区块链领域有很多数字货币骗局。最常见的诈骗包括：勒索、虚假交易平台、礼品诈骗、社交媒体网络钓鱼。剪贴板劫持者&quot恶意软件、钓鱼邮件、庞氏骗局和传销以及勒索软件。

本文，我们将简单介绍每一种骗局，让您学习和掌握应对常见比特币骗局的有效措施，爱护您的数字货币资产。

简介

每当一项新技术问世，犯罪分子就会闻风而动，伺机行骗。遗憾的是比特币作为一种无国界的数字货币，给设计数字货币骗局的不法分子创造了绝佳的机会。

比特币的去中心化特性让用户可以完全控制自己的投资。然而，这一特点的缺点是很难为其制定一个适当的监管和执法框架。。不法分子设计陷阱，诱导用户在使用比特币时出错，最终成功盗取比特币，受害者几乎没有办法挽回损失。

因此，了解犯罪分子的诈骗手段，识别潜在的危险信号非常重要。。需要警惕的比特币骗局有很多种，有些比较频繁。因此，我们将讨论八种常见的比特币骗局及相关防范策略。

常见比特币诈骗及防范策略

勒索

勒索是犯罪分子常用的手段，用手中的敏感信息威胁他人，非法索要钱财。他们通常要求以数字货币支付赔偿，最常选择的货币是比特币。

犯罪分子收集或编造敏感的个人信息，并向受害者施加压力。迫使他们支付比特币或其他货币。

防止比特币勒索的最佳策略是谨慎选择自己的登录凭据，密切关注自己访问过的网站以及在哪些网站上留下了个人信息。使用双因素身份认证也是明智的预防措施。。即使不法分子利用虚假信息勒索钱财，你也能立即知晓并采取对策。

假交易平台

顾名思义，假交易平台是合法交易平台在数字货币上的仿冒品，诱骗用户在此交易。。这种骗局通常以手机app的形式出现，也有可能是桌面应用或假冒网站。与&quot真人&quot，有些假的交易平台几乎可以以假乱真，所以一定要仔细辨别真伪

。这些假的交易平台看起来合法，但其目的是窃取数字货币。

他们往往以免费的数字货币、诱人的价格、低廉的交易费用甚至赠品来诱惑数字货币交易者和投资者。

为了防止这种欺诈行为，我们应该对合法交易平台的真实网址进行书签标记。，每次登录前请仔细检查。我们还可以使用货币安全验证来检查网站、电报组和Twitter帐户的合法性。

至于手机App，需要审核开发者信息、下载量、用户评价。

礼品骗局

通过赠送骗局盗取数字货币的常用方法是用免费赠品换取小额金钱。犯罪分子一般会要求受害者先将钱转到特定的比特币地址，并允许更多的比特币作为回报(比如转0.1个比特币可以获得0.5个比特币)。然而转账后，受害人不会收到任何礼物，也无法追回资金。

礼品骗局种类繁多。除了比特币，不法分子还会骗取其他数字货币(如以太坊、币安币、XRP等。).有时候，他们可能会询问私钥或其他敏感信息。

Twitter等社交平台是赠送骗局的重灾区。犯罪分子经常在社交平台上的热门推文、重要新闻和公告(如协议升级公告或ICO公告)中寻找机会。

防止礼品欺诈最好的方法就是不要贪图小利，拒绝一切需要提前转账的礼品活动。合法捐赠活动从不要求参与者提供资金。

社交媒体钓鱼

社交媒体钓鱼是一种常见的比特币骗局。。像礼物骗局一样，这种骗局在社交媒体上也很常见。犯罪分子经常在社交媒体上创建账户，冒充数字货币(也称为&quot冒名顶替者&quot).之后，他们通过推文或聊天信息发送假礼物。

防止社交媒体钓鱼的最佳策略是仔细核对，验证对方是否真的是自己。一些社交媒体平台为认证用户添加专属标志，如Twitter和脸书，它们使用蓝色复选标记。

剪贴板劫持程序恶意软件

以&quot剪贴板劫持者&quot恶意软件窃取资金是非常秘密的。他们劫持剪贴板数

据，只要你一不小心，资金就会直接转到犯罪分子的账户上。

比如你想把比特币转给你的朋友鲍勃。正常操作模式是Bob提供他的比特币地址，然后你复制粘贴到你的比特币钱包里。但是，如果你的设备被剪贴板劫持者恶意软件入侵，软件会在粘贴地址的瞬间，自动将地址替换为不法分子的比特币地址。。只要你发送并确认交易，你所有的比特币都会落入不法之徒手中，鲍勃将收不到任何钱。

为了防止这种骗局，我们必须时刻注意电脑的安全，警惕各种可疑的消息或邮件。，可能带有受感染的附件或危险链接。请注意您浏览的网站和设备中安装的软件。还可以考虑安装杀毒软件，定期扫描设备，筛查潜在风险。此外，及时更新设备的操作系统(OS)也非常重要。

钓鱼邮件

钓鱼的形式多种多样，最常见的方式就是使用钓鱼邮件。在电子邮件中，犯罪分子诱使收件人下载受感染的文件或点击链接访问看似合法的恶意网站。。这类邮件模仿用户常用的产品或服务向其发送信息，危险性极大。

犯罪分子通常会在邮件中催促收件人立即采取行动，以确保账户和资金的安全。他们可能会要求对方更新自己的账户信息、重设密码或上传文档。目标通常是收集登录凭证和窃取帐户信息。

防止网络钓鱼电子邮件的第一步是检查电子邮件是否是从原始来源发送的。如果有疑问，可以直接联系相关公司，确认是否发了邮件。然后您也可以将鼠标悬停在链接上(无需点击)来检查URL中是否有拼写错误、异常字符或其他异常。唐&#039；不要点击链接，即使你没有&#039；我没有发现任何危险迹象。如果您需要登录您的帐户，建议您手动输入网址或从收藏夹打开网页。

庞氏骗局和传销

庞氏骗局和传销是最古老的金融骗局。庞氏骗局的欺骗策略是不断吸收新投资者的资金，并向早期成员支付投资回报。一旦罪犯能够&#039；不能吸引新的投资者，资金链会断裂。OneCoin是数字货币庞氏骗局的经典案例。

传销是一种商业模式，按照注册会员招募新会员的数量向其支付费用。一旦没有新成员加入，资金链也会断裂。

在传销中，参与者需要做更多的工作：组织者在最上面。他们会招募一定数量的人

为他们工作，这些人也会招募自己的人，以此类推，最后得到一个庞大的架构，这个架构会成倍的增长和扩张。，不断产生新的关卡(因此得名&quot金字塔&quot)

防止这两种骗局的最好办法就是仔细研究购买的数字货币，无论是假币还是比特币。如果数字货币或比特币基金的价值完全来自新的投资者或成员，，很可能是庞氏骗局或者传销。

勒索软件

勒索软件是一种恶意软件，可以锁定用户&#039；移动设备或计算机，并阻止他们访问重要数据。除非支付赎金(通常是比特币)，否则无法解锁。。这类软件破坏力极强，如果医院、机场或政府机构不幸被抓，后果严重。

赎金软件通常会阻止用户访问重要文件或数据库，威胁他们在规定期限前支付赎金，否则将彻底删除数据。不幸地即使赎金支付了，我们也可以&#039；我不能保证罪犯会遵守诺言。

我们可以采取以下措施来防范勒索病毒的攻击：

安装杀毒软件，及时更新操作系统和应用程序。

避免点击广告和可疑链接。

小心处理电子邮件附件，特别注意带有&quot。exe&quot，&quot。vbs&quot和&quot。scr&quot。

定期备份文件，即使设备被感染也可以恢复。

访问NoMoreRansom获取防范勒索软件和免费系统恢复工具的建议。

总结

比特币骗局种类繁多，需要警惕。但是，防止被骗的第一步是了解这些骗局的实施过程。只有学会如何防范这些最常见的比特币骗局。