工行安徽省分行电子银行专题报道案例篇：

冒名注册电子银行、出售网银账户……网银欺诈层出不穷

你的“钱袋子”守住了吗？

近年来，在金融领域冒名注册电子银行、出售网银账户、成批可疑人员注册网银以及诱骗客户登录假网站、假支付链接等欺诈风险事件时有发生，特别是今年涉及工银密码器客户被外部欺诈而造成资金损失事件呈高发态势。记者日前走进工行安徽省分行营业部，采集了一些百姓日常生活中常见的欺诈案例，并邀请工行安徽省分行营业部电子银行中心专业人员对这些案列进行风险分析、给出防范意见，希望可以提升读者的安全防范意识、减少不必要的损失。

周学鸿 记者 邹传科

案列分析篇

案例1：

轻信诈骗电话，险被骗取巨款

省城某行客户2012年7月在工行一家支行办理了一张理财金卡，存入12万元定期一年，然后主动要求开立个人电子银行并领工银电子密码器；当天下午17:30左右，该客户来到该支行声称自己的钱不对，经查询，客户的119950元已通过网银转到他人卡，该支行立即让客户向公安机关报案：她是在当天中午接到自称北京公安局电话，通知她涉及到反洗钱要冻结她的社保卡，账户网银是对方进行操作的，她告诉了对方卡号、登录密码及电子密码器上的动态密码。

工行提示：中老年及女性客户属电子银行风险高发人群，他们往往防范意识淡薄，容易轻信电信诈骗，缺乏必要的自我安全保护意识。银行柜面经办人员在客户办理电子银行业务时都会进行风险、安全提示，发放《电子银行安全宣传折页》、签订《工银密码器领用须知》，希望广大客户能仔细阅读，掌握必要的安全防范措施，严防客户因被欺诈而损失资金。

案例2：

被聊天网站诱骗，损失巨额资金

客户张先生2012年4月在工行办理了银行卡，并开通了个人网上银行并领取工银电子密码器，据张先生反映：2013年2月17日在非本人操作的情况下被他人从网银转走了9.5万元（余额变动提醒短信通知），随即客户拨打了95588电话，要求进行核查，经确认该账户转出9.5万元后，在客服建议下，客户向公安部门报警。4月中旬该客户以“储蓄存款合同纠纷”案由向法院提起民事诉讼，6月法院做出一审判决：原告的诉讼请求没有事实和法律依据，判决驳回张先生的诉讼请求。7月客户不服一审判决，上诉至中级人民法院，9月3日中级法院终审判决：驳回诉讼请求，维持一审判决。

在此期间，工行积极配合公安机关对该案件进行侦破，5月将该案犯罪嫌疑人在湖南省娄底市抓获，后经审理，犯罪嫌疑人交代，当日张先生登录某互联网“裸聊”网站，犯罪嫌疑人要求张先生支付10元费用，随即发送给其一个假工行网银支付链接，在获取客户卡号、登录密码等信息后，再诱骗其操作电子密码器，获得支付9.5万元的动态密码，从而迅速盗取了张先生账户资金。

工行提示：工行电子银行对外交易，无论是何安全介质，都必须是经客户操作确认，此案例是客户安全防范意识不强，没有认真阅读《电子银行安全折页》和产品说明书中有关风险防范提示内容，轻信登录他人发送的假支付链接，不知晓输入密码器的交易要素信息规则（含随机数字或转入账号6位+交易金额），在操作时未发现其支付的实际金额为9.5万元，才造成自己巨额资金损失。

案例3：

收到诈骗短信，登录假冒网站被骗

近期，工行某支行接客户王某反映：该客户手机接收到关于要求客户进行工行电子密码器升级的短信（内容为：“尊敬的工行用户您好：您的电子密码器即将于今日过期，请尽快登录www.iecnce.com进行升级，给您带来不便敬请谅解！【工商银行】），然后打开链接短信提供的网站后登录并按照页面要求输入卡号、身份证号码、注册手机号码、登录密码和密码器动态密码升级成功后，发现客户账户资金5613元被窃取了。

工行提示：近期社会不法分子针对工行电子密码器客户实施诈骗活动异常猖獗，他们利用车载“伪基站”移动设备，成批、大量、不间断向手机用户发送工行电子密码器需要升级、积分兑换、支付核对等信息，此类诈骗短信发送的号码多为"106★★★95588"（甚至已改号为95588号码），落款为[工商银行]，但提供的假冒网站网址与工行网站不同（工行网址：icbc.com.cn），页面基本相同，具有很强的迷惑性和隐蔽性，极易造成我行密码器客户在不知情的状况下，如客户按照短信提示内容登录假网站操作，最后账户资金被盗转。

案例启示篇

练就“火眼金睛”专访坏人诈骗

从初期的假网站、木马病毒发展到现在利用“伪基站”假冒以"95588"群发密码器诈骗短信，因其成本低廉、发送量大，又有很强的谜惑性。目前不法分子把电子银行客户作为犯罪攻击的主要对象，给客户造成经济损失。而在周学鸿看来，客户限于自身的识别与防范能力有限，仅靠银行安全宣传也难以奏效，因此提高广大百姓的安全防范意识、完善银行防范措施相结合才能取得实效。

掌握安全防范知识很重要

在银行方面看来，上述典型案例分析说明，客户在注册电子银行业务后，重点关注的是如何使用电子银行功能，而没有了解、掌握电子银行业务的风险防范知识，更没有认真阅读《电子银行安全折页》和产品说明书中有关风险防范提示内容，同时缺乏必要的警惕性，从而给犯罪分子有可趁之机。因此，加强电子银行客户安全教育，认真履行风险提示义务，提高客户安全防范意识十分重要。

提高风险防范意识有必要

“对于大多数电子银行客户来说，首次使用电子银行产品，关注的是如何正确操作，不太注重或忽视了安全提示内容，认为只要银行卡和网银安全介质保管在自己身边，密码不告诉其他人就认为没有风险。”周学鸿分析，殊不知在方便进行网上支付和介质操作等环节上同样存在很大的风险，通过已发生的客户被诈骗案例说明，无一不是客户对网上银行、手机银行使用的安全风险防范意识不强，没有良好的使用电子银行产品习惯而造成。“特别是年龄偏大的客户，对电子银行产品安全知识掌握的较少，又比较轻信陌生电话、短信，从而成为犯罪分子攻击的主要对象。”

防骗有诀窍 工行来支招

1.不要在公共场所（如网吧、公共图书馆等）使用网上银行，因为您无法知道这些计算机是否装有恶意的监测程序。

2.切勿向别人透露您的用户名、密码或任何个人身份识别资料。

3.不要开启不明来历的电子邮件。

4. 不要点击来历不明的链接，不要扫描来历不明的二维码，不要随意下载安装软件。

5.在任何时候及情况下，不要将您的账号、密码告诉别人；不要相信任何通过电子邮件、短信、电话等方式索要卡号和密码的行为。若有任何怀疑，请立即致电95588与我们联系。

6.选择不容易猜测的密码（建议不要使用您的出生日期、电话号码、相同数字、连续数字和身份证号码中前几位或后几位等），以免被有心人士猜中。

7.不要随意向他人提供电子密码器生成的数字。

8.如有疑问，请及时拨打中国工商银行服务热线95588咨询。