

火币交易所安全吗？火币网安全稳定运营数字资产交易所四年多，管理资产超过10亿美元，服务百万用户，专业的分布式架构和抗DDOS攻击系统，98%的数字资产存储多签名冷钱包。作为世界“火币”一直秉承为用户提供安全可靠服务的理念，以“唐”“不要作恶”作为团队“火币”的行为准则，并依靠专业的风险控制体系来保护您的账户和资产。如何加强火币网的账户安全？

- 1.在OTC买卖钱，如何保证自己的钱安全？如果你是买方，当你从卖方那里买了钱，卖方的钱会被平台冻结，卖家的钱将会在你付款给卖家后发放给你。如果卖家在你付款后没有把钱发放给你，你可以提出投诉。火币OTC作为第三方，将参与处理纠纷。你必须是一个商人才能发布广告。商家分为认证商家和超级商家，超级商家需要通过比认证商家更严格的认证。由于商家接受非实名支付，他人的支付账户被冻结，平台将调查问题资金来源，并有权直接冻结商家平台账户，取消商家认证资格。在一般交易区购买需要实名认证。
- 2.在火币Pro交易如何保证自己的资产安全？2018年1月，火币推出投资者保护基金。每季度将20%的利润用于在流通市场回购HT，回购的HT全部提供柴火投资者保障基金，用于平台突发风险时提前赔付柴火用户，保障投资者权益。2018年2月，火币全球专业站正式推出另一项用户资金保障机制——“安全储备机制”：

1. 火币安全储备总额为20000BTC，为平台的自有资产，存储在独立的地址，专门用于应对可能出现的极端突发安全事故；
- 2.对于非用户原因造成的任何用户资产损失，自有，火币全球专业站会从安全备用金中提取资金提前全额支付给用户。

如何加强账号的安全性？最好设置复杂且唯一的密码，长度至少为8个字符。建议密码包含大小写字母、数字或特殊符号，没有明显的规律性。最好不要包括你的姓名、邮箱、生日、手机等容易被别人获取的信息。比如李鸿，123456，qwerty，huobi123，abc123都是不推荐的密码，比如W@ng32#4ef

。

或者iehie8#We12或者Uith!3Le4。Oa

都是推荐的密码格式。您还可以通过定期更改密码(每三个月一次)来增强账户的安全性。最好每次都彻底改密码。建议您使用密码管理器1

密码或LastPass来记录和管理密码。另外，千万不要把自己的密码透露给别人，柴火的员工也绝对不会问你要密码。双因素身份验证建议您绑定GoogleAuthenticator。GoogleAuthenticator，即Google

Authenticator，是Google推出的一款动态密码工具。需要用手机扫描FirePro提供的条形码或者输入密钥。添加完成后，每十秒钟就会在认证器上生成一个有效的6位验证码。绑定成功后，每次登录FirePro都需要输入Googleauthenticator上显

示的6位验证码。关注钓鱼，关注亲的邮件。尽量不要点击邮件中的链接或附件。登录账号前确保链接是火币Pro的官网。火币Pro绝不会要求你输入密码、短信或邮件验证码和谷歌验证码。如何防范网络钓鱼攻击1。什么是钓鱼攻击？，是通过冒充他人获取用户名、密码、信息、身份证等个人敏感信息的犯罪诈骗过程。这些通信都自称是()官员、运营商、客服或网管，目的是为了诱骗受害者相信。。2.网络钓鱼的传播方式是通过病毒罪犯克隆一个一模一样的站，然后使用一些电脑病毒程序和垃圾软件向客户发送虚假的网站地址；电脑，或者放在搜索网站上诱骗用户登录。，以窃取用户账号密码、交易信息或资料等。不法分子通过短信的方式，利用短信的优势，冒充消防战士向用户发送诈骗短信，声称用户中奖或账号被他人盗用，要求用户尽快登录短信中指定的站点进行身份验证。。该网站是不法分子为获取用户信息而建立的虚假网站。如果用户登录并操作网站，用户；的账号、密码等信息会被非法获取。建一个假网站。犯罪分子首先建立一个假网站。比如www.hbg.br.com，他接待了用户；的举报，然后在QQ、微信等社交平台网站发布虚假活动信息，往往给用户画了一个饼。当用户登录假冒网站时，账户密码信息会被不法分子获知。。通过假冒官方邮箱的非法组件发送欺诈性电子邮件，诱使用户登录虚假网站。这些邮件大多需要收件人点击邮件上的链接地址，登录类似火币的界面。com因为各种原因，比如中奖，升级系统。一旦用户在这个指定的登录世界中输入账号密码等信息，这些信息就会被窃取。通过社区转发钓鱼网站链接，引诱用户登录假冒网站。3.使用更安全的chrome浏览器来防止网络钓鱼。，并升级至最新版本；注：Chrome是谷歌的产品，安全性是公认的高。最新版本升级是因为低版本会有很多漏洞。例如，"恶意代码网络钓鱼攻击"链接：https://blog.csdn.net/qq_27446553/article/details/70255763不要随意安装浏览器插件；注意：浏览器插件有非常强的权限。，有被盗的风险，比如"chrome"。唐；不要打开不可信的链接地址，也不要；不要在未知的站上输入火币的账号密码和个人信息。，以免被钓鱼站或网络窃取；安装杀毒软件，定期给电脑和电脑消毒；按时更新系统补丁；请不要将官方发送的验证码给别人；当您登录或进行交易时，请确认该域名是否属于火币网。对于未知域名，请咨询客服。反病毒和特洛伊木马指南检查计算机是否感染了病毒或特洛伊木马的步骤：1.在浏览器的隐形窗口模式下登录FirePro，准备检查充值/提现地址是否正确。。如下图：Chrome(CtrlShiftN)打开一个新的隐身窗口。



2. 在记事本中记录一个正确的取现地址，然后试着将该地址粘贴到地址栏中，检查地址栏中显示的地址是否与记事本上的地址相同。3. 下载火币APP，对比APP的充值/提现地址与Web端的地址是否一致。。如果检查后发现地址不同，说明你的电脑很可能感染了病毒或者木马。有以下建议：安装杀毒软件，定期查杀木马病毒；更新系统补丁；不要点击来源不明的文件；绑定Google身份验证器，具体方法[点击这里](#)；请使用1密码等专业密码管理工具；如遇账户异常，请及时反馈给客服，客服会针对您的问题给出相应的解决方案；尽可能使用Chrome(谷歌浏览器)，并升级到最高版本；卸载插件或未知第三方软件；极端情况下，可能需要格式化硬盘，重装操作系统；寻求计算机安全专家的支持服务。