Web3安全警示丨看似转账测试，实则盗取资产，警惕来路不明的收款二维码

近期，Bitrace 收到一例援助请求，受害人称其在扫码向对方转账 1 USDT测验后，钱包剩余资金尽数被盗。“我仅仅是扫了一下二维码，怎么就会被盗”，受害人对此表示不解。

本文将深入剖析二维码转账测试骗局的实现手段，结合真实案例展开链上追踪，以提醒用户在加密货币交易中时刻保持警惕。



### 骗术解读

深入了解情况后我们发现，表面上这是一种通过收款二维码转账测试以实施盗窃的新型诈骗手段，本质上是骗取钱包授权。

骗子通过社交平台添加用户为好友，建立初步的信任后，寻找合适的时机抛出 OTC 请求。他们会通过略低于市场价的汇率吸引用户，在双方就交易细则达成一致后，对方会主动向用户打款小额 $USDT 博取信任，并以长期合作为由慷慨地提供 $TRX 作为手续费。

来不及感慨遇到了「大善人」，用户便收到了一张收款二维码的截图，这时，骗子会要求用户进行小额回款测试。



通过一系列前期铺垫，用户的交易风险似乎已降至最低。“回款的 $USDT 和交易需要的手续费都是对面转我的，就算是骗子我也不会有损失”，思考后用户便扫码回款，不料资金尽数被盗。



下面以一起真实案例中受害人提供的收款二维码为例进行骗术拆解。

Bitrace 使用空钱包测试扫描后，出现了一个第三方网站https://sktnid[.].com/，通过引导后便来到如下界面。截图右上角标记“欧易官方认证”，支持 USDT 汇款，此页面十分劣质，但缺少经验的用户较难辨别，殊不知危险已悄然而至。



当用户在此界面按照骗子的要求输入指定的回款金额后，点击“下一步”便跳转至钱包的签署界面，一旦再次点击确认，即与智能合约产生交互，此时钱包的授权被窃取。骗子通过授权把受害人的资产全部转移。

一次精心铺垫的以小额转账测试为由，通过二维码骗取授权的骗局就此完成。

### 资金分析

扫码转账测试骗局的成功率及危害性远比想象中高。Bitrace 进一步分析受害人提供的地址后发现，在 2024.7.11 - 2024.7.17 仅一周的时间内，嫌疑人地址TT...m1mV1已通过这一手段骗取 27 名疑似受害人近 12 万 USDT，经流 5 层地址后分别转入 3 个 Huione 账户进行资金清洗。



区块链的匿名特性，使得加密资金转账追踪存在难度，即使找到地址，要找出地址背后的实体也存在困难。幸运的是，Bitrace 通过该团伙收款二维码显示的 TD...XRWVe 地址，回溯初始手续费来源，结果显示为某中心化交易所。这使得匿名的链上地址与现实身份有了连结。



目前，Bitrace 已指导受害人联系警方报案，以期帮助受害人通过合规的执法流程提升资金追回概率。

### 写在最后

对于不走平台的场外 OTC，用户务必谨慎核实对方身份，不轻信任何来历不明的二维码及链接。此外，在交易前，对对手方地址进行风险筛查十分重要，Bitrace 即将上线风险一键速查工具，旨在帮助用户识别目标地址的潜在风险，支持免费体验，敬请关注。