支付安全·防范电信网络新型欺诈

随着互联网、大数据、人工智能等技术的迅猛发展，电信网络欺诈也频频翻新作案手法，呈现出精准化、多样化、团伙化、跨境化等特征，严重损害社会诚信和社会秩序，成为影响群众财产安全和社会和谐稳定的一大公害。

党中央、国务院高度重视反欺诈工作，要求各相关部门加强协作密切配合，从保护人民群众财产安全的高度，加大打击欺诈行为的工作力度。人民银行积极贯彻，于 2019 年 3 月发布了《关于进一步加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》提出 21 项措施，进一步筑牢金融业支付结算安全防线。中国支付清算协会提醒广大消费者：管好你的账户、用好你的 APP、护好你的个人信息、守好你的资金、看懂反欺诈套路。

一、管好你的账户

（一）合理分类银行账户，防范电信网络诈骗：

通过分层、分类地使用银行账户，可以为个人建立资金防火墙，有效地保护个人银行账户资金和信息安全。

1、账户清理更便利，犯罪源头被切断。除社保、公积金等特殊账户外，境内银行账户的变更和撤销服务均可跨网点办理。每人在同一家银行只能开设一个Ⅰ类账户，闲

置账户建议配合银行进行清理或降级，防止被犯罪分子冒用、盗用。

2、电子账户有限额，风险损失可控制。II 类、III 类账户消费、转账有限额，帮助消费者享受到小额账户电子支付便利性的同时，有效隔离风险、控制电信网络欺诈的损失。

3、个人信息不泄露，远程开户真便利。II 类、III 类银行账户可通过电子渠道开立，消费者应更加注重保护身份证、银行卡、预留手机号和支付密码等个人信息，防范由于信息泄露导致被不法分子伪冒开户和盗用。

（二）保护自身权益，远离银行账户和支付账户买卖

买卖银行账户和支付账户是违法行为。

违反法律法规：

《关于办理电信诈骗等刑事案件适用法律若干问题的意见》：

明知他人实施电信网络诈骗犯罪,具有下列情形之一的,以共同犯罪论处,但法律和司法解释另有规定的除外:1.提供信用卡、资金支付结算账户、手机卡、通讯工具的;……

《关于进一步加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》：

银行和支付机构对经设区的市级及以上公安机关认定的出租、出借、出售、购买银行账户（含银行卡）或者支付

账户的单位和个人及相关组织者，假冒他人身份或者虚构代理关系开立银行账户或者支付账户的单位和个人，5 年内暂停其银行账户非柜面业务、支付账户所有业务，并不得为其新开立账户。

人民银行将上述单位和个人信息移送金融信用信息基础数据库并向社会公布。

二、护好你的个人信息

随着支付的电子化、远程化，个人信息泄露已成为消费者使用移动支付过程中最常遇到的安全问题。护好个人身份信息，从身边做起：

一是完成支付工具实名认证，以便手机等支付设备或支付账号被盗后找回账户及资金。

二是谨慎提供个人信息。不轻易透露身份证号码、银行卡号、有效期、安全码等信息，不向银行和支付机构业务流程外的任何渠道提供支付密码和短信验证码等，不向任何人发送带有银行卡信息和支付信息的图片。

三是不明 WiFi 不连、不明链接不点、不明二维码不扫、不明网站不上，连接免费 wifi 时不登录网上银行、手机银行、支付机构 APP 进行账户查询、支付等操作。

四是支付密码设置动态更新并加强保护。避免使用生日、手机号码等简单数字密码，防止不法分子通过撞库盗号。

五是申办银行卡要通过正规金融机构渠道提出申请，谨防

黑中介留存个人身份信息后伪冒办卡，防范伪卡盗刷风险。选用安全性更高的支付工具，建议将磁条卡升级为芯片卡。

六是警惕冒充公安、警官、法院、检察院要求上报个人信息或转账的电信网络欺诈，收到此类信息应第一时间与官方平台联系，核实信息真伪。果断拒绝在电话、短信、微信等非面对面环境中索要个人信息的行为。

三、用好你的 APP

1、通过正规应用商店等渠道下载金融理财类 APP，以免手机感染木马病毒或者误装仿冒软件。恶意软件可以通过启动其仿冒界面来覆盖原界面，导致用户在仿冒界面中输入账号信息。

2、不要被高回报诱惑，远离炒汇、现金贷、套路贷等虚拟 APP 交易平台。警惕金融类 APP 利用虚拟币或区块链技术的幌子进行诈骗、传销等犯罪活动。

3、按需开通手机 APP 的隐私权限，及时关闭不必要的 APP 权限。

四、守好你的资金

（一）二维码支付

1、扫商户收款码付款时，要确认收款商户名称、交易金额等信息是否正确。

2、被商户扫付款码付款时，要留意自己周围的环境是否安全，不要过早打开付款码。注意保护支付密码，避免被拍照盗用产生资金损失。

3、条码支付适合小额高频交易，单笔金额较大的交易建议使用刷卡或网上银行、手机银行等支付工具。

（二）转账管理

1.谨慎转账至陌生账户，对来路不明或非日常转账要求要进一步核实。

2.客户办理转账业务时可以选择实时到账或普通到账、次日到账等非实时到账。

3.通过银行自助柜员机办理转账业务时，要认真核对转账受理界面中文显示的收款人姓名、账号和转账金额等信息。若选择实时到账，需要对此进行确认。

4.非必要时建议选择“次日到账”等非实时到账，如发现疑似遭遇电信诈骗可及时联系银行客服热线或至网点柜面申请撤销转账。

5.ATM 出现吞卡故障、扣账不吐钞等情况时，不要马上离开，可在原地拨打银行服务电话求助，谨防被不法分子转移注意力，调包银行卡。

（三）免密免签业务管理

1.　开通小额免密免签支付服务后，将不再需输入密码也不需要签名即可完成支付，提升了支付便捷性，便利了日常生活。

2.　免密免签业务适用于小额场景，开通时建议设置支付限额。

3.用户对于开通免密免签业务具有知情权和自主选择权。用户可根据使用频率及场景自主选择开通银行卡或其他支付工具的免密免签或自动扣款服务。

4.中国银联联合各商业银行提供闪付小额免密“风险全额赔付”服务，对于正常用卡客户发生的双免盗用损失，经核实可得到全额赔付。

五、看懂新型欺诈套路

随着金融欺诈与大数据、人工智能等金融科技技术的结合，电信网络新型欺诈通过对不同群体进行标签化分类，精准定位目标受众，准确匹配犯罪场景，大大增加了防范电信网络新型欺诈的难度。

常见典型欺诈类型：高利理财类、网络借贷类、冒充虚构类、消费金融类、非法集资类

高利理财类主要是以低投资获得高利息、“消费返利”、投资境外股权、外汇，投资“区块链”、“虚拟货币”为噱头进行“利益”诱惑实施欺诈。

网络借贷类通常通过网络虚假广告引诱、缴纳保证金、中介代办、担保公司模式等方式盗取投资者信息，以低息贷款进行引诱。

冒充虚构类主要通过冒充熟人、领导、公检法，或虚构绑架、中奖、到付快递等骗局，诱骗受害人转账汇款。

消费金融类主要有网络支付诈骗、虚假营销、骗取网购运费险、骗取消费退款、网络刷单诈骗等欺诈方式。

非法集资类包括擅自发行股票、债券，利用传销或秘密串联的形式非法集资，甚至利用地下钱庄等民间会社形式非法集资，签订商品经销经济合同的形式进行非法集资。

不论套路多么复杂，各类电信网络欺诈最终都需要转移诈骗资金，因此合法科学安全地使用账户及支付资金是防范电信网络新型欺诈的重要防线。

风险案例

一、提升信用卡额度骗局

受害人收到 XX 银行的信用卡提升额度的短信，其点击短信内的链接并按照网页内提示填写了个人信息及信用卡账号和密码，在填写了两次验证码后被盗刷 33000 元。

提示：

一是不要轻信任何套取个人信息的电话、短信或广告。

二是不要将卡号、密码、身份证号等信息资料轻易透露给他人。

三是对于银行卡使用中不清楚的事项，应向发放信用卡的银行专门机构咨询，发现银行信用卡或密码遗失应当及时办理挂失手续。

二、短信二维码电信诈骗

某客户收到一条短信，显示账户已转出 36000 元，用途不明，着急查询银行卡账户余额。客户拨打短信中的电话询问相关扣款情况，对方告诉客户是因为他们操作失误导致扣款，只需客户扫描短信中的二维码就能进行还款操作。

客户来到银行，大堂经理看了一下收到的扣款短信，发现其界面显示为“某游戏平台支付界面，支付金额为 1 万元”。同时，对方语气急促不停向客户催促要求尽快输入密码，且支付金额与短信金额不一致。大堂经理判断该客户疑似遭遇

电信诈骗，故立即让客户挂断电话，关闭支付界面，同时告知客户可能遭遇电信诈骗，建议客户到开户行对扣款情况进行详细查询。客户进行账户余额查询，发现资金状况完好后，方明白自己险些上当。

提示：

1.收到来路不明的短信，应第一时间与官方平台联系，核实信息真伪。

2.若遭遇“扣款”，及时查询账户动态，必要时前往银行柜台咨询情况。

3.不要轻易点击或扫描陌生人提供的链接及二维码。

资料来源：中国支付清算协会