

网银时代如何修好防盗课ATM安全取款七绝招 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__E7_BD_91_E9_93_B6_E6_97_B6_E4_c40_64663.htm 近日，国家计算机病毒应急处理中心提醒，一种新的恶意木马程序正在盗取个人网上银行账号和密码。虽然此类病毒信息发布已不是第一次，银行也早已有了相应的防范措施，但很多对网上银行了解不够深入的客户仍然会产生这样的疑问：我们网上银行的资金安全吗？面对越来越多的恶意木马程序、假网站、假邮件、假短信等网络诈骗，用户如何才能确保自己的账号、密码不被窃取？怎样才能让网上银行万无一失、安全无忧？带着这些问题，记者采访了中国工商银行电子银行部有关专家，请他为广大网银用户释疑解惑。工行专家介绍，正如人体病毒和人体共生一样，网络病毒的存在已经是网络世界中的一种常见现象，专门针对网上银行的病毒也屡见不鲜，几乎每隔一段时间有关部门或杀毒软件公司就会发布一些新的网络病毒样本信息。其实，这些病毒样本能不能传播是一回事，即使广泛传播，以目前的网上银行安全技术而言，也并不可怕。工行专家指出，像工行这样曾多次在国际上获得网银大奖认可的银行来说，工行网上银行的安全性能已经达到国际先进水平，完全能够很好地防范网络病毒的侵入。目前，工行网上银行已经采取了防病毒安全控件、余额变动提醒、预留信息验证等一系列安全措施来保障网银安全，但是，一些客户在使用过程中缺乏必要的安全保护意识，造成了损失。据了解，针对不同需要，银行往往为客户提供不同的安全手段以供选择。一种是凭借账号（或别名一种为自己的网上银

行所取的个性化名字)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。工行专家告诉记者,用密码和账号登陆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陆网上银行,达到窃取客户资金的目的。从近年的几起网银案件来看,不法分子多是利用这样的犯罪手段得逞的。例如,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,几天后客户才发现账户资金被盗。还有一家公司的**管,将自己的银行卡和密码交给下属到银行办理业务,该下属利用银行卡和密码申请了网上银行,随后辞职并通过网上银行转移该高管资金。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,如果暂时没有申请工行电子银行客户证书U盾的,首先需要重新设置自己的网银密码。目前,工行网银系统已经强制要求客户密码必须是6位以上的数字加字母形式,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漏自己的银行卡号、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，工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。如果客户对所进行的网上银行交易有任何疑问，要马上拨打工行24小时客户服务热线95588进行咨询。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。专家还提醒，客户申请使用工行网上银行的，最好能同时申请使用工行U盾。U盾是一种外形类似U盘，基于智能芯片加密技术的数字证书。可以说，U盾是网上银行的物理“身份证”和“安全钥匙”，是目前安全级别最高的一种网银安全措施。客户申请了U盾后，所有涉及资金对外转移的网银操作，都必须使用U盾才能完成。因此，客户只要保证U盾、U盾密码、账号（别名）、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，资金损失的可能性几乎为零。目前U盾的价格已不足80元，客户只需凭网银注册卡、身份证件到工行网点申请，即可获得网上银行最高级别的安全保障。（记者卫容之）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