数字货币世界是最需要关注信息安全的地方。如果你有任何闪失和粗心大意，你可能会失去所有的硬币和NFT。

1.永远不要重复使用你的密码

因为你永远不知道自己注册的网站是否有一天会出现安全漏洞。

如果想查看自己使用的账号密码是否有泄露的可能，可以去这个网站：haveeibeenpwned。com

。

2.使用密码管理器来帮助你管理密码

如果你注册了很多网站，每个网站都使用唯一的密码，那么你需要一个密码管理器来帮助你管理密码。

。您可以使用密码管理器，如1Password或LastPass，使您管理密码更容易、更安全。

3.每个重要帐号都加上2FA（双重认证机制）验证

尽量不要用SMS(短消息)作为你的2FA认证，因为信息可能会被黑客截获，电信公司也可能有破绽。

您应该使用2FA认证工具，如GoogleAuthenticator或Authory。如果使用Authory，建议你备份到另一部手机后关闭多设备功能。

4.用硬件2FA

如果你有很多钱要管理，可以考虑硬件2FA，比如USB设备比如Yubico，GoogleTitan或者忒提丝，如果你用这个方法的话。

，您需要在登录前使用这些设备验证您的身份。

硬件2FA

5.使用数字货币冷钱包

如果您使用Metamask或其他热门钱包来管理您的数字货币资产。

请将资产转移到Trezor或Ledger的冷钱包中。黑客时刻关注着热门钱包是否存在漏洞。如果你有很多资产还在热钱包里，请马上买个冷钱包。

6.卸载不明的Chrome套件

Chrome套件对你浏览网页是有帮助的，但是有些套件可能是恶意软件，你可能在安装的时候给他太多权限读取你电脑里的数据。

唐&#039；除非你100%信任这个包的开发者，否则不要冒这个险。

7.把钱包套件独立出来

如果您必须使用其他Chrome包，请将Metamask包放在另一个独立帐户下。

。您可以为每个钱包套餐创建不同的帐户。

8.限制智能合约的允许（Enable）使用代币上限

当你与智能合约交互时，你会经常看到智能合约要求你给它令牌的使用权。

除非你百分百信任团队，否则不要&#039；不要给它无限的令牌权。如果代码有漏洞或者团队恶意跑路，你的钱包可能就被清空了。

智能合同权限设置

9.不要暴露你的地址信息

如果你想时不时的用数字货币转账，尽量用交易所转账，比如币安，FTX。频繁使用私人地址转账可能会在网上暴露各种个人信息。

10.保护你手机的资安

美国已经发生多起SIM卡被劫持的事件。请尽量保证手机安全。

11.不要点击来路不明的广告

请养成不点广告的习惯！

钓鱼网站经常使用与知名网站相似的名称来迷惑用户。尤其是现在谷歌放宽了数字货币广告的限制，会出现更多的钓鱼网站来欺骗用户。

12.小心空投信息跟私信

最近经常有各种关于诈骗空头或者收集免费代币的信息，无论是在脸书，YouTube还是Discord，Telegram私信等等。有太多的信息需要控制。记住，天下没有免费的午餐。

如果他一开始就想给你送钱，有很大可能是诈骗。

13.永远不要打开陌生的档案或文件

你永远不知道这个文件会不会偷偷帮你安装一个键盘记录器。

记得把你的电脑设置成总是显示分机，不要&#039；不要随意打开压缩文件。

14.小心E-mail地址

你有没有注意到下面截图里的邮件有什么奇怪的地方？

注意是否Coingecko&#039sI少了一点，黑客就会用这个特殊的文字来骗你。