建行蓝E卫士 时刻守护金融消费安全

中国建设银行 China Construction Bank 洛阳分行

对于每位客户来说，无论是网购支付还是日常金融消费，安全永远是首要前提。正是源于对安全守护的践行，建行移动金融得到众多用户的青睐。建行安全守护代言人——“建行蓝E卫士”也成为了家喻户晓的品牌。

“蓝E卫士”努力创造安全支付环境

2015年，建行专门打造了建行反欺诈卫士卡通形象“蓝E卫士”，并在微信、微博、网站等互联网渠道，以“蓝E卫士”为主题对信息泄露、伪基站等当前典型高发的风险进行多轮次宣传教育。同时在行内定期进行风险提示和预警，通过网点和短信等渠道开展客户安全教育和警示。通过一系列安全宣传活动，有效提升了客户风险防范意识和技能。

建行专门组建反钓鱼队伍，开启24小时不间断的钓鱼网站主动搜索排查机制，不断分析钓鱼网页规律，做到查防结合，积极应对多样化、域名种类复杂化的形势。建行自主创新开发的“一种反钓鱼监测系统和方法”获得国家知识产权局授予发明专利，通过提升钓鱼网站监测系统的智能化水平，加大对高危、重点钓鱼网站侦测频率。此外，建行与中国互联网应急管理中心、公安机关、腾讯、360安全中心等外部机构建立数据共享机制，拓宽钓鱼网站来源渠道，鼓励行内行外积极举报钓鱼网站，并及时报送相关部门进行关停，大幅减少钓鱼网站存活时间，努力为用户提供安全的网络支付环境。

建行在国内率先建立网络金融反欺诈平台，依托全行统一、跨渠道的网络金融反欺诈系统，实现网上银行、手机银行、网上支付等电子渠道交易的7×24小时全面风险监控，对高风险交易实时阻断后进行人工分析、外呼核实、加黑名单等处理。一方面通过研究典型欺诈案例特征，结合客户历史交易行为习惯，部署相应的控制策略和措施，并动态调整；另一方面通过位置服务、终端识别等新技术应用，持续优化提高监控策略的有效性，将高命中率的监控模型应用系统智能化自动防控。

通过充分利用现代化的信息技术和大数据分析，依托基于用户行为分析的风险引擎，实时快速分析网络金融渠道客户交易行为细节，建立电子化、流程化、规范化的管理方式。对海量的数据进行比对、甄选，主动识别异常行为，采集异常行为数据，进行实时分析判断。挖掘欺诈团伙作案特征和规律，根据风险形势变化，实时动态部署智能化监控策略，扩大风控覆盖范围和拦截半径，实现精准识别高风险网络金融交易。

安全常识记心中

个人电子银行风险提示要点

1.提醒客户妥善保管账户介质、身份证件、安全产品等重要物品，不要将上述物品转交他人（包括银行工作人员）保管或使用，不要泄露银行密码、证件号码、银行卡号、电子银行渠道登录密码、手机密码等重要信息。

2.提醒客户不要设置简单的、有规律的、容易猜测的银行密码或手机服务密码。

3.提醒客户必须签约或登记本人的手机号码，当本人手机遗失或转让时，应及时注销电子银行服务，当本人手机号码更新后，应及时到银行更新。

4.提醒客户防止无抵押贷款、低息贷款、信用贷款、验资等各种名义的诈骗手段。

5.提醒客户不要在公共场所（如网吧、图书馆等）使用网上银行，以防止这些计算机可能装有恶意的监测程序，或被他人窥视。不要点击陌生人发送的邮件和“链接”，以防止使用的计算机中木马病毒或受到诈骗。

6.提醒客户谨慎在相关网站注册留存个人实名制相关信息，包括姓名、身份证号、手机号、电子邮箱等。

7.提醒客户定期下载安装最新的操作系统和浏览器安全程序或补丁；安装防火墙及防病毒软件，并定期杀毒；每次操作后要清除浏览器里的历史记录。

8.提醒客户网上购物选择信誉好、规模大网站，在使用网上银行进行支付时，不要开启来历不明的电子邮件和操作系统、MSN和QQ等工具软件的远程协助功能。

9.使用完网上银行后及时拔出网银盾并退出网上银行。

10.认准建行网站www.ccb.com，避免误入假冒网站，不要采用链接方式访问。如有疑问请及时拨打客户服务热线95533。

11.提醒客户开通建行手机银行后，一旦激活，即使更改了账户密码，手机银行也同样无需账户密码就可以进行资金转账汇款。

企业网银风险提示要点

1.提示客户妥善保管网银盾，要及时定期修改网银盾密码，不要将操作员网银盾、主管网银盾交与他人保管，同时不要将企业网银登录密码及交易密码透露、告知包括自称银行工作人员在内的任何人，避免发生资金风险。

2.提示客户企业网上银行跨行授权支付功能的风险点，签订跨行授权支付协议前，应仔细阅读建行跨行授权查询支付协议内容，对于协议内容不理解的部分，应及时到网点或致电95533或通过建行官方网站www.ccb.com进行查询，充分了解清楚后，方可办理。

火眼金睛识“套路”

亲们，这些年是否被“套路”过？身边的朋友是否也被坑过？不管有没有，练就一双“火眼金睛”，才是永远不被“套路”的法宝！建行专家与您分享网络支付常见案例：

▶▶冷饭新炒

“退款”“订单失效”“付款不成功”……一些骗子捏造所谓的“系统故障”“没有支付成功”等理由，通过发送链接等形式诱骗用户登录钓鱼网站，骗取用户的信用卡卡号、安全码、短信验证码等网络支付信息。其实，付款是否成功，在官方购物网站的交易详细页面即可查询，切勿轻信不明短信。

特点：看似司空见惯的老套路，实则变幻路数，让人放松警惕，迷惑性强。

对策：要保护好信用卡卡号、安全码等重要信息，短信验证码等同网络支付密码，任何索要短信动态验证码的，一律是诈骗！

▶▶换汤换药

情况一：拼团低价买水果，推出低价拼单，引诱用户下载使用，在得到用户的手机号、身份证号、信用卡卡号、安全码等敏感信息后，冒充银行、电信运营商等实施诈骗。

情况二：扫二维码送礼品，以各种优惠打折活动为借口，诱骗用户扫描包含木马病毒的二维码，病毒潜伏在移动终端后台中运行，持卡人的信息就会悄无声息地被盗取。

特点：利用某些用户贪小便宜的心理，骗取个人敏感信息，从而实施诈骗，套取资金。

对策：

1.扫码前一定要确认该二维码是否出自正规的网站，谨防“山寨”应用软件，发布在来路不明的网站上的二维码切记不要扫描，更不要点开链接或下载安装。

2.保护好个人重要账号信息，包括银行卡信息、网银账号、支付宝账号、微信账号等。

3.要及时为各类移动终端安装安全防护软件并定期更新。

▶▶旧招新拆

情况一：利用伪基站发送含网址链接、回拨电话的短信，冒充银行、电信运营商发布所谓“紧急通知”，通知内容如“银行系统升级”“银监局新规，要求补录个人信息”。

情况二：伪冒银行服务号，声称“积分兑换现金”“调高消费额度”，要求告知、转发动态验证码。通过诱导用户点击钓鱼网站链接或者回拨短信中的诈骗电话，从而骗取如信用卡卡号、有效期、安全码、短信验证码等敏感信息。

特点：目的都是引诱客户点击虚假短信中的钓鱼网站网址，骗取短信验证码。

对策：

1.要冷静，要保持头脑清醒，牢记贪小便宜易受大损失。

2.要通过正规渠道办理业务，对建行信用卡业务有任何疑问，请向建行工作人员询问。