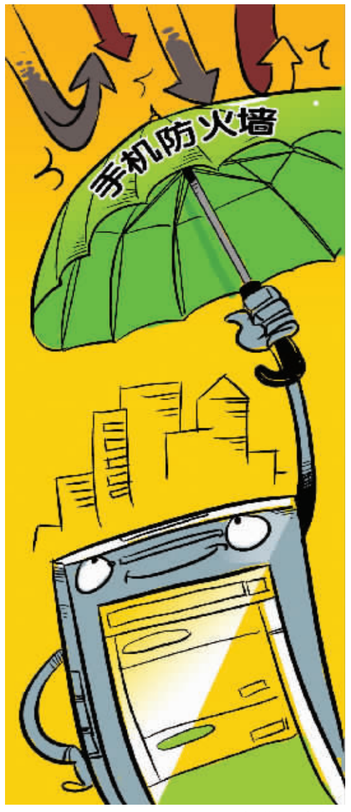

本版漫画 俞晓翔

电子银行、手机银行在给客户带来便捷的同时，也隐含着相应的风险。此时，需要使用者提高防范意识，识破网络诈骗、手机诈骗的常用手段。

不要贪图便宜、刺激——

安全的第一道防火墙在自己

电子银行防骗——记清官网和客服电话

南京市公安部门相关人士告诉记者，近几年，手机银行和电子银行的诈骗案例数目不断升高，诈骗花样层出不穷，受害人在不经意之间便损失惨重。

其中，网络诈骗主要是通过冒充官网或客服电话向受害人索要账号和密码。在此提醒市民，首先要记清楚官方网站的网址或客服电话，不要相信任何来自非官方网站或非客服电话发来的信息。登录网站时不要通过链接或是他人的指示登录网址。

“这类犯罪中，犯罪分子向受害者发出短信，称其银行卡在某地商场、酒店等消费场所刷卡消费××元，或称已从账户中扣除银行卡费×××元，如有疑问，可致电××号码查询。一旦受害人回电，犯罪分子就会冒充银行客服人员或公安机关金融犯罪调查科人员，谎称该卡可能被复制，想方设法让客户按其指示操作，实际上，完成操作后，受害人的资金就被转到犯罪分子指定的账户了。”

小心钓鱼链接网站

最近兴起另一种通过电子银行的诈骗方式，即犯罪分子通过钓鱼链接、交易失败提示、客服聊天等组合，诱骗受害者进行“网银授权支付”，授权骗子用另一个网银账户对自己账户进行资金操作，损失惨重。

和传统的诈骗方式不同的是，受害者的主要损失并不是因为在虚假的购物网站上进行购物，而是因为他们在“交易失败”后向店家进行申诉时，被骗子的客服QQ诱骗进入了一个称为“授权××银行账户支付协议签约”的页面，并被告知这是内部号码或内部规则，可以放心操作。

当受害者按照骗子客服的指示完成操作后，实际上就已经授权了骗子使用另外一个网银账户对自己的网银进行转账或支付操作。在完成授权后的几分钟内，受害者网银账户中的资金就会被全部转出。

动态密码勿予他人

一般针对网银用户，银行都会设置有U盾加密，或是动态密码保护，或是手机验证码这三类方式进行交易操作保护。

针对这三种保护方式，犯罪分子一般会采取相应的诈骗手段，若是受害人使用U盾进行网银保护，犯罪分子会通过给计算机植入病毒，对受害人的电脑进行远程操控，再由犯罪分子操作受害人的电脑，将受害人的银行卡内的资金通过远程操控转移走。

如果受害人使用的是动态密码保护，犯罪分子会假冒销售客服或者物流工作人员等虚假身份，提示受害人交易出现问题，要对受害人的交易进行帮助，并告知这些服务都是免费的，或者还有一定的补偿，要受害人告知动态账号密码，受害人一般认为自己的银行卡号未被掌握，告知动态密码也无所谓，所以就将动态密码告知犯罪分子，其实在前期交易环节犯罪分子已经掌握了受害人的银行账号，一旦得到受害人的动态密码，犯罪分子会迅速将受害人卡上的资金进行转移。

第三种手机短信验证码的诈骗方式基本和动态密码相似。

手机银行防骗——避免越狱，安全软件很重要

随着智能手机的普及，曾令电脑操作系统闻风色变的木马病毒也随之转移。360安全中心最新发布的2013年第一季度中国手机安全报告显示，今年一季度新增手机木马样本104020款，感染数达2800万人次。

南京市公安人员提醒，目前虽然手机诈骗犯罪的数目远远小于网络诈骗，但手机端的安全防控其实不如PC端成熟，要尽量让自己的手机远离木马。应该注意的是，手机购物时，如果卖家提出用官方指定之外的聊天工具沟通，无论怎么诱惑都别同意；此外，应该下载官方应用的手机购物、支付软件，在安装应用过程中，一定要仔细阅读应用授权说明，对于索要太多权限的软件，建议拒绝安装；第三是尽可能避免对手机root、刷机、越狱。如果手机已被木马入侵，建议在备份重要文件后，将手机恢复出厂设置。

而360手机安全专家则提醒智能手机用户，一定要安装手机安全软件，及时升级并查杀内置木马病毒。如果用户要安装应用软件，应该在正规手机商城下载应用；同时，不随意扫二维码，建议用带有安全检测功能的手机安全软件扫描二维码。

文/现代快报记者 杨连双

安全卫士

中行网银安全机制全解析

三道防线

●第一道防线

用户名（6-20位数字和英文字母）、静态密码(8-20位数字和英文字母）和图形验证码（4位数字和英文字母，系统随机生成），通过保障客户登录安全。中行网银在登录环节设置了保护机制，多次密码输入错误即锁定用户登录，以防他人恶意破解客户密码。

●第二道防线

在进行向他人转账、支付、缴费、还款等重要交易时，需输入安全认证工具密码。中行网银采取中银E盾和中银E令两种高端安全认证工具。在进行上述交易时，中银E令用户需输入动态口令、中银E盾用户需输入静态密码，对交易逐笔进行认证，保障交易安全。

●第三道防线

中行网银将通过手机交易码短信提示中银E令用户关键的交易信息，客户确认是自己发起的真实交易后，输入手机交易码方可完成交易。中行网银通过中银E盾的液晶显示屏，提示中银E盾用户关键的交易信息，客户确认后按下“OK”键方可完成交易，否则可取消交易。

九重安全

●安全控件

主要用于防范恶意程序的攻击，如木马程序等，它是通过切断键盘操作与木马病毒之间的通道，来更好地保护网上银行用户的信息安全。

●中银E信

中国银行向网银客户提供短信提醒服务—“中银E信”，以方便您随时了解网银变动情况，使网上交易既轻松又安全。

●预留信息

预留信息是提高您对假网站辨别能力的一种简单有效的方法。在每次登录时，该信息将显示在欢迎页面上，如该网站未能正确显示您预留的欢迎信息，说明该网站不是中行网站。

●登录记录

您登录后，网上银行欢迎页面将显示上次“登录记录”，便于您核对实际登录情况，如发现异常可及时采取措施。

●登录锁定

为避免他人恶意试取您的登录信息，同一用户一天登录验证连续5次无效，网银即暂时冻结该客户登录，次日零点自动解冻；用户名、密码连续累计15次校验未通过或动态口令连续累计15次错误，即锁定该客户登录，需要客户持有效身份证件到银行柜台解锁。

●信息屏蔽

网银中关联账户的账号/卡号部分信息被屏蔽，保证客户账户信息安全。

●限额控制

您可自行在网上银行中设置转账汇款等交易的每日累计金额，有效控制风险。

●会话超时

登录网上银行之后，如果较长时间没有进行任何操作，系统将提示“会话超时”并自动签退。如需继续使用，须重新登录。目前网上银行会话超时设置为15分钟。

●退出按钮

网上银行页面右上角设有“退出”按钮，每次使用网上银行后，点击“退出”按钮，再关闭浏览器结束使用，保证安全退出网上银行。