

06年电子指导新型安全威胁叫板电子商务 PDF转换可能丢失
图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/62/2021_2022_06_E5_B9_B4_E7_94_B5_E5_AD_c40_62060.htm 电子商务的安全威胁已经出现许多新特点，致使用户在稀里糊涂中上当受骗，懊悔不已。魔高一尺，道是否可以高出一丈？目前，假冒网站、邮件欺骗、木马病毒已经成为新形势下电子商务面临的最重要的现实安全威胁；2005年我国网络用户被骗金额近1亿元人民币，今年“五一”黄金周期间，银行卡相关病毒数和网络钓鱼网站数量进一步急速上升。以上事实和最近大量网络诈骗案的接连发生，提出了一系列值得我们思索和警示的问题。因此，把握电子商务安全预警、安全防范的新情况、新特点和新技术，对于加快电子商务的发展具有重要意义。网络钓鱼已经成为当前电子商务的重要风险 网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性邮件，意图引诱收信人给出敏感信息如用户名、口令、帐号ID、ATM PIN 码或信用卡详细信息的一种攻击方式。最典型的网络钓鱼攻击是将收信人引诱到一个通过精心设计与目标网站非常相似的钓鱼网站上，获取个人敏感信息，而这些个人的信息被泄露以后，网络钓鱼攻击者就可以假冒受害者进行欺诈性金融交易，从而获得经济利益，致使受害者经常遭受显著的经济损失。网络钓鱼的诱骗手段很多，主要有：通过网络发布虚假、低价的产品的三种攻击方式信息作为诱饵，诱使购物心切的人们上当受骗；利用一些网络技术四处传播木马病毒，窃取电脑机密；窃取银行卡的帐号、密码等重要信息，让人们受到经济上的损失；搭建虚假电子商务平台建立假冒网站等实

施欺诈行为，从而达到“网络钓鱼”的目的。以上是三种网络诈骗的重要手法，随着钓鱼式攻击技术的发展，新的攻击方式不断出现和扩展，其攻击手段越来越狡猾，调查表明今年以来有关部门就监测到上百起钓鱼式攻击方式。截至2005年5月的一年中，有7300万美国互联网用户收到过平均50多封/人的网络钓鱼邮件，比2004年前6个月增加了4倍。也就是说，每五个美国人中就有一个成为那些网络钓鱼者的攻击目标。因此，网络钓鱼去年给美国造成了近10亿美元的经济损失。根据国家计算机网络应急技术处理协调中心的统计，目前中国的网络钓鱼网站占全球钓鱼网站的13%，名列全球第二位。去年一年，公安部侦破网络诈骗案件1350起，自2004年7月以来，该类欺诈报告更是以月均26%的速度递增。仅2004年“国家计算机网络应急技术处理协调中心”就接到了金融网站和电子商务网站的仿冒报告223起。2005年4月以来，国内著名电子商务网站“淘宝网”连续发生数起卖家网上帐户被盗事件。此类偷窃行为给用户造成严重的经济损失，对中国电子商务的危害也最大。对于当前大量发生在各网站的网民被骗案件，相当多的电子商务平台以“我只提供平台，风险与我无关”自居。因此，对入住的交易主体缺少必要的审查和管理，缺少网络化的交易监管，缺少对交易风险的提示和告诫，更缺少对交易风险的必要的赔付保障，以至网络骗子横行，网络钓鱼案件频发。网络钓鱼诈骗的主要危害

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