 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。 电子证书确保安全 据了解，针对不同需要，银行往往为客户提供了不同的安全手段以供选择。一种是凭借账号和密码就可以进入并使用网上银行，另一种是使用网上银行电子证书。工行电子银行部有关专家告诉记者，用密码和账号登录使用网上银行这种方式比较简单，但安全性也相对较差。一旦网络犯罪分子通过假网站、木马程序、假电子邮件等方式骗取到了用户的账户名和密码等敏感信息，就能以客户的名义登录网上银行，达到窃取客户资金的目的。 专家提醒，客户申请使用网上银行的，最好能同时申请电子证书。电子证书是一种外形类似U盘，基于智能芯片加密技术的数字证书，是目前安全级别最高的一种网银安全措施。申请后，所有涉及资金对外转移的网银操作，都必须使用电子证书才能完成。因此，客户只要保证电子证书、电子证书密码、账号、登录密码和支付密码这些所有的安全措施不被同一个人窃取，任何病毒、木马、黑客、假网站的网络诈骗方式都无法窃取客户资金。 个人安全防范意识最重要 工行专家介绍，从近年的几起网银案件来看，不法分子多是利用一些客户在使用过程中缺乏必要的安全保护意识得逞的。在近期破获的一起网银案件中，犯罪分子攻破了一家小网站并窃取了该网站的客户信息（包括用户名、密码、银行卡号等），而该网站部分客户在普通网站上的密码和网上银行密码设置相同，给了犯罪分子以可乘之机。又如，一用户在一家非法的游戏装备交易网站购物时，轻易地在该网站输入了网银的

卡号、密码，当时该网站提示密码错误，客户也未作什么补救措施，几天后才发现账户资金被盗。从上述案件看，客户的安全意识不强，没有保护好自己的账号、密码等敏感信息，是导致目前绝大多数网银资金被盗案件发生的根本原因。对此，工行专家建议用户，如果暂时没有申请电子银行客户证书的，首先需要重新设置自己的网银密码。客户的网银密码最好不要与电子邮箱密码或其他网站的注册密码相同，用户设置的支付密码也不要与登录密码相同，以充分发挥工行网银双重密码保护的作用。其次，为了保障网银账户安全，客户不要向任何未经安全确认的网站和个人泄露自己的银行卡号、密码、身份证号码等重要信息，避免被不法分子利用。除正常的登录、交易外，银行不会以任何理由通过网络向客户索要卡号、密码等重要信息。第三，不要轻易下载或点击一些来历不明的软件或邮件，最好不要在公共场所（如网吧、公共图书馆等）使用网上银行。此外，客户最好是能安装正版杀毒软件和防火墙，并及时进行更新，阻击网络病毒入侵。