



防范电信网络诈骗 宣传手册

江苏省公安厅



反电信网络诈骗总队



新闻宣传中心

江苏省公安厅



反电信网络诈骗总队



新闻宣传中心

前言

近年来,电信网络诈骗犯罪案件居高不下,已成为上升最快、占比最高、群众反应最强烈的主流犯罪,严重危害广大人民群众的获得感、幸福感、安全感。

当前,全省各地、各有关部门正在开展打击治理电信网络诈骗犯罪“百日行动”,坚决维护人民群众财产安全和社会治安大局稳定。省公安厅反诈总队、新闻中心精心梳理防骗知识要点,编制本手册,助力反诈宣传走进千家万户、渗入千行百业。

目 录

TABLE OF CONTENTS



电信网络诈骗十大高发类型

- ▶ 01 刷单返利诈骗
- ▶ 02 虚假网络投资理财诈骗
- ▶ 03 冒充电商物流客服诈骗
- ▶ 04 虚假贷款诈骗
- ▶ 05 虚假征信诈骗
- ▶ 06 虚假购物、服务诈骗
- ▶ 07 冒充领导熟人等特定身份诈骗
- ▶ 08 网络游戏产品虚假交易诈骗
- ▶ 09 冒充公检法及政府机关诈骗
- ▶ 10 裸聊敲诈



《反电信网络诈骗法》

01

刷单返利诈骗



易受骗群体：待业群体、学生群体等

作案手法

▶ 第一步：

骗子通过电话、短信、网页及社交媒体等渠道发布招聘兼职刷单的广告，诱骗受害人加入群聊。



第二步：

前期，骗子会发布简单任务，完成即给小额返利来获取受害人信任，随后便以“充值越多、返利越多”为由，引导受害人加大投入。



▶ 第三步：

待受害人垫付大额资金后，骗子便会以“卡单、联单、操作失误”等理由拒不返还资金，并诱导其不断转账汇款，直至受害人发现被骗。



“复合型刷单返利”骗局

刷单+色情：

骗子通过各种渠道传播色情信息，吸引受害人上钩，随后声称完成**刷单任务**才能享受服务。

刷单+网络赌博：

所谓的刷单平台就是**跨境网络赌博平台**，刷单就是下注赌博，而平台的盈利都是假象，最终钱款都将“有去无回”。

刷单+招聘：

骗子冒充知名公司发布假冒招聘广告，所谓的工作就是让你在指定**网络平台充钱、做任务**。

典型案例

某日，张女士在观看短视频直播时看到了一个招聘兼职刷单的广告，于是扫码加入了聊天群中，群里的客服先是派发了一些关注账号、点赞短视频的任务，完成后截图发群里就可领取小额红包。张女士做了2天任务，共领到200元的红包。后客服称群里的任务派发完了，需要更换平台才能继续刷单，张女士便扫码下载了一个叫“XX互联”的APP。平台客服为张女士派发了一组“联单”任务，连续完成三笔订单就可领取高额佣金，张女士先后转账三次共计13万元，完成后张女士发现平台账号里的资金无法提现，客服称张女士最后一笔订单支付超期，导致任务失败，需要再完成一次“联单”任务才能连本带利全部提出，无奈之下张女士又转账13万元，后客服仍以各种理由要求张女士继续转账，张女士这才意识到自己遭遇诈骗。



反诈高频词

“高额佣金”

没有动动手指就能赚钱的好事，骗子前期给予**小额返利**，就是为了骗取信任，为实施诈骗进行铺垫。

“正规兼职”

为骗取信任，前期刷单操作大多在正规平台进行，“**点赞关注**”“**帮刷信誉**”“**打榜助力**”等行为看似正规，实则是刷单诈骗的前置环节，后期引诱受害人下载涉诈APP，借机实施诈骗。

“充值垫付”

骗子以高额佣金为诱饵，引诱受害人完成任务，实则锁定的就是受害人的垫付资金。

请牢记

凡是以获取返利，引导大家垫付资金做刷单“任务”的，都是诈骗！切记，刷单入了套，本金要不到！

02 虚假网络投资理财诈骗

易受骗群体：热衷于投资、炒股的群体

作案手法

▶ 第一步：

骗子通过各种渠道发布**投资理财**的推广消息，宣称掌握各种投资技巧和内幕消息，将受害人引至事先搭建好的群聊之中，冒充**投资导师、金融理财顾问**等专家身份，以直播授课、晒虚假盈利截图等方式骗取受害人信任。



第二步：

骗子诱导受害人进入**虚假的投资APP、网站**，引导小额投资试水，前期可以获取低额返利，待受害人彻底卸下防备后，便以“**稳赚不赔**”等名义诱骗其加大资金投入。



▶ 第三步：

当受害人投入大量资金后，投资平台看似不断盈利实则无法提现，骗子会以“**登录异常**”“**服务器维护**”“**银行账户冻结**”等各种理由，要求受害人缴纳“解冻费”“保证金”等费用，直至掏空钱包。



在该类骗局中，骗子还可能精准锁定受害人身份，伪装成“**高富帅**”“**白富美**”等人设，以恋爱交友为由骗取受害人信任，随后以“**有特殊资源**”“**平台有漏洞**”为由，诱骗受害人至虚假的投资理财平台进行投资，以此实施诈骗。

典型案例

35岁的陆女士通过“某爱网”添加了一名好友，对方自称在某期货公司工作，陆女士与对方十分聊得来，便以恋爱交友的名义开始相处。聊天过程中，对方透露自己发现了一个期货投资平台的漏洞，已经赚了很多钱，还以在外出差为由，请陆女士登录自己账号代为操作，陆女士登录账号后，发现确实盈利颇丰。后对方劝陆女士一起投资，在感情和利益的双重诱惑下，陆女士加入其中，先后向对方指定账户中转账汇款60万元。过了一个月，陆女士想要提现时，发现平台显示账号异常被冻结，而对方也把自己的账号拉黑。无奈之下陆女士只能报警求助，这才发现自己被骗。



反诈高频词

“稳赚不赔”“超高回报”

骗子塑造的投资项目都是超高年化收益，动辄20%以上，甚至高达50%，而且“**稳赚不赔**”。可真有发财的机会，为什么要带非亲非故的陌生人赚钱？

“投资导师”“理财专家”

骗子常会伪装成经验丰富的投资专家，如何分辨呢？登录【**中国证券业协会**】网址，即可查询机构和个人是否合规、有无备案，还可查询人员的从业资质、执业编号等信息。

“投资软件”“权威平台”

金融类APP在手机应用商城的上架审核十分严格，需要提供**营业执照、证书、协议**等相关资质文件。由于虚假投资理财类诈骗APP无法通过正规途径在应用市场上架，骗子只能通过**创建网址链接、发送APK安装包或扫描二维码的方式**让用户下载安装虚假投资理财APP或进入虚假投资网站。

“指定账户”

正规投资平台只能转账到开设的**专用对公账户**，凡是要求直接将资金转入个人账户或要求转账的对公账户与平台名称不符的，极有可能是虚假投资理财涉诈平台。

请牢
记

不要轻信非正规渠道推荐的投资理财，凡是标榜“**内幕消息**”“**稳定高回报**”的网络投资理财，都是诈骗！

03 冒充电商物流客服诈骗

易受骗群体：经常进行网上购物的群体

作案手法

▶ 第一步：

骗子冒充电商或物流客服工作人员联系受害人，说出通过非法渠道获取的身份信息、购物信息或是物流信息，谎称受害人购买的商品有质量问题或是快递丢失，要对其进行退款赔偿。



第二步：

骗子会发送虚假的退赔链接或二维码，诱导受害人在网页上填写自己的银行卡信息及手机验证码等信息，从而将受害人银行卡内的钱款转走，或是以“激活退款通道”“缴纳退款保证金”等理由，要求受害人转账汇款，从而实施诈骗。



典型案例

某日，市民王小姐接到一个自称是淘宝商家客服的电话，说王小姐在网上购买的奶瓶有质量问题，要给她退款赔偿。王小姐加了对方QQ后，收到了一条链接，点开后页面显示为退款中心，王小姐按照网页引导填写了自己的身份证号、银行卡号、手机号、余额等信息，随后还将手机收到的验证码也输入到网页之中。没多久，王小姐就收到短信消息，显示自己的银行账户被转出1万元。



反诈高频词

“商品质量有问题”

网购商品存在质量问题需要理赔退款，会通过**购买平台原路返还**，不需要通过其他平台完成操作。

“快递丢失”

如果快递丢失，物流公司一般会将等额货款赔给卖家（寄件人），再由卖家重新发货，而不会主动联系收件人进行理赔。

“退款链接”“理赔页面”

看似正规的退赔链接或二维码，打开后实则是**虚假的涉诈平台**，一旦在其中填写**个人银行卡信息及手机验证码**等信息，即有可能遭遇财产损失。



请牢记

电商客服来电主动退赔，要求先转账再退款的都是诈骗！
如有疑问，可通过官方平台进行核实。

04 虚假贷款诈骗



易受骗群体：无业、个体等有贷款需求的群体

作案手法

▶ 第一步：

骗子伪装成正规金融机构客服，通过**电话、短信或网络等**渠道发布虚假贷款广告，并以“无抵押、免担保、零门槛、快到账”等诱导性话语，吸引受害人上钩。



第二步：

骗子会诱导受害人**下载虚假贷款APP或者登录虚假贷款网站**，填写贷款申请信息，并签订所谓的电子贷款合同，制造放款假象。



▶ 第三步：

骗子会以“**贷款需要审核**”为由，要求受害人先缴纳**“保证金”“手续费”**，或是以操作失误、征信异常、流水不足等原因，要求受害人缴纳各种费用，直至掏空受害人的钱包。

典型案例

某日，马某接到一通电话，对方自称是某贷款公司客服，声称可以提供小额免息贷款，于是马某添加了对方好友并扫码下载了一个名为“某某E贷”贷款APP。马某在该APP申请了5万贷款额度，还签署了电子借款合同。很快，平台就显示贷款已经下发，但马某申请提现时一直显示提现失败，客服表示马某申请贷款时银行卡号填错了一位数字，导致账号被冻结，需要缴纳5000元解冻费才能提现，同时承诺解冻后会全额退还所有费用。马某因着急用钱，就按客服要求缴纳了费用。随后，客服又以验证还款能力、刷流水等理由要求马某继续转账，还指导马某去各大正规平台申请贷款，后马某将贷到的资金全部转给客服指定账号，共计20余万元。



反诈高频词

“无抵押、免征信、秒到账”

正规贷款有严格的资质审核，任何声称**无需抵押、不查征信、快速到账**的网贷平台都有极大风险，切勿轻信。

“超低利率”“无手续费”

正规借贷平台都有规范的利率与手续费，如果有平台声称可以提供**超低利率与手续费**的借贷服务，那很有可能是骗子抛下的诱饵。

请牢记

不要轻信网络贷款广告，申请贷款一定要到正规的金融机构。
凡是网上贷款要先缴费的，都是诈骗！

05 虚假征信诈骗

易受骗群体：高知群体、借贷群体

作案手法

▶ 第一步：

骗子多冒充互联网金融平台客服或银保监会工作人员，谎称因国家出台新征信政策，要求受害人关闭在平台上开通的金融业务，或者是注销曾以学生身份申请的校园贷款，否则将影响个人征信。



第二步：

骗子会出示仿冒的工作证件、征信报告等官方文件，以此打消受害人疑虑，随后诱导受害人下载具有共享屏幕功能的会议软件，并以指导操作等各种理由，要求其开启“**共享屏幕**”功能，借机窃取受害人的身份信息。



▶ 第三步：

骗子会以“**数据异常**”“**操作失误**”等理由要求受害人将银行账户内的资金或在网贷平台上申请的贷款转入指定账户之中。



典型案例

刘女士接到一个自称是“京东客服”的陌生来电，对方称刘女士开通了京东金条的贷款业务，因贷款利息过高，超过了国家相关规定，为避免影响个人征信，建议其取消贷款并关闭京东金条。刘女士下载并登录京东，发现自己的京东金条页面显示借款额度为20万元，便相信了对方的话。随后，刘女士按照对方要求下载了某视频会议APP，开通了屏幕共享功能，先后将自己银行卡内余额分6次共计46万元，转入指定银行账户中用于“取消贷款”。



反诈高频词

“银保监会”“京东客服”

银保监会、京东客服电话不会主动外呼，外呼客服号码为固定短号码。如接到自称**银保监会**、**京东客服**的电话，应当提高警惕。

“征信受损”“帮助修复”

骗子通常会强调受害人征信有问题，不修复对以后的生活和事业都有影响。事实上，个人征信由中国人民银行征信中心统一管理，任何人无权删除、修改。

“注销校园贷”“消除不良记录” “降低贷款利率”“注销借贷账户”

这些都是骗子的常用话术，目的就是为了让受害人相信骗子身份，从而配合骗子完成操作。

“共享屏幕”

使用“**共享屏幕**”功能是此类诈骗的固定套路，一旦使用这一功能，即使骗子不主动询问，也能看到受害人手机上的所有信息，包括输入密码时的数字和显示顺序、收到的验证码等，从而转走卡内资金！

请牢记

凡是以“修复征信”等为由，要求开通贷款提额转账或是共享屏幕的，都是诈骗！

06

虚假购物、服务诈骗

易受骗群体：热衷于在网购平台或其他社交平台购买商品的群体

作案手法

▶ 第一步：

骗子在网购平台、社交媒体或其他网站发布优惠打折、海外代购、低价转让等极具诱惑性的商品信息，或者声称可以提供论文代写、私家侦探等服务，吸引潜在受害人上钩。



第二步：

吸引到有购买意愿的受害人后，骗子便会添加其社交账号进行商议，进而以**私下交易**可以节约手续费等理由，要求受害人**直接转账**，或诱导受害人进入虚假的交易网站支付费用。



▶ 第三步：

在受害人付款后，骗子会以**收取运费、加缴关税、缴纳定金、交易税、手续费**等理由，要求受害人继续转账，进而完成诈骗。

典型案例

于某在某二手购物平台浏览时，发现有一款自己心仪已久的九成新手表，价格远低于同类商品，于是添加对方QQ好友并表达购买意向。双方在一番讨价还价后达成共识，但对方说购物平台的手续费高，要求于某在QQ中直接支付货款。于某急于得到心仪的手表，便扫描对方发来的二维码，直接支付3.5万元。对方表示近期发货，但于某迟迟没有收到商品，再去联系对方时，才发现自己已被拉黑。



反诈高频词

“内部优惠”“超低折扣”

骗子利用了受害人贪图小利的心理，以提供**低价折扣商品、服务为诱饵**，吸引受害人上钩。

“手续费高”“私下交易”

正规平台的交易安全、有保障，骗子以**手续费高等理由**，引导受害人脱离正规平台私下交易，实则是为了规避平台的监管。

“论文代写”“私家侦探”

骗子声称可以提供**论文代写、私家侦探等特殊服务**，事实上，这些都是违法服务，**一定要谨慎面对！**

请牢记

网络交易请选择正规平台，严格遵循官方交易流程，警惕虚假网站和钓鱼链接，切勿脱离平台直接转账汇款！

07

冒充领导熟人等特定身份诈骗

易受骗群体：行政单位、企事业单位等群体

常见诈骗套路

▶ 套路一：冒充老板身份

此类诈骗主要针对企业财会人员。骗子仿冒或盗用公司老板QQ、微信、钉钉等社交账号，将财务人员拉入虚假“公司内部群”，编造支付“合同保证金、业务款”等理由，要求财务人员向指定银行账户转账汇款。



套路二：冒充领导身份

骗子通过非法渠道获取受害人手机通讯录及相关信息，冒充“领导”主动添加好友，以“暖心关怀”骗取信任，随后以不便出面等理由，要求受害人代为转账，并以时间紧迫、机会难得等借口不断催促。



▶ 套路三：冒充熟人身份

骗子通过非法渠道窃取受害人身份信息，随后冒充亲属、好友等身份联系受害人，向其提出转账汇款的要求，转账理由多种多样，如急需用钱、操作不便、账号异常等。



典型案例

某日，赵先生的微信上收到了一条好友申请，对方备注是自己公司的李经理，赵先生便通过了好友验证。随后，“李经理”发消息称这是他的私人微信，一位领导找自己借钱，要立即将10万元钱转给领导，为避免“麻烦”，请赵先生代为操作，同时还发送了一张转账成功的截图，声称已向赵先生的账户转账10万。在“李经理”的不断催促下，赵先生没多想，便向“李经理”提供的银行账号中转账10万元。然而，赵先生迟迟没有收到“李经理”转过来的10万元，便电话联系李经理询问情况，没想到李经理根本不知道此事，这时赵先生才发现自己被骗。



反诈高频词

“转账截图”“打款回执单”

骗子为了骗取受害人信任，往往会出现所谓的汇款截图，声称已向账户转账但银行到账有延迟，请求受害人先行支付。事实上，利用PS技术可以轻易处理此类图片，一定要以实际到账为准。

“银行年检”“税务稽查”

这些都是骗子编造的理由，目的就是与企业财会人员建立联系，随后将其拉至虚假的聊天群中，进而实施诈骗。

“急需用钱”“不方便电话”

骗子为了避免受害人进行核实，往往会编造各种理由，营造紧急情形，催促受害人尽快转账。

请牢记

凡是遇到领导、熟人要求转账汇款的情形，务必通过电话或当面核实确认，千万不能随意转账，避免遭遇财产损失！

08

网络游戏产品虚假交易诈骗

易受骗群体：喜爱网络游戏的群体、未成年群体/学生群体

作案手法

▶ 第一步：

骗子通过社交媒体、游戏公屏及官方交易平台等渠道，发布买卖游戏账号、装备或点卡等广告，或是发布可以免费获取游戏装备、参加抽奖资格等广告，借机锁定目标。



第二步：



骗子诱导受害人在虚假的游戏交易平台进行交易，随后以“账号异常”“操作失误”等理由，要求受害人缴纳各种费用，或是要求受害人在虚假链接中填写自己的银行卡信息及手机验证码信息，直接转走卡内资金，还有一些骗子会要求受害人直接转账汇款，从而完成诈骗。

典型案例

某日，马某在家玩网游时，收到了陌生玩家的私信，称想要高价购买马某的游戏账号。两人添加好友并商定好价格后，对方指导马某点击链接进入一个叫“快乐售”的平台完成交易。交易完成后，马某发现自己账户里的钱无法提现，平台客服说马某的银行卡号填写错误，导致账号被冻结，随后以缴纳保证金、刷流水解冻等名义，诱骗马某向指定账户多次转账，共计被骗4万元。



反诈高频词

“低价出售”“高价收购”

低价出售、高价收购游戏账号、装备、游戏币等，都是骗子精心设计的诱饵，目的就是吸引潜在受害人上钩。

“升级代练”

骗子声称可以低价代练游戏账号等级，从而骗取受害人的游戏账号密码以及代练费用，等收到钱款后，便会将其账号中的财物洗劫一空。

“送皮肤”“抽奖品”

骗子发布赠送游戏装备或免费抽礼品等消息搭识未成年受害人，后以账号异常被冻结为由，诱导、恐吓未成年受害人使用家长手机转账汇款。提示家长一定要保管好自己的支付密码，切勿随意向孩子透露，避免被骗子利用实施诈骗。



请牢记

需在正规平台进行网络游戏产品交易，切勿随意泄露自己的游戏账号信息以及银行账户信息，凡是私下交易均存在被骗风险！

09 冒充公检法及政府机关诈骗

易受骗群体：女性

作案手法

▶ 第一步：

骗子通过非法渠道获取受害人身份信息，**冒充公检法机关工作人员**拨打受害人电话，以受害人涉嫌重大案件为由，对其进行威逼、恐吓，要求配合处理。



第二步：

骗子会向受害人发送**虚假的警官证、通缉令、逮捕证等法律文书**，或是让受害人登录**虚假的内部网址**查看涉案信息，以此激化受害人恐慌情绪。



▶ 第三步：

骗子以洗清嫌疑为由，要求受害人将名下所有资金转到指定的“**安全账户**”，或是要求受害人下载具有屏幕共享功能的会议软件，借机窃取受害人银行卡信息以及手机验证码等信息，直接转走卡内资金，从而达到诈骗目的。



典型案例

某日，市民王女士接到了一个陌生电话，对方自称是北京市公安局民警，说王女士名下有一张银行卡涉嫌参与洗钱犯罪，要求其配合调查。王女士表示完全不知情，并焦急的询问“民警”应当如何处理，对方称该洗钱团伙已被武汉市公安局抓获，随后将电话转接至武汉市公安局立案侦查处，转接后，电话那头的“刘警官”要求王女士找一个没有人的地方，添加其好友在线办理案件。通话过程中，对方要求王女士如实告知名下所有银行账户信息，并且提供收到的手机验证码。为配合民警办案，洗清自己的嫌疑，王女士完全照做，直到银行卡内的20万元全被转走，才意识到自己可能被骗。



反诈高频词

“涉嫌犯罪”“在线办案”

骗子利用了受害人对于公检法等权威机关的敬畏心理，虚构涉嫌**参与洗钱、诈骗等犯罪事件**，以不配合处理便会实施拘捕为由，激化受害人恐慌情绪。

“通缉令”“逮捕证”“警官证”

为骗取受害人信任，骗子还会向其发送虚假的“**通缉令”“逮捕证”“警官证**”等法律文书，但事实上，公检法机关不会通过电话、短信、网络等形式办案，也不会通过互联网发送相关材料。

“绝密案件”“禁止外传”

骗子会以**案件涉密、不能泄露**为由，诱导受害人至宾馆等**独立封闭空间**，有些骗子甚至会将受害人的电话设置为呼叫转移，以此阻断其与外界的联系。

“转接电话”

一些骗局中，骗子会先**冒充客服人员**，虚构受害人身上的异常事件，如**大额转账、异常订单**等，随后将电话转接至“**公安机关**”。事实上，公检法机关不存在部门之间相互转接电话的情形。

“安全账户”“资金清查”

骗子会以**需要资金清查**为由，要求受害人配合转账至安全账户。请注意，公检法机关从未设立所谓的“**安全账户”“验资账户**”，更不会以配合办案为由要求个人转账汇款。

请牢记

凡是自称公检法机关工作人员，以涉嫌犯罪，需要洗脱嫌疑、自证清白为由，要求转账汇款至“安全账户”的，都是诈骗！

10

裸聊敲诈



易受骗群体：单身男性

作案手法

▶ 第一步：

骗子通过短信、社交媒体及短视频平台等多种渠道发布色情诱导信息，或是线下发送色情小卡片，引导受害人添加好友。



第二步：

骗子通过预先录制的美女裸聊视频或通过美颜、变声等技术手段欺骗受害人，诱导其进行裸聊，并偷偷录制不雅视频、照片。



▶ 第三步：

骗子以“帮我点赞”“增加人气”等为由，引导受害人下载木马APP，并打着“直播”“视频”等幌子诱骗其开启通讯录、实时位置、短信等权限。



第四步：

在获取受害人的“不雅视频”和“通讯录”后，骗子便会以群发受害人不雅视频、照片为威胁，不断向其索要钱财。



典型案例

赵某到外地出差，夜晚在酒店中玩手机时，收到了陌生女子的QQ好友申请，通过后赵某便与对方开展暧昧聊天。随后，对方提出想与赵某视频，并且要求“坦诚相见”，于是赵某赤身裸体拨通视频，屏幕那头的女子直接脱起了衣服，视频只接通了几秒就被挂断。对方发消息称在QQ视频不安全，要求赵某点击链接下载一款直播APP，称可以在里面继续视频。赵某下载后发现软件无法使用，正想询问情况，对方却一改温柔语气，恐吓赵某要求转账汇款，否则就把赵某的不雅视频发给其手机通讯录里的好友。无奈之下，赵某只能按照对方要求，先后共计转出48万元。



反诈高频词

“坦诚相见”

骗子通常会主动提出要“坦诚相见”，不少人以为自己艳福不浅，不曾想反倒被骗子截取自己的私密视频、照片。即使没有“坦诚相见”，但视频中露出的脸部同样可能被骗子截取，利用PS技术处理成裸照。

“破财免灾”

骗子以散播不雅视频、照片为由索要钱财，一旦受害人为了平息事件选择“破财免灾”，便会不断被骗子敲诈勒索，直至掏空钱包。

请牢记

色字头上一把刀，割破面子和钱包。远离网络不良行为，切勿因寻求刺激而落入“桃色陷阱”。

《反电信网络诈骗法》

将如何影响你的生活？

多办几张银行卡？

《中华人民共和国反电信网络诈骗法》规定

- 开立银行账户、支付账户不得超出国家有关规定限制的数量。
- 对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户。



多办几张电话卡？

《中华人民共和国反电信网络诈骗法》规定

- 办理电话卡不得超出国家有关规定限制的数量。
- 对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。



售卖个人信息帮转账？

《中华人民共和国反电信网络诈骗法》规定

- 任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助：
 - 出售、提供个人信息；
 - 帮助他人通过虚拟货币交易等方式洗钱；
 - 其他为电信网络诈骗活动提供支持或者帮助的行为。



制贩猫池、GOIP设备？

《中华人民共和国反电信网络诈骗法》规定

- 任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件：
 - 电话卡批量插入设备；
 - 具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；
 - 批量账号、网络地址自动切换系统，批量接收提供短信验证、语音验证的平台；
 - 其他用于实施电信网络诈骗等违法犯罪的设备、软件。



买卖、出租、出借“两卡”？

《中华人民共和国反电信网络诈骗法》规定

- 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等，不得提供实名核验帮助；不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。
- 对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者，以及因从事电信网络诈骗活动或者关联犯罪受过刑事处罚的人员，可以按照国家有关规定记入信用记录，采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。



到境外参加涉诈活动？

《中华人民共和国反电信网络诈骗法》规定

- 对前往电信网络诈骗活动严重地区的人员，出境活动存在重大涉电信网络诈骗活动嫌疑的，移民管理机构可以决定不准其出境。
- 因从事电信网络诈骗活动受过刑事处罚的人员，设区的市级以上公安机关可以根据犯罪情况和预防再犯罪的需要，决定自处罚完毕之日起六个月至三年以内不准其出境，并通知移民管理机构执行。



《反电信网络诈骗法》

十五日以下拘留一至十倍的罚款



从事电信网络诈骗活动尚不构成犯罪的

第三十八条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。

前款行为尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款；没有违法所得或者违法所得不足一万元的，处十万元以下罚款。

非法制造、买卖、使用GOIP、猫池等设备， 为实施电信网络诈骗活动提供支持或帮助

第十四条 任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件：

- (一)电话卡批量插入设备；
- (二)具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；
- (三)批量账号、网络地址自动切换系统，批量接收提供短信验证、语音验证的平台；
- (四)其他用于实施电信网络诈骗等违法犯罪的设备、软件。

第二十五条 任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助：

- (一)出售、提供个人信息；
- (二)帮助他人通过虚拟货币交易等方式洗钱；
- (三)其他为电信网络诈骗活动提供支持或者帮助的行为。

第四十二条 违反本法第十四条、第二十五条第一款规定的，没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款；没有违法所得或者违法所得不足五万元的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。

提供实名核验帮助假冒身份开卡开户

第三十一条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等，不得提供实名核验帮助；不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

第四十四条 违反本法第三十一条第一款规定的，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款；没有违法所得或者违法所得不足二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。

牢记

“三不一多”原则，
守好您的钱袋子！
未知链接不点击，
陌生来电不轻信
个人信息不透露，
转账汇款多核实

96110是全国反诈预警劝阻专线：

当您接到96110的来电，说明您或您的家人可能正在遭遇电信网络诈骗，请一定要及时接听并配合民警开展见面劝阻工作。

如有疑问，可拨打96110进行咨询！不幸被骗，请立即拨打**110**报警求助！