在币圈里，虚拟货币被盗成为常见的事情。不管是个人钱包被盗还是交易所钱包被盗，最后承担损失的都是投资者自己。所以，保证钱包的安全是很重要的事情。

在热钱包使用的时候，都会让你记住所谓的助记词，其实这个助记词就相当于你的私钥，只是他用更简单的形式展示出来。平台会把你的私钥和这个助记词一一对应保存在服务器中，但是这时候就有个问题是：如果哪一天黑客把这个服务器给攻破了，你的私钥也就会随之丢失，数字资产随时会被转走。比如之前币安被黑客攻击一夜被盗7个亿，曾是世界上比特币第一大交易所的Mtgox更是因为被黑客攻击而倒闭。

所以，基于这一点，建议虚拟币持有者尽可能地去使用冷钱包来保障自己的资产安全，因为冷钱包平台不会保存或备份你的私钥，私钥是保存在本地的。即使黑客攻击了官方的服务器也根本没法获得你钱包的信息。

为了防止丢币，这个时候最重要的就是：

1.我们自己一定要把私钥保存好。千万别保存在什么网盘、联网的电脑、甚至是微信，更不要去截图，这不是懒的时候。可以把私钥中的代码全部都抄写到本子上放在保险箱或者其他安全的地方，可别随手一扔，到时候不小心当了烧火纸用那就真的要哭晕在厕所了。

2.尽量多保存几份。比如在纸上抄一份或多份，在u盘上也在备份一次，在电脑上登录钱包之前注意好好杀杀毒，一些不该看的网页，是吧，少看，防患于未然嘛。针对网页上的安全提示不要心存侥幸，像这次mytherwallet事件那些被骗的用户，后悔也晚了，所以宁可错过，不要做错。

虚拟货币网络里的东西是每一笔“交易”，是不能离开网络的。但私钥和地址是完全可以不存储在网络服务器上的，以此最大程度保证钱包资产安全，这是最关键的，也是每一个圈内玩家最需谨记的。

对于币圈小白来说，希望能通过区块天眼APP上的曝光栏，大家可以识别币圈里的套路、骗局，学会保护自己。