 电子商务由于方便、快捷开展得如火如荼，但是作为电子商务重要支付形式的电子支付却面临着各种安全问题，而且，这种问题日益凸现，所以作为用户需要 2003年1月中国互联网信息中心(CNNIC)发布的《中国互联网络发展状况分析报告》显示：2002年网上购物人数比2001年增长将近一倍，已经接近2000万。随着网上交易的发展，电子支付开始逐渐被人们认可，但是“ 云网事件 ”的发生却不得不使我们关注电子支付的安全性。据AC尼尔森公司在2003年3月～4月做的一个调查表明，目前安全性是网上购物者用信用卡支付的主要顾虑。安全问题已成为电子支付发展面临的重要挑战。 真假“ 云网 ” 云网（www.cncard.com）是一家网上交易公司，顾客可以通过在线支付的形式购买上网卡、IP卡之类的商品，在业内已有了一定的知名度。可是最近经常有供货商向他们质询:“ 我们根本没有那种上网卡，你们怎么打着我们公司的名义卖。 ”云网公司对此一头雾水，因为他们卖的商品都是由厂家供应的。后来，经过调查，他们发现，原来最近一些论坛上出现了很多推荐另一个“ 云网 ”（www.kncard.com.cn）的帖子。这个“ 云网 ”的界面与真云网非常相似，而且也从事与真云网类似的网上交易，但实际上，它所出售的商品都是不存在的。 在这个“ 云网 ”网站，虽然会出现假的银行支付界面（没有经银行授权），要求用户输入银行卡号和密码，但即使输入正确银行卡号和密码后，系统却总提示交易失败，而用户

的银行卡号和密码却可能已被泄露给这个网站，并有可能被这个网站利用来从用户的银行账户上提取现金或消费。 对此，云网公司很是气愤，“ 该网站根本不是为了进行电子交易，它的主要目的是为了骗取用户的卡号和密码，并用用户的卡号和密码进行消费，这种行为属于诈骗，使我们的商誉受到了严重影响。 ”云网公司的员工说。 当记者试图联系另一个“ 云网 ”，却发现，这个网站的很多信息都是假的。虽然假云网页面上有工商局的红盾标志，但记者通过北京市工商管理局的网站查询，发现该网址没有备案。假云网页面上还有ICP登记号，记者又到北京市通信管理局的网站进行查询，发现确实有这个登记号，但那是一家叫“ 歌曲大本营 ”的网站，网址和业务都不一样。 是否主机托管机构会对网站的内容负责呢？就此，记者询问了一家做主机托管的公司，他们说：一般只要被托管的公司提供公司法人的身份证复印件，就可以提供主机空间和域名，对客户利用网站从事的何种业务并没有限制，其网站的内容和业务应该由公安机关管理。涉及这个事件的银行已经报案，公安机构也已经受理，并展开调查。 对于“ 云网事件 ”，中国人民大学法学院郭禾教授认为：它涉及到某些法律规定，首先，模仿注册商标和界面，这种行为侵犯了知识产权；其次，云网是从事电子商务的网站，假云网利用其名称从事相同的业务，属于不正当竞争；最后，利用网站骗取用户的账号信息属于窃取他人隐私，另外，如果那个网站的人员利用骗取的用户卡号和密码进行转账和消费的话，其行为将构成侵犯个人的财产权，应该负刑事责任。 电子支付存在风险 虽然人们在电子支付的技术实现上采取了很多安全措施，但是由于电子交易包括很多环节

，还是存在着一定的安全风险。 对外经济贸易大学信息学院院长兼电子商务研究所所长陈进教授介绍说：现在银行数据系统的安全措施很严，要想攻破它是不太可能的，而且电子交易在传输用户账号信息时都要求强加密的，即使截获也很难破译。但电子支付还是面临着一些威胁。“ 比如有些商家为了方便，会存储用户的数据进行存储，如果商家数据库被攻破，将导致用户账号信息泄露。现在已经出现了这样的案例，今年10月，北京市首例操纵期货价格案在西城法院开庭，一家期货经纪有限公司的客户代表在互联网上发布了自己编制的程序“ 期货精灵 ”，诱使他人下载安装，以此方法截获十多个上网交易客户的资金账号和密码，导致客户损失。如何避免危险 从用户角度，安全意识的增强很重要。当你在网络上进行电子交易时，一定注意以下几点：一，确保网站网址的正确，网站的知名度较高。中国的电子交易网站一般都是链接到银行进行交易，不要在不明来历的商户网站直接输入账号信息。二，查看网站是否有ICP号，ICP号是否正确，国家规定经营性网站必须在当地的通信管理局登记，北京网站的登记信息可在北京市通信管理局网站（http://www.bca.gov.cn/）上查到。三，查看网站是否有工商局的标志，标志是否登记。对于北京的经营性网站，必须到工商局办理网站备案登记，该标志是一个红色的盾牌，点击网站界面上的红盾，会自动链接到北京市工商局的网站登记网站（http://www.hd315.gov.cn/）上，显示出该网站的登记信息，可以查看该信息与网站实际情况是否一致。四，正规电子交易网站在传输用户账号信息时都要加密，此时地址是以“ https ”而不是通常的“ http ”开头的。加密传输时，浏览器

下面会出现一个小锁，点击小锁会显示证书，只能相信权威机构颁发的证书。不要相信不明来历的证书，目前我国电子交易常用的证书包括由中国金融认证中心（CFCA）颁发的证书和各个银行自己颁发的证书。 从技术角度，我们还应增强加密的强度，提高盗用账号的难度，例如Visa信用卡最近为了增进其信用卡在电子交易中的安全性，推出了 ” Verify by Visa “ 的服务，增加了一个密码，交易时用户除了输入卡号外，还要输入密码。 从社会角度，良好的信用机制可以减少电子支付的风险。“ 其实中国的电子支付系统比外国要安全，中国的支付必须都连到银行的系统进行，而在外国，支付可以在商家的网站进行，而且他们的信用卡只有一个卡号，没有密码，但他们能保证一定程度的安全是因为他们的信用机制较为完善。 ” 陈进说。“ 对于像假云网这样的诈骗例子，银行和网站应及时向社会公布，避免用户遭受更大的损失 ”。 从法律的角度，完善的法律是保证电子支付安全的前提。郭禾教授认为，现在关于电子商务的法律从总的原则上已经足够，但在具体细节和操作上还有待完善，如现在合同法上已承认数字签名的法律效力，但具备什么样技术条件的数字签名才是有效的还需确定，还有网站泄露用户的账号信息应当承担何种程度的责任。同时，郭禾认为，政府职能部门今后应加大对电子商务网站的管理，避免通过电子交易进行诈骗的现象发生。 很多时候，电子支付的危险并不是来自电子支付本身，而是由于人们缺乏警惕性。如果我们能提高警惕性，电子支付还是足够安全的。虽然电子支付现在还存在一些风险，但电子商务和电子支付能给我们带来极大的方便，因此我们不能因噎废食，而应逐渐完善它，使我们最终可

以放心地享受电子支付带给我们的便利。 我国现行电子支付的安全机制 电子支付系统的安全要求包括：保密性、认证、数据完整性、交互操作性等。目前，国内外使用的保障电子商务支付系统安全的协议包括：SSL（Secure Socket Layer）、SET（Secure Electronic Transaction）等协议标准。国内的电子支付系统共有三种安全实现方式：SSL、SET和Non－SET。SET协议是由Visa和MasterCard推出的，它可以对每个参与者进行多点认证，对交易的每个环节也进行认证，拥有较高的安全性，中国银行就是采用这种协议。但由于它的复杂，在国内开展得不是很普遍。 SSL是一种点对点的协议，可以保证双方通信时数据的完整性和保密性，目前在中国可以支持128位的加密，招商银行、工商银行就是采用了这种方式。由于它被IE、NESCAPE等浏览器所内置，实现起来非常方便，国内的电子交易很多都采用这种协议。 中国金融认证中心还推出了另外一种系统Non-SET，它是基于PKI的，除了加密功能外，还有数字签名功能、证书管理和在线CRL（证书废止列表）查询等功能。 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