各位老铁们，大家好，今天由我来为大家分享比特币大事件，以及比特币重大事件的相关问题知识，希望对大家有所帮助。如果可以帮助到大家，还望关注收藏下本站，您的支持是我们最大的动力，谢谢大家了哈，下面我们开始吧！

本文目录

比特币抢劫事件层出不穷，如何在保护财产的同时保护人身安全？

比特币，让人爱，又让害怕。爱是因为，巨大的涨幅带来的回报，害怕是因为可能引发人身安全的风险，比特币也可能被黑客盯上而不翼而飞。

一，如何确保比特币的安全呢?

第一点，不要把比特币放在交易所，所有数字货币的交易所都不安全，前几年日本交易所就被黑客攻击导致破产。同时，交易所自身也是缺乏底线，可能监守自盗，也会与黑客串通起来，里应外合将客户的比特币盗走。

第二点，比特币最好放在自己的钱包里面，需要把交易所里面的比特币提取出来，保管在自己的钱包，这样比较安全。不过，选择什么钱包就很关键了，建议选择全节点的硬件钱包，虽然比较麻烦，但是更加安全。现在市场上的很多钱包，都有后门，也有风险，您的比特币放在里面，很有可能也会被盗。

第三点，最好买一台新电脑，做比特币的交易和钱包的保管。新电脑，中病毒的可能性比较小。新电脑，也不要经常上网，减少中病毒的概率。

第四点，做好钱包和比特币的备份。买几个大品牌的硬盘，作为硬件钱包，相互备份，防止文件损坏。

第五点，硬件钱包，最好分开地方存放，不要集中在一个地方。比如，如果全部放在家里，万一被偷了，就很麻烦。建议在银行开一个保险箱，用来存放备份的硬件钱包。

第六点，不要告诉任何人，自己买了比特币。害人之心不可有，防人之心不可无，如果自己说者无心，听者有心，告诉别人买了比特币，可能就会被盯上，引发风险

。

二，看看近期全球的比特币风险事件。

苹果联合创始人史蒂夫·沃兹尼亚克，在纽约时报全球商业峰会上说，“我有7枚比特币通过欺诈被偷走了。就连苹果创始人的比特币，都会被偷走，更何况普通人呢。

欧洲刑警组织的网络犯罪分析人士JarekJacubchek，最近告诉BusinessInsider，网络犯罪分子的选择从比特币转移到了其它数字货币上。随着比特币的价格上涨，黑客或者犯罪分子，更会盯上比特币，因为巨大利益会让坏人更容易做坏事。

2018年2月，韩国和日本又发生交易所被盗的事件，还有香港在去年也发生数字货币被盗的事件。

黑客利用软件和网站挖币。根据卡巴斯基实验室的数据，2016年至2017年，利用受害者电脑硬件资源，挖掘加密虚拟货币的攻击增加了近1.5倍。

三，比特币与人生。

比特币，大多数人无法理解，也不相信比特币。

比特币就是20年前的互联网，也是20年前的房地产，具有很好的长期投资机会。

我们需要重视这个机会，必须加强学习，才不会被时代和科技淘汰。

关注微信公众号：雄风投资

比特币勒索邮件怎么处理？

比特币勒索邮件是指邮箱里收到一封电子邮件，邮件的内容一般含有：电脑上的恶意软件已经通过网络摄像头捕获到了收件人的不雅照片、知道收件人的真实密码等，让收件人产生恐惧，并要求以“比特币”的形式支付封口费。

这种比特币勒索邮件的内容往往是以英文或者日文的形式出现，如下图：

英文版

日文版

这种勒索邮件并不可信

这种手法其实是特别拙劣，你的电脑也没有所谓的恶意软件和木马。真正的恶意软件勒索长这样：

并且电脑内的文件都会被加密。对于黑客而言，他通过木马获得密码，也会直接使用病毒勒索，而不是使用门槛最低的邮件。

那勒索邮件内的密码，是从哪里获得的呢？

密码可能并不是从我们本地的电脑泄露的，而是由一些网站或平台因为各种原因，泄露了用户的账户名或明文密码。

一些黑客就将他们打包成“数据包”，在暗网上公开出售。而这些账户，大多为邮箱名，所以只能通过邮件进行敲诈勒索。

举个例子：

2011年CSDN曾曝出遭遇密码泄露事件，600万用户信息被泄露。随后，密码泄露事件波及天涯论坛等网站，4000万账户密码陆续遭泄露。这些密码，全部都是以明文的形式泄露，成为了敲诈勒索的渠道。

这种勒索邮件只是最普通的勒索方式，可怕的是针对特定对象的定制勒索。比如勒索邮件中附带的一张PS的“不雅照片”，这种PS痕迹是比较严重的，只有头像是自己的，照片中的身份和背景并不是自己的。

为什么勒索比特币？

与比特币相关的勒索案件屡见不鲜，花样百出，就是比特币匿名、难以追踪，一串私钥就对应一笔“钱”，正好符合勒索人的需求。

与常见的货币不同，比特币不依靠特定的货币机构发行，它只是依据特定的算法通过大量的计算产生，所以它可以绕开银行系统，并且可以轻易的跨国交易。比特币使用这个P2P网络中众多节点构成的分布式数据库来确认、记录交易行为，并使用密码学设计来确保各个环节的安全性。这些都让比特币具有了不易溯源，不会暴露身份，而且可以快速广泛流通。

在很多人眼中，“自带光环”的比特币成为了争取货币自由、实现资产增值、发展致富技术的有声力量，但它还有着另一幅面孔：犯罪分子的帮凶。

中国互联网金融协会发布《关于防范比特币等所谓“虚拟货币”风险的提示》，称比特币等所谓“虚拟货币”缺乏明确的价值基础，比特币等所谓“虚拟货币”日益成为洗钱、贩毒、走私、非法集资等违法犯罪活动的工具，投资者应保持警惕，发现违法犯罪活动线索应立即报案。

收到比特币勒索邮件该怎么办？

一般情况下是可以忽略这种邮件，因为这种邮件都是大规模群发的，虚晃到一个是一个。如果涉及到真实的账户和密码，可以分析一下是通过什么渠道泄露出去的，并且马上更改一些重要的密码。

如果勒索人通过邮件还会有下一步的行动，并且确实掌握了很多重要的资料。那么无论如何都不要给勒索人转比特币，这绝对是一个无底洞，保留好所有的证据，报警是好的选择。

以上个人浅见，欢迎批评指正。

认同我的看法，请点个赞再走，感谢！

喜欢我的，请关注我，再次感谢！

这次的比特币劫持事件，会不会让苹果的Mac销量猛增？

这次病毒攻击的主要对象是政府部门和企事业单位，而政府部门和企事业单位要求的电脑系统兼容性要求高，短期内更换至苹果Mac是不可能的，况且苹果Mac的系统软件不足，这事硬伤。苹果Mac系统也有bug也有病毒，只是用户量少没被媒体放大罢了。现在你去买一台苹果的Mac电脑，不出一个月你还是要装Windows系统，结果还是会中毒，我们能做的就是多买一个移动硬盘，把重要的资料放进移动硬盘进行储存备份。总结不：大卖的不是苹果Mac电脑而是移动硬盘或者U盘。要涨的不是苹果的股价，而是希捷、三星、西部数据等股价。

下一个引爆比特币大跌的可能是什么事件？

应该是usdt暴雷吧。usdt暴雷绝对是币圈核武器。usdt是币圈虚拟货币之间的流通凭证，其兴衰直接关系币圈兴亡。泰达公司充当了央行角色，通过发行usdt推动币价上涨，再卖出虚拟币完成套现。所有的盈利可以拿出一部分充做储备金，并超额发行usdt。超发的usdt继续进入币圈流通，进一步推高币价，击鼓传花的游戏就能一直玩下去。其实泰达公司从未承诺1:1储备金保证，其信用风险具有很大不确定性。其暴雷是早晚的事，至于什么时候暴雷，我想应该会有征兆。

我一直相信usdt会暴雷，有这几个方面考量。首先币圈良莠不齐，各种垃圾币无序超发，助长了歪风邪气。这是币圈衰败的征兆之一。这股歪风邪气会凶狠的收割投资者，让投资者认清真相及时止损离场。其次垃圾币超发后，usdt不足以支撑币圈总市值，会出现跌多涨少的情况，没有赚钱效应了，会导致很多投资人离场。当虚拟货币超发到usdt都不能扭转币圈颓势的时候，usdt就失去了信用。那个时候usdt就会墙倒众人推，最后的疯狂挤兑将给与虚拟货币最沉重的一击。

珍爱生命，远离虚拟货币骗局吧。少做梦，多做实事才是正道。

如果你还想了解更多这方面的信息，记得收藏关注本站。