硬件钱包100%安全？你需要了解的2类欺诈

作者：Bitrace

硬件钱包是一种专为储存加密货币设计的物理设备，被认为是安全存管加密资产的重要手段。其内置的安全芯片离线存储私钥，确保用户掌握加密货币的完全控制权。硬件钱包通常在离线状态下操作，这进一步减少了被互联网黑客攻击的风险。

然而，在投资者群体普遍缺乏了解的情况下，仍然出现大量针对小白用户的欺诈事件，导致其存放在硬件钱包中的资产丢失。本文将介绍两种常见的硬件钱包盗币手法——硬件钱包说明书欺诈与硬件钱包改造伪装骗局。

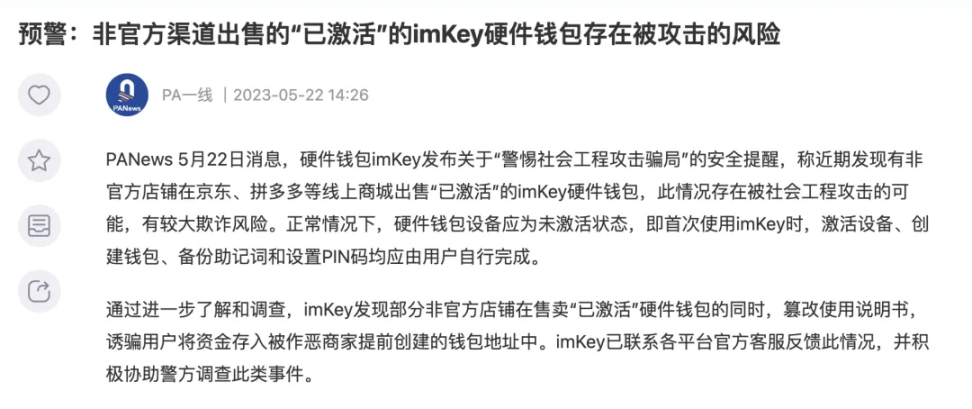
### 硬件钱包说明书欺诈

此类盗币手法核心是利用普通投资者对硬件钱包使用方法的不了解，通过替换虚假说明书，误导受害人向钓鱼地址转账。受害人从第三方电商平台购入硬件钱包，打开包装后，按照「说明书」上标注的「初始 Pin 码」打开硬件钱包，在备份了「说明书」上印制的「助记词」后，向钱包地址存入了大量资金，最终失窃。



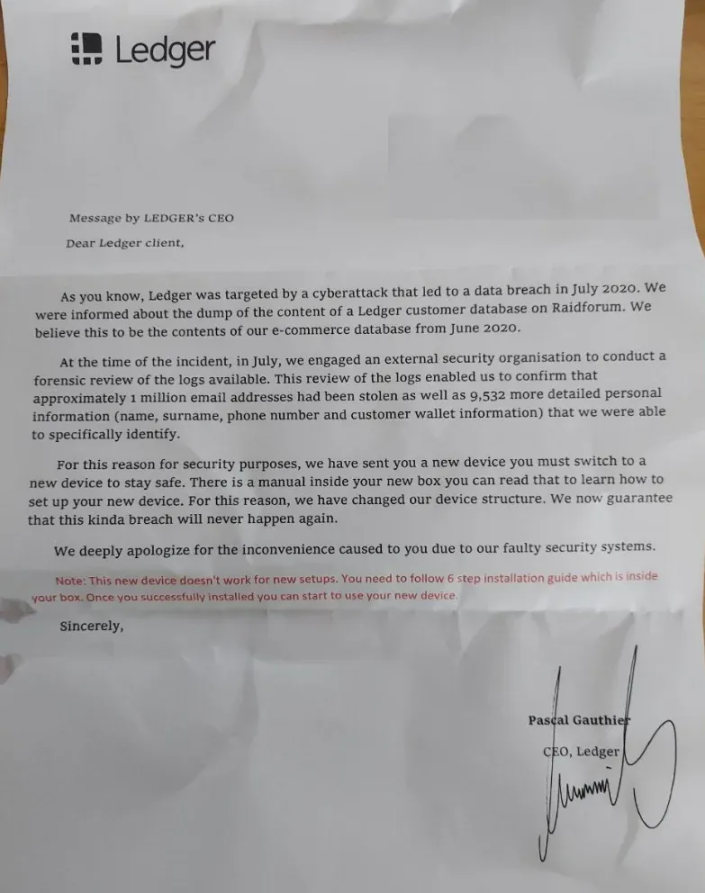
其原因并非钱包在硬件层面遭到破解，而是盗币者通过提前激活获取地址助记词，伪造虚假说明书进行二次封装，再通过非官方的渠道将已激活的硬件钱包销售给受害人，一旦目标对象向地址内转入加密资产，就将进入标准假钱包盗币流程。

华语地区的二级市场上也存在类似风险，知名硬件钱包厂商 imkey 曾发布提醒——发现部分非官方店铺在售卖「已激活」硬件钱包的同时，篡改使用说明书，诱骗用户将资金存入被作恶商家提前创建的钱包地址中。可见，识别官方电商店铺的重要性等同于识别官方网址。

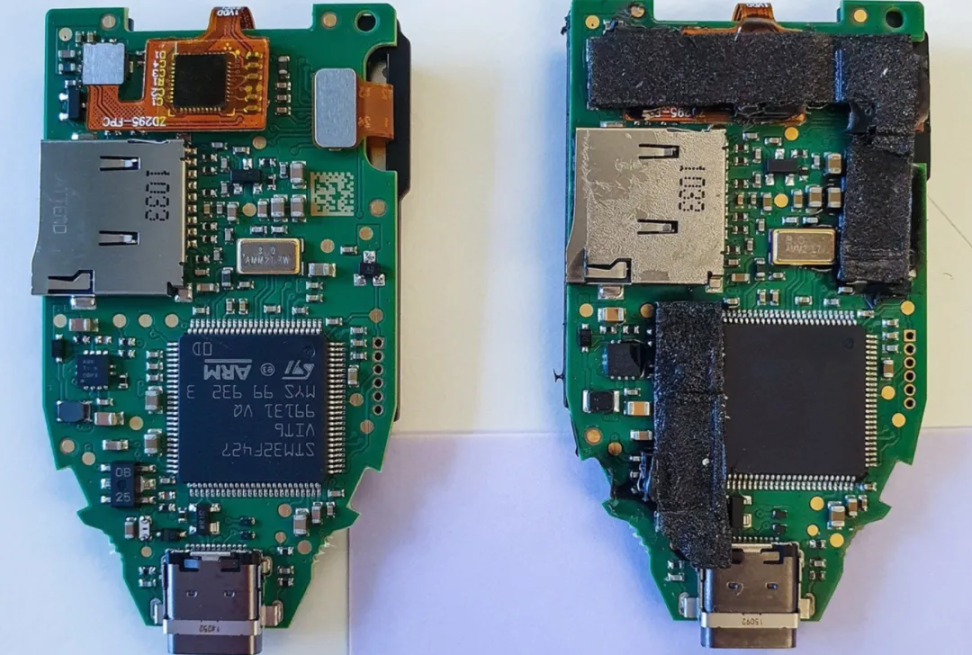


### 硬件钱包设备遭改造

一位 Ledger 用户在未曾下单的情况下收到一个包裹，内含有一个全新的 Ledger X 硬件钱包和一封附带的信件。信件表示，由于 Ledger 公司遭受网络攻击导致用户数据泄露，特此向受影响的客户发送了新的硬件钱包设备，并在信件中要求用户更换设备以保证安全。



然而，这封信的真实性存疑，Ledger 公司 CEO Pascal Gauthier 明确表示，对于个人数据的意外泄露，公司不会做出任何赔偿。该用户也表示这是一个骗局，他分享了更多的图片，并打开设备展示了硬件钱包塑料盒内部，明显有被篡改的痕迹。



此外，卡巴斯基安全团队也曾通报了一起仿冒 Trezor 硬件钱包的案例，受害人在非官方渠道购买了一台 Trezor Model T ，但该设备已经被攻击者更换内部固件，将能够获得对用户加密资产的访问权限，进而采取盗币行为。

### 写在最后

通过上述案例不难看出，针对硬件钱包的供应链攻击已经非常广泛，普通投资者以及硬件钱包厂商应当对此提高警惕。正确的使用方式将能有效规避盗币风险：