中国银行 BANK OF CHINA
BEIJING 2022
北京2022年冬奥会官方合作伙伴
Official Partner of the Olympic Winter Games Beijing 2022

中国银行甘肃省分行积极担当社会责任 全面提升消费者权益保护工作水平

积极担当社会责任、履行社会义务，维护消费者合法权益不受侵害，是商业银行在经营活动中贯彻始终的一项重要工作，也是商业银行持续提升服务水平、完善产品结构、防范和化解金融风险的重要推动力，对普及金融知识、提升公民金融素养、促进社会公平正义有着积极意义。

作为历史悠久的国有大型商业银行，中国银行甘肃省分行认真落实党的十九大精神，以习近平新时代中国特色社会主义思想为指导，落实总行制定的新发展战略，始终把广大消费者的权益摆在首位，把维护消费者权益贯穿到企业战略决策、产品研发、风险管控等各项工作中，通过积极开展各项消费者权益保护工作，树立了大行形象，得到社会的广泛认可。

近年来，越来越多的消费者体验到了科技变革对生活带来的影响，各类网络支付、快捷支付方式在方便大家的同时，也为不法分子谋取利益提供了有利的犯罪工具，持续不断的银行卡盗刷、网络诈骗案件发生在每个人的身边，普及、了解、掌握信用卡与网络支付安全知识，与每一位金融消费者的利益息息相关，今天就为大家介绍一下相关知识，防患于未然。

网络支付安全知识指南之“故事里的事，没有安全就没有支付”

以下每一个案例后面都有个人资金的损失，都有很惨痛的教训。吸取教训，我们就能绕开陷阱，提前预防，保证网络支付安全。

案例一：注意网络支付陷阱！

从广东出发参加朋友婚礼的覃女士在一酒店上网买机票，多次输入密码网上仍显示支付未成功，但卡上的近15万元却被转走了。经过覃女士的追踪发现，这笔钱到了游戏公司的账户，被采购成游戏点卡。

【安全提示】

1.使用办公、家庭外的电脑时，存在资料泄露的风险。不排除电脑已中了木马病毒，尽量不使用公共电脑进行支付，必须使用的，在使用前请先查杀木马或病毒，并开启防火墙保护功能。

2.不断让输密码，存在被套资料的潜在风险，应立即停止支付。

3.查询资金被转移后，请记录单号，即刻报警，请警方处理，保存收到的银行提醒短信，作为辅助凭证。

4.及时和网络支付的银行、第三方支付机构客服联系，及时了解资金去向，尽可能减小损失。

案例二：防网购火车票中木马病毒盗卡！

周先生在一家旅馆电脑访问12306.cn网站购票付款时，网页自动跳转到游戏点卡交易页面，网银付款对象也从“铁道部资金结算中心”变为第三方支付平台，收款商户是某网络科技有限公司。由于周先生并没有注意看收款方，导致资金被转移。事后得知，旅馆电脑事先已被植入木马，劫持火车票款为黑客购买游戏币。

1.支付完成时，原来的网页没有显示支付成功，但同时跳转出来的另一个页面，显示支付成功，点开发现是某网络科技有限公司的网页，与原网站不符。

2.即刻收到银行消费短信，显示被划走的金额，远远大于一张票价。

3.资金结算时，突然转到游戏点卡缴费页。

【安全提示】

1.使用公共电脑进行支付的，在使用前应先查杀木马或病毒，并开启防火墙保护功能。

2.在支付时应当注意订单内容，防止订单被替换后继续支付。

3.采取短信验证的辅助方式，对订单支付信息再次确认后再支付。

4.确认被钓鱼后，请即刻向公安部门报案。请保存相关网站截图和收到的银行提醒短信，作为辅助凭证。及时和银行、第三方支付机构联系，减小损失。

案例三：账户密码单独设置

南京网友小米最近在一家社交网站的用户名和密码被盗，她也没在意，就重新注册了一个，谁知道没过两天，其支付账户上却被人盗用在网上购买了几百元的游戏点卡——原来，其为了省事，微博、邮箱和网络支付账号都使用相同的账户与密码，结果被人盗用了支付账户。

【安全提示】

1.网络支付账号和密码应该单独设置，不要和其他网上账户相同。

2.密码设置要独特性，不能为了记忆方便，设置一些简易或者与生日、电话号码等关联的密码。

3.在支付账户中不要存入大额资金，对于支付账户开启电子证书、短信验证等多重保护，保证账户安全。

4.一旦发现支付账户被盗，及时与支付机构联系，冻结账户，防止损失扩大。

案例四：“免费Wi-Fi15分钟盗走密码”

凌晨1点，在北京工作的银先生在睡前通过手机银行查看账户。睡下后没多久，凌晨2点多，短信声响起，银行发来的取款提醒，称其银行卡刚从ATM取款机上取出人民币2000元。而此时，银行卡就在他身上。

正当银先生诧异的时候，第二条、第三条内容相似的短信进来了，有现金取款的，有银行转账的。1小时不到，17条提醒短信，银先生共被转走3.4万元(现金取款7次共1.4万元，银行转账共2万元)。因卡是在长沙办的，天一亮，银先生立马赶回长沙报了警。

银先生自述有“蹭网”的喜好，只要有免费Wi-Fi，他就会“蹭”。“肯定是用Wi-Fi的时候被盯上了，被人盗取了我的网银信息。”不法分子会设置没有密码的Wi-Fi吸引手机用户使用。一旦连上钓鱼Wi-Fi，手机用户的操作记录就会被复制，被相关软件破解。用户的账号被盗分两种：网站加密性不高时，直接被不法分子破解；安全系数高的网站，如银行、支付宝等网站，黑客则会引导用户到山寨钓鱼网站，从而获取账号和密码。因网上银行、支付宝等金融类网站和手机客户端信息经过了层层加密，破解的难度大，而微博、QQ、邮箱、游戏等账号则会相对容易。

【安全提示】

1.平时最好关闭Wi-Fi自动连接。手动使用时，也应看清Wi-Fi名称，尽量不在不明的Wi-Fi上进行网络支付。

2.在登录手机银行或者支付机构网站时，最好不要直接通过浏览器，而应用银行或者第三方支付公司专用应用程序。

3.发现银行卡被盗刷，应当及时与银行联系，冻结银行账户，并及时报警。

网络支付安全知识指南之“有防范才能有安全，六大法宝让你身处安全线以内”

目前，很多消费者对于网络支付安全存在“误区”，一种是放任自流型。我只管上网支付，安全是银行和支付机构的事情，和我无关；一种是过度防护型，谨小慎微，每次使用网络支付都是如临大敌，生怕一不小心被人诈骗，无论多少，无论好坏，反正只要有的安全措施和工具都一股脑用上，导致网络支付的用户体验很差，有时候反而成为用户负担；还有一种是疏忽大意型，容易轻信网上的邮件和留言，该装的安全软件也不装，为了省事，账号和密码设置过于简单等等。为确保网络支付安全，用户首先要有安全意识和基本防范技能。

第一法宝：确保终端安全，保证安全锁完好

及时更新杀毒软件，操作系统补丁。

直接从官方网站上下载安装银行、第三方支付的控件和软件。

不要轻易点击不明链接，或他人发送过来的链接，文件。

第二法宝：妥善保管敏感信息，保证钥匙没丢

身份证信息、账户信息、银行卡信息、手机号等要妥善保管，不轻易提供给他人。

不轻易在小网站或不知名的网站上预留以上信息。

第三法宝：重视密码安全，安全的第三重保障

要设置个性密码。单独设置，不与其他公共场合常用的密码相同。

请不要使用连续、重复、简单的数字组合或与本人生日、电话号码、身份证号码等相关的数字信息。短信验证码、动态口令等动态密码涉及到账户安全、资金安全，不提供给任何他人，包括自称为工作人员或客服的人员。任何索取短信验证码的行为都属于诈骗行为。

妥善保管支付口令牌等支付安全工具，不要将其交付他人。使用完毕后应及时从电脑上取回。若遗失，请尽快到银行柜台办理挂失及补办手续。

第四法宝：充分使用银行或者支付机构提供的各类安全产品

银行或者支付机构提供的各类安全工具或者产品，针对性强，安全保障比较好。用户在使用网络支付时，务必充分使用这些安全工具或者产品，比如申请数字证书、开通手机动态口令、短信提醒等服务，以提高账户及交易的安全性。如果您经常进行网上支付，建议您前往银行柜台办理网银专业版开通手续，在上网终端安装网银数字证书，确保银行账户安全。

第五法宝：培养良好的安全支付习惯

尽量不要在网吧、图书馆等公共场所使用网上银行，若在公用电脑上使用网上银行，请务必确认所有信息都被清除后再关闭电脑浏览器。

申请网上支付服务时，您可以根据自己的需要自由定制您支付的交易限额，请根据您实际使用情况进行设定，以避免日后可能给您带来的经济损失。

交易完成后不论系统提示成功与否，都要查询账户余额和交易明细。要定期查看历史交易明细并定期打印网络支付业务对账单，如发现异常交易或账务差错，应立即与银行或者支付机构联系，避免损失。

仔细核对支付信息。核对支付时请注意核对页面显示的“商户名称”、“商品名称”、“数量”和“总金额”等信息，防止误付、错付。

个人资料(联系电话、地址等)有任何变更，请及时通知银行或者支付机构修改相关资料或通过客户端自行修改。

第六法宝：选择银行和有资质的支付机构进行网络支付

要尽量选择商业银行与获得人民银行许可的支付机构进行网络支付业务。这些机构的资信较好，安全防范的措施相对完备，用户可以放心选择。对那些没有相关资质或者来路不明的机构提供的网络支付业务，要谨慎选择，如果确实想用，也要多方验证后再使用。

网络支付安全知识指南之“网络支付安全七字口诀”

陌生电话要警惕，可疑短信需注意
升级网银假信息，钓鱼网站莫点击
刷卡消费欠话费，细分真伪辨猫腻
中奖退税送便宜，哄你汇钱是目的
暴利理财和投资，多是骗局莫搭理
若是有人要验资，多半是来把人欺
亲朋好友遇事急，不忙汇款先联系
冒充领导公检法，提防骗子在演戏
来电自称黑社会，立刻报警不迟疑
别人替您办网银，定要坚决把他拒
网银本人来开通，安全工具自己拿
网络手机和电话，电子支付方便您
但若您听坏人语，轻易开通他得利
任凭骗术千万变，我自心中有主意
不理不信不汇款，小心谨慎防万一

远离非法集资建设美好生活 非法集资的概念、特征、表现、欺诈手段、识别方法

一、非法集资的概念

非法集资是违反国家金融管理法律规定，向社会公众(包括单位和个人)吸收资金的行为，非法集资行为需要同时具有非法性、公开性、利诱性、社会性四个特征要件，具体为：一是未经有关部门依法批准或者借用合法经营的形式吸收资金；二是通过媒体、推介会、传单、手机短信等途径向社会公开宣传；三是承诺在一定期限内以货币、实物、股权等方式还本付息或者给付回报；四是向社会公众即社会不特定对象吸收资金。

二、非法集资典型特征

1.未经有关单位依法批准，包括没有批准权限的部门批准进行集资，即集资者不具备集资的主体资格。

2.承诺在一定期限内给出资人还本付息或者给付回报，还本付息的形式为主，也有实物、股权等其他形式。

3.向社会公众即社会不特定对象吸收资金。

4.以合法形式掩盖其非法集资的实质。为掩盖其非法目的，犯罪分子往往与投资人(受害人)签订合同，伪装成正常的生产经营活动，最大限度地实现其骗取资金的最终目的。

5.集资初期往往积极兑现承诺，骗取信任，以吸引更多的人的加入，使集资规模呈几何级放大，集资资金被集资策划组织者大肆挥霍。

三、非法集资的主要表现形式

1.借种植、养殖、项目开发、庄园开发、生态环保投资等名义非法集资。

2.以发行或变相发行股票、债券、彩票、投资基金等权利凭证或者以期货交易、典当为名进行非法集资。

3.通过认领股份、入股分红进行非法集资。

4.通过会员卡、会员证、席位证、优惠卡、消费卡等方式进行非法集资。

5.以商品销售与返租、回购与转让、发展会员、商家联盟与“快速积分法”等方式进行非法集资。

6.利用民间“会”、“社”等或者地下钱庄进行非法集资。

7.利用现代电子网络技术构造的“虚拟”产品，如“电子商铺”、“电子百货”、投资委托经营、到期回购等方式进行非法集资。

8.对物业、地产等资产进行等份分割，通过出售其份额的处置权进行非法集资。

9.以签订商品经销合同等形式进行非法集资。

10.利用传销或秘密串联的形式非法集资。

11.利用互联网设立投资基金的形式进行非法集资。

12.利用“电子黄金投资”形式进行非法集资。

四、非法集资常见的欺诈手段

1.承诺高额回报 不法分子为吸引群众上当受骗，往往编造“天上掉馅饼”、“一夜成富翁”的神话，通过暴利引诱许诺投资者高额回报。为了骗取更多的人参与集资，非法集资者在集资初期，往往按时足额兑现承诺本息，待集资达到一定的规模后，便秘密转移资金或携款潜逃，使集资参与者遭受惨重的经济损失。

2.编造虚假项目 不法分子大多通过注册合法的公司或者企业，打着响应国家产业政策、支持新农村建设、实践“经济学理论”等旗号，经营项目由传统的种植、养殖行业发展到高新技术开发、集资建房、投资入股、售后返租等内容，以订立合同为幌子，编造虚假项目，承诺高额固定收益，骗取社会公众投资。有的不法分子假借委托理财名义，故意混淆投资理财概念，利用电子黄金、投资基金、网络炒汇、电子商务等新名词迷惑社会公众，承诺稳定高额回报，欺骗社会公众投资。

3.以虚假宣传造势 不法分子为了骗取社会公众的信任，在宣传上往往一掷千金，采取聘用明星代言、在著名报刊上刊登专访文章、雇人广为散发宣传单、进行社会捐赠等方式，加大宣传力度，制造虚假声势，骗取社会公众投资。有的不法分子利用网络虚拟空间将网站设在异地或租用境外服务器设立网站。还有通过网站、博客、论坛等网络平台和QQ、MSN等即时通讯工具，传播虚假信息，骗取社会公众投资。一旦被查，便以下线不按规则操作为名，迅速关闭网站，携款潜逃。

4.利用亲情诱骗 不法分子往往利用亲戚、朋友、同乡等关系，用高额回报诱惑社会公众参与投资。有些参与传销人员，在传销组织的精神洗脑或人身强制下，为了完成或增加自己的业绩，不惜利用亲情、地缘关系拉拢亲朋、同学或邻居加入，使参与人员迅速蔓延，集资规模不断扩大。

五、非法集资的识别方法

1.看集资主体资格是否合法，是否获得相关部门的批准；是否向社会不特定对象募集资金；是否承诺高额回报，非法集资行为一般具有许诺一定比例集资回报的特点；是否以合法形式掩盖非法集资的性质。

2.增强理性投资意识。高收益往往伴随着高风险，不规范的经济活动更是蕴藏着巨大风险，坚信“天上不会掉馅饼”，对高额回报，快速致富的投资项目要进行冷静分析，认清非法集资的本质和危害，提高识别能力，自觉抵制各种诱惑。

3.增强参与非法集资风险自担意识。非法集资是违法行为，参与者投入非法集资的资金及相关利益不受法律保护。当一些单位或者个人以高额投资回报兜售高息存款、股票、债券、基金和开发项目时，一定要认真识别，谨慎对待。