合约

编辑代币权限数量的能力

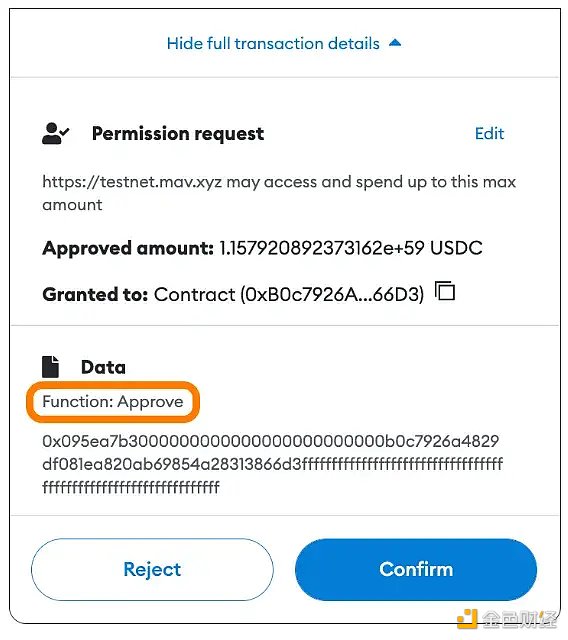


在完整详情下拉菜单中，我们看到一个额外的信息：批准功能。

所有 ERC-20 代币必须具有 ERC-20 标准所概述的某些特性和属性。

其中之一是智能合约可以根据批准的数量移动代币的能力。

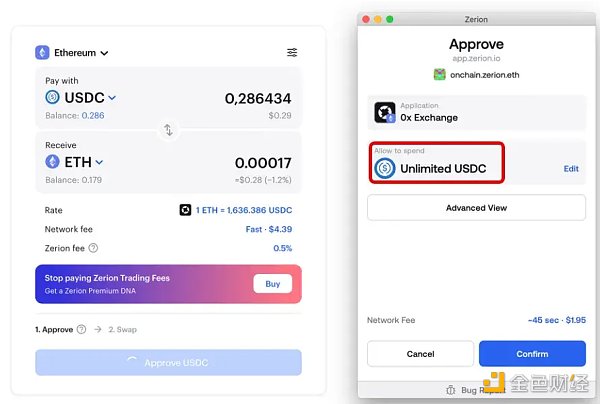
这些批准的危险在于，如果您将代币权限授予恶意智能合约，您的资产可能会被盗或耗尽。



### 无限制与自定义限制批准（ERC-20 代币）

许多 DeFi 应用默认会提示您对 ERC-20 代币进行无限制批准。

这样做是为了改善用户体验，因为它更方便，不需要未来可能的额外批准，从而节省时间和 gas 费用。



### 为什么这很重要？

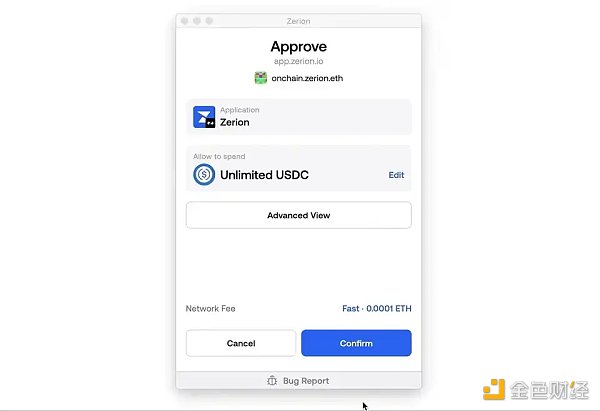
允许对无限数量的代币进行批准可能会让您的资金面临风险。

手动将代币批准设置为特定数量，可以限制该 dApp 在未签署新的更大额度批准之前，能够移动的代币最大数量。

这样可以降低您在智能合约被利用时的风险。如果您对某个 dApp 授予了无限制的批准，而该 dApp 出现漏洞，您可能会失去所有已批准的代币，这些代币来自持有这些资产并授予该批准的钱包。

例如，Multichain WETH（WETH 是 ETH 的 ERC-20 代币包装）就曾遭遇过这样的漏洞。

这个常用的桥接因滥用以前的无限制代币权限而被攻击，导致用户资金被盗。



下面是一个示例（使用 Zerion 钱包），展示如何将默认的无限制批准更改为手动批准。

### NFT批准

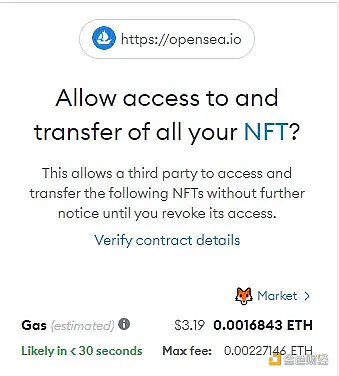
「setApprovalForAll」用于 NFT

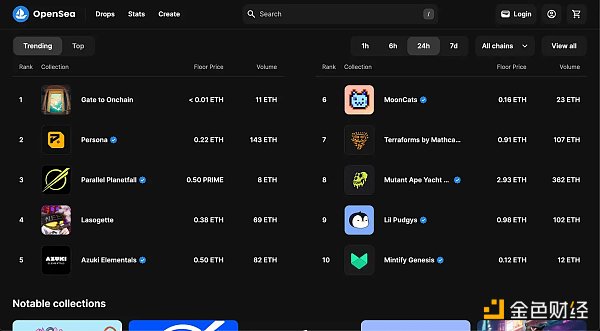
这是一个常用但潜在危险的批准，通常在您想出售 NFT 时授予值得信赖的 NFT 市场。

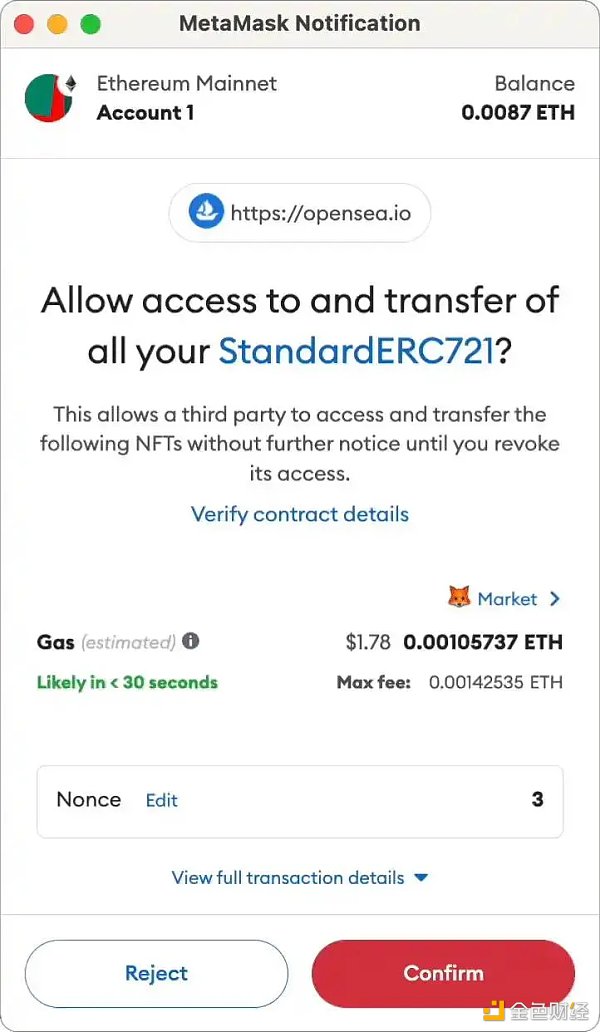
这使得市场的智能合约能够转移您的 NFT。因此，当您将 NFT 出售给买家时，市场的智能合约可以自动将 NFT 移动到买家那里。

此批准授予对特定集合或合约地址的所有 NFT 代币的访问权限。

这也可能被恶意网站或合约用来窃取您的 NFT。







### 恶意行为者滥用「setApprovalForAll」的示例

经典的「钱包账户缩水」在 FOMO 免费铸造的情况下是这样的：

用户访问一个他们认为是合法的恶意网站。

当他们将钱包连接到网站时，网站只能查看钱包的内容。

然而，恶意网站会扫描钱包中最高价值的 NFT，并提示用户从 MetaMask (MM) 对该 NFT 的合约地址进行「设置所有批准」。

用户以为自己在铸造 NFT，实际上却是在授予恶意合约移动这些代币的权限。

随后，骗子盗取代币，并在物品被标记为被盗之前，将其清算到 OpenSea 或 Blur 的出价中。

### 签名与批准

批准需要支付 gas 费，因为它们涉及交易处理。

签名则无需 gas ，通常用于登录 dApp，以证明您对该钱包的控制权。

签名通常是低风险的操作，但仍可能被用来利用先前授予的对像 OpenSea 这样的可信网站的批准。

对于 ERC-20 代币，您还可以通过无 gas 的签名修改您的批准，因为最近在以太坊上引入了允许功能。

如果您使用像 1inch 这样的去中心化交易所（DEX），可以看到这一点。

### 代币批准要点

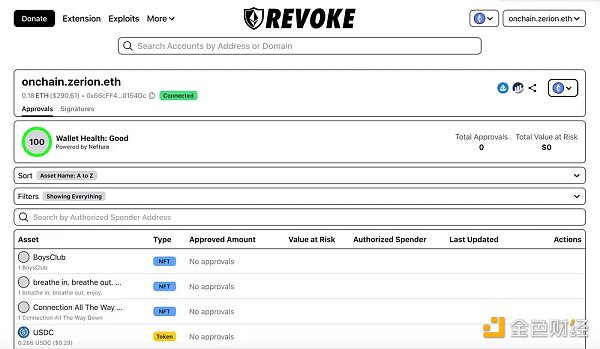
在给予任何批准时要谨慎，确保您知道自己在批准哪些代币以及对哪个智能合约（可利用 etherscan）。

限制您的批准风险：

使用多个钱包（批准是特定于钱包的）——不要对您的保险库或高价值钱包签署批准。

理想情况下，减少或完全避免对 ERC-20 代币授予无限制批准。

定期通过 etherscan 或 revoke.cash 检查和撤销批准。



### 硬件 / 冷钱包

热钱包通过您的计算机或手机连接到互联网，密钥和钱包凭证在线或本地存储在您的浏览器中。

冷钱包是硬件设备，密钥在完全离线的状态下生成和存储，并且物理上靠近您。

考虑到一个 Ledger 的价格大约为 $120，如果您有超过 $1000 的加密资产，您可能应该购买并设置一个 Ledger。您可以将 Ledger 钱包连接到您的 MetaMask (MM)，以便在保持一定安全性的同时享有与其他热钱包相同的功能。

Ledger 和 Trezor 是最受欢迎的选择。我喜欢 Ledger，因为它与浏览器钱包（类似于 Rabby 和 MM）的兼容性最好。



### 购买 Ledger 时的最佳实践

始终从官方制造商网站购买，切勿在 Ebay 或 Amazon 上购买——可能会被篡改或预装恶意软件。

确保您收到物品时包装是密封的。

第一次设置 Ledger 时，它会生成一个助记词。

只能将助记词写在物理纸上，或者在未来将其写在钢板上，以确保您的助记词短语防火防水。

绝不要拍摄或在任何键盘（包括手机）上输入助记词——这会将助记词数字化，您的冷钱包将变成不安全的热钱包。

加密资产并不是存储在硬件钱包上，而是「在」由助记词短语生成的钱包中。

助记词短语（12-24 个单词）是所有的一切，必须不惜一切代价保护和安全。

它提供对所有在该助记词短语下生成的钱包的完全控制和访问权限。

助记词不是特定于设备的，您可以将其「导入」到另一个硬件钱包中作为备份（如果需要）。

如果助记词丢失或损坏，并且原始硬件钱包也丢失、损坏或被锁定，您将永久失去对所有资产的访问权限。

有多种助记词存储方法，例如，将其分成多个部分，增加部分之间的物理距离，存放在不明显的地方（例如，冰箱底部的汤罐，您财产地下的某个地方等）。

至少您应该有 2-3 份副本，其中一份应为钢制，以防水和火灾。

「私钥」类似于助记词短语，但仅针对一个特定钱包。它通常用于将热钱包导入新的 MetaMask (MM) 账户或在自动化工具（如交易机器人）中使用。

### 第 25 个单词 - Ledger

除了原始的 24 个单词助记词，Ledger 还提供一个可选的额外安全功能。

密码短语是一项高级功能，可以将您选择的最多 100 个字符的第 25 个单词添加到您的恢复短语中。

使用密码短语会生成一组完全不同的地址，这些地址无法仅通过 24 个单词的恢复短语访问。

除了增加安全层，密码短语在您受到威胁时还能提供合理的否认。

如果使用密码短语，务必安全存储或准确记住它，逐个字符并区分大小写。

这是针对「$5 扳手攻击」这种身体威胁情况的唯一和最终防御措施。

为什么要经历这么多麻烦来设置硬件钱包？

热钱包将私钥存储在连接到互联网的位置。

通过互联网被欺骗、误导和操纵以泄露这些凭证是极其简单的。

拥有冷钱包意味着，骗子需要物理上找到并获取您的 Ledger 或助记词才能访问这些钱包及其内部资产。

助记词一旦被泄露，所有热钱包及其中的资产都将面临风险，即使那些没有与恶意网站或合约互动的资产也不例外。

### 过去人们被「黑客攻击」的常见方式

过去人们通过热钱包遭遇「黑客攻击」（助记词短语泄露）的常见方式包括：

被欺骗下载恶意软件，例如通过工作机会 PDF、测试版游戏、通过 Google 表格运行宏，或模仿合法网站和服务。

与恶意合约互动：在模仿网站进行 FOMO 铸造，或与未知空投或接收的 NFT 合约互动。

将密钥和助记词插入或发送给「客户支持」或相关程序 / 表单。