2006年电子技术讨论如何安全使用网上银行 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/64/2021_2022_2006_E5_B9_B4_E7_94_B5_c40_64672.htm 7月5日，国家计算机病毒应急处理中心提醒，监测发现一个恶意诱骗用户暴露银行个人银行账号密码的网银木马Ｔｒｏｊ Ｓｐｙ＿Ｂａｎｋｅｒ．ＹＹ。该木马会监视ＩＥ浏览器正在访问的网页，如果发现用户正在登录某银行网站，就会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，通过邮件将窃取的信息发送出去。同时，一种名为"网络钓鱼"的金融诈骗行为也正在国内兴起。 不少市民会有这样的疑问：我们网上银行的资金安全吗？怎样才能让网上银行万无一失？ "网络钓鱼" 伪造银行网站 "网络钓鱼"，是指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。诈骗者通常会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，调查显示，在所有接触诈骗信息的用户中，高达５％的人都会对这些骗局做出响应。近期，"网络钓鱼"越来越猖獗。 去年以来，国内银行网站屡屡出现"赝品"，这些冒牌网站的共同点是网址及页面与真网站相似。如已发现的假冒中国银行的域名ｗｗｗ．ｂａｎｋ－ｏｆｆ－ｃｈｉｎａ．ｃｏｍ，与该银行网站ｗｗｗ．ｂａｎｋ－ｏｆ－ｃｈｉｎａ．ｃｏｍ只多一个英文字母ｆ；假冒中国工商银行域名ｗｗｗ．１ｃｂｃ．ｃｏｍ．ｃｎ，与中国工商银行网站ｗｗｗ．ｉｃｂｃ．ｃｏｍ．ｃｎ，也只是"１"和"ｉ"一字之差；而假冒中国农业银行域名是ｗｗｗ．９６５５５５．ｃｏｍ，与中国农业银行网站ｗｗｗ．９５５９９．ｃｏｍ也较为相近。市民一旦输

入了账号及密码，用户的资料就会落入网贼的手中。 同时，一些钓鱼网站采取用ｅ－ｍａｉｌ的形式，诱使上网者点击相关链接，利用某些漏洞自动下载木马程序，盗取客户的账号、密码。 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