我国电子商务发展的安全环境及现状电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/545/2021_2022__E6_88_91_E5_9B_BD_E7_94_B5_E5_c40_545970.htm 网上购物大军达到2000万人，在全体互联网网民中，有过购物经历的网民占近20%的比例。根据国家信息化办公室公布的数据，目前仍有60%的中小企业的信息化程度处于初级阶段。 因此，电子商务是互联网应用发展的必然趋势，也是国际金融贸易中越来越重要的经营模式，以后它还会逐渐地成为我们经济生活中一个重要部分。但同时我们也看到，我国的电子商务还处于了发展的初级阶段还有很长的路要走，从而安全是保证电子商务健康有序发展的关键因素。 根据调查显示，目前电子商务安全主要存在的问题是： (1)计算机网络安全 (2)商品的品质 (3)商家的诚信 (4)货款的支付 (5)商品的递送 (6)买卖纠纷处理 (7)网站售后服务 以上问题可以归结为两大部分：计算机网络安全和商务交易安全。 计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。考|试/大电子商务的一个重要技术特征是利用IT技术来传输和处理商业信息。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起。没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。只有解决好以上的矛盾，电子商务才能保证又快又好的发展。 2网络安全技术策略 电子商务的安全问题，可以归结两大类问题：一是支付安全，二是认证安全。 2.1支付安全 由于网络天生的不安全性，特别是其网上支付领域有着各种各样的交易风险。但无论是何种风险，其根本原因都是由于登

录密码或支付密码泄露造成的。 2.1.1密码管理问题 大部分公司和个人受到网络攻击的主要原因是密码政策管理不善。大多数用户使用的密码都是字典中可查到的普通单词姓名或者其他简单的密码。有86%的用户在所有网站上使用的都是同一个密码或者有限的几个密码。许多攻击者还会直接使用软件强力破解一些安全性弱的密码。 因此，因此建议用户使用复杂的密码，降低被病毒破译密码的可能性，提高计算机系统的安全性。需要注意：考|试/大一是密码不要设置为姓名、普通单词一、电话号码、生日等简单密码.二是结合字母、数字、大小写共组密码.三是密码位数应尽量大于9位。 2.1.2网络病毒、木马问题 现今流行的很多木马病毒都是专门用于窃取网上银行密码而编制的。木马会监视IE浏览器正在访问的网页，如果发现用户正在登录个人银行，直接进行键盘记录输入的帐号、密码，或者弹出伪造的登录对话框，诱骗用户输入登录密码和支付密码.然后通过邮件将窃取的信息发送出去。 因此，需要做好自身电脑的日常安全维护，注意以下几点: 一是经常给电脑系统升级，二是安装杀毒软件、防火墙，经常升级和杀毒，三在平时上网是尽量不上一些小型网站，选大型网站，知名度比较高的网站，避免网站挂有病毒、木马造成中毒，四尽量不要在公共电脑上使用自己的有关资金的帐户和密码，五有条件的情况下，在初装系统后确认电脑安全的后，给自己的电脑做上备份，在使用资金帐户前做一次系统恢复。 2.1.3钓鱼平台“ 网络钓鱼 ”攻击者利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，如将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌。受骗者往往会泄露自己的财务数据，如信用卡号、账户号和口

令等。 因此，在登录支付资金时，应注意：一是确认该网是否是官方网站，二是仔细核对该网的域名是否正确，注意小写“1”与“L”、“0”与“O”等情况，三保证良好的上网习惯，收藏常用的网址，减少网上链接。 2.1.4硬件数字认证 在电子商务体系构建的过渡时期，道高一尺，魔高一丈。各类病毒层出不穷，考|试/大木马也在天天更新，今天这种技术安全，明天就不一定安全。 因此，数字证书的引入是在线支付安全问题的最终解决方案之一。网上支付不安全，选择网下加以弥补。 以工商银行2003年推出并获得国家专利的客户证书USBkey(U盾)为例。从技术角度看.u盾是用于网上银行电子签名和数字认证的工具，它内置微型智能卡处理器，采用1024位非对称密钥算法对数据进行加密、解密和数字签名.确保网上交易的保密性、真实性、完整性和不可否认性。它顺利地解决了当前网银密码泄漏的问题。有了硬件数字证书的应用，即使你的密码泄漏了。没有证书，黑客还是不能够使用你的帐户。 动态电子密码的应用也可以确保电子银行帐号的安全。现行的有两种方式，一种是在使用时查看当前的动态电子密码。另一种是临时通过绑定手机、密宝等通信工具，向帐户所在银行申请临时密码。由于具有较强的时效性，从而保障帐户资金的安全。还有其它消极的防护措施。如某些网上银行交易金额限制，单次为300元，每日限额为3000元。考|试/大主要是为了降低电子支付交易风险.但在一定程度上会给大额交易带来不便。这种措施其实治标不治本。 2.2 认证安全 电子商务为了保证网络上传递信息的安全，通常采用加密的方法。但这是不够的，如何确定交易双方的身份，如何获得通讯对方的公钥并且相信此公钥是由某个身份确定

的人拥有的，解决方法就是找一个大家共同信任的第三方，即认证中心(CertificateAuthorITy，CA)颁发电子证书。用户之间利用证书来保证安全性和双方身份的合法性，只有确定身份后，交易的纠纷，才得到有效的裁决。 总之，电子商务的安全是个非常复杂的问题，它的保障机制必须是有机的，多层次的，需要有企业管理方面，技术支持方面的协调来实现考|试/大。它是一个系统有机的整体，不仅需要计算机网络安全的保证，也需要商务交易安全上的保障，更需要管理上的进步，才能确保电子商务的安全。同时我国在电子商务技术性较为落后，必须加强具有自主产权的信息安全产品的研究，注意加强信息安全人才的培养，多方共同努力建立科学的电子商务安全机制，才能为我国的电子商务又快又好的发展保驾护行。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com