pluxee

中国人民银行

中国支付清算协会
Payment & Clearing Association of China

反诈是门必修课，筑牢防线守好责

2025 年全民反诈在行动

宣传手册

上海普乐斯支付有限公司

二〇二五年六月

目录

一、 深入贯彻学习习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示精神

习近平总书记对打击治理电信网络诈骗犯罪活动高度重视，多次作出重要指示批示。2021 年 4 月 6 日，习近平对打击治理电信网络诈骗犯罪工作作出重要指示强调，打击治理电信网络诈骗活动“要坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势，为建设更高水平的平安中国、法治中国作出新的更大的贡献”。2021 年 5 月 1 日,习近平总书记再次作出重要批示。2021 年 12 月 6 日,中央政治局就建设中国特色社会主义法治体系进行第三十五次集体学习,习近平总书记在主持学习时指出:“对人民群众反映强烈的电信网络诈骗、新型毒品犯罪和‘邪教式’追星、‘饭圈’乱象、‘阴阳合同’等娱乐圈突出问题,要从完善法律入手进行规制,补齐监管漏洞和短板,决不能放任不管。” 习近平总书记的这些重要指示批示从指导思想、基本原则、具体举措、关键环节、制度构建等方面提出明确要求,为打击治理电信网络诈骗犯罪工作指明了方向,提供了根本遵循。

2021 年 4 月 9 日，全国打击治理电信网络新型违法犯罪工作电

视电话会议在京召开。会议强调，要深入贯彻落实习近平总书记重要指示精神和党中央决策部署，坚持“四专两合力”总体思路，以落实反电信网络诈骗法和中办国办《关于加强打击治理电信网络诈骗违法犯罪工作的意见》为契机，以减少人民群众财产损失为目标，全面加强打防管控各项措施，推动打击治理工作不断迈上新台阶，确保电信网络诈骗犯罪多发高发态势得到有效遏制，全力夺取反诈人民战争新胜利，以实际行动彰显主题教育成效。

2022 年，全国公安机关认真贯彻落实习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示精神，落实中共中央办公厅、国务院办公厅《关于加强打击治理电信网络诈骗违法犯罪工作的意见》部署要求，按照“四专两合力”总体工作思路，持续向电信网络诈骗犯罪发起凌厉攻势，截至 11 月底，全国共破获电信网络诈骗案件 39.1 万起，同比上升 5.7%，抓获犯罪嫌疑人数同比上升 64.4%，立案数同比下降 17.3%，造成财产损失数额同比下降 1.3%，实现了“两升两降”工作目标，打击治理电信网络诈骗犯罪取得显著成效。

会议指出，要进一步加大打击力度。要坚持依法严打方针，深入开展“云剑”“断卡”“断流”“拔钉”等专项行动，集中攻坚一批大案要案，坚决打掉犯罪分子的嚣张气焰。要联合挂牌督办一批重大案件，公开曝光一批典型案例，形成强大震慑。要持续组织区域会战，发起集群战役，严厉打击引流推广、转账洗钱、技术开发等犯罪团伙，坚决切断犯罪关键链条。要加强国际执法合作，打击摧毁境外诈骗窝点，缉捕境外重大在逃人员。要及时研究制定出台司法解释和法律适用指

导意见，依法从严惩处电信网络诈骗及其关联违法犯罪。

会议强调，要进一步织密防护网络。要坚持关口前移、预防为先，综合采取多种防范措施，最大限度预防案件发生、减少群众财产损失。要加强技术反制，优化诈骗电话、短信、网址、域名动态封堵和处置机制，完善涉诈资金快速止付、冻结和延迟到账机制。要加强预警劝阻，及时发现潜在受害群众，分级分类实施预警劝阻，建立精准预警劝阻工作机制，深化反诈劝阻专线（96110）、预警劝阻短信系统（12381）建设，及时开展电话预警和见面劝阻。要加强资金返还，坚持“依法、精准、及时”原则，最大力度追缴涉诈资金，最大限度返还被骗财产。要加强宣传防范，建立全方位、广覆盖的反诈宣传体系，努力营造全社会反诈浓厚氛围，不断增强群众防骗意识和识骗能力。

会议指出，要进一步抓好源头管控。要落实属地主体责任，聚焦涉诈重点人员和黑灰产业，把源头管控各项工作抓实抓细抓到位。要加强出入境证件申办审查，对涉诈人员、出境作案嫌疑人员落实法定不准出境措施，严打偷渡等非法出境活动。要加大教育劝返力度，敦促出境作案人员尽快回国投案自首。重点地区要加强综合整治、专项整治、依法整治，并优化产业布局，拓宽就业渠道，教育引导广大群众树立正确的价值观、财富观，营造良好社会风气。对出境务工、旅游、留学人员，要针对性开展宣传教育，提醒广大民众高度警惕和识别海外“高薪”招聘虚假信息，避免落入电信网络诈骗、网络赌博等违法陷阱，危害生命财产安全。

会议强调，要进一步深化行业治理。要认真贯彻落实反电信网络

诈骗法，加大治理力度，堵塞监管漏洞，全力挤压涉诈违法犯罪活动空间。要聚焦切断涉诈“资金链”，出台更加严格的管理规定，督促金融机构完善异常账户和可疑交易监测机制，落实涉诈资金管控措施，努力实现被骗资金拦得住、追得回、返得了。要深入开展“断卡”专项整治行动，组织开展电信行业专项督导检查，杜绝滥发新卡、批量注册网络账号、群发诈骗短信等行业乱象。要组织开展涉诈网络黑灰产专项整治，建立网络巡查监测机制，及时发现、快速处置网上涉诈有害信息。要健全行业主管部门、企业、用户三级责任制，建立电信网络诈骗严重失信主体名单制度，及时约谈、督导、曝光问题突出企业，实现更佳惩治效果。

会议要求，要进一步强化组织推进。要加强统筹组织、协调推进，确保到年底基本形成与打击治理电信网络诈骗犯罪新形势新任务相适应的工作机制和工作格局。要推动各级党委和政府把反诈工作摆在突出位置来抓，统筹力量资源，加大保障力度，加强“四专两合力”建设，努力构建党委领导、政府主导、部门主责、行业监管、有关方面齐抓共管的整体格局。要牢固树立“一盘棋”思想，密切配合、通力合作，加强督导检查，狠抓责任落实，广泛动员人民群众和社会各界积极参与打击治理工作，做到全民反诈、全社会反诈。

二、读懂《中华人民共和国反电信网络诈骗法》

1、总则

《中华人民共和国反电信网络诈骗法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十六次会议于 2022 年 9 月 2 日通过，自 2022 年 12 月 1 日起施行。全文共七章 50 条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任、附则。

《反电信网络诈骗法》明确了电信网络诈骗的定义，即“以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。”该法为预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全提供法律保障。

2、电信治理

- 电信业务经营者应当依法全面落实电话用户真实身份信息登记制度。
- 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。
- 电信业务经营者对监测识别的涉诈异常电话卡用户应当重新进行实名核验，根据风险等级采取有区别的、相应的核验措施。对未按规定核验或者核验未通过的，电信业务经营者可以限制、暂停

有关电话卡功能。

◆ 电信业务经营者建立物联网卡用户风险评估制度，评估未通过的，不得向其销售物联网卡;严格登记物联网卡用户身份信息;采取有效技术措施限定物联网卡开通功能、使用场景和适用设备。

3、金融治理

银行业金融机构、非银行支付机构为客户开立银行账户、支付账户及提供支付结算服务，和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等被用于电信网络诈骗活动。

- 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。
- 银行业金融机构、非银行支付机构应当建立开立企业账户异常情形的风险防控机制。
- 银行业金融机构、非银行支付机构应当对银行账户、支付账户及支付结算服务加强监测，建立完善符合电信网络诈骗活动特征的异常账户和可疑交易监测机制。
- 银行业金融机构、非银行支付机构应当按照国家有关规定，完整、准确传输直接提供商品或者服务的商户名称、收付款客户名称及账号等交易信息，保证交易信息的真实、完整和支付全流程中的一致性。

4、互联网治理

电信业务经营者、互联网服务提供者为用户提供下列服务，在与用户签订协议或者确认提供服务时，应当依法要求用户提供真实身份信息，用户不提供真实身份信息的，不得提供服务:

- 提供互联网接入服务；
- 提供网络代理等网络地址转换服务；
- 提供互联网域名注册、服务器托管、空间租用、云服务、内容分发服务；
- 提供信息、软件发布服务，或者提供即时通讯、网络交易、网络游戏、网络直播发布、广告推广服务。

互联网服务提供者对监测识别的涉诈异常账号应当重新核验，根据国家有关规定采取限制功能、暂停服务等处置措施。

互联网服务提供者应当根据公安机关、电信主管部门要求，对涉案电话卡、涉诈异常电话卡所关联注册的有关互联网账号进行核验，根据风险情况，采取限期改正、限制功能、暂停使用、关闭账号、禁止重新注册等处置措施。

5、综合措施

- ◆ 金融、电信、网信部门依照职责对银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者落实本法规定情况进行监督检查。有关监督检查活动应当依法规范开展。
- ◆ 电信业务经营者、银行业金融机构、非银行支付机构、互联网服

务提供者应当对从业人员和用户开展反电信网络诈骗宣传，在有关业务活动中对防范电信网络诈骗作出提示，对本领域新出现的电信网络诈骗手段及时向用户作出提醒，对非法买卖、出租、出借本人有关卡、账户、账号等被用于电信网络诈骗的法律责任作出警示。

◆ 对经设区的市级以上公安机关认定的实施买卖、出租、出借银行账户、支付账户，假冒他人身份或者虚构代理关系开立银行卡的单位、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。

6、法律责任

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。

（1）银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的，由有关主管部门责令改正，

- 未落实国家有关规定确定的反电信网络诈骗内部控制机制的;
- 未履行尽职调查义务和有关风险管理措施的;
- 未履行对异常账户、可疑交易的风险监测和相关处置义务的;
- 未按照规定完整、准确传输有关交易信息的。

情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；**情节严重的**，处五十万元以上五百万元以下罚款，并可以

由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。

（2）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，违反上述规定，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。

三、个人账户的使用与保护

1、支付工具的使用

※ 支付工具使用注意事项

- 开通余额变动提醒功能，及时发现非本人操作风险。
- 各种账号的登录密码尽量使用不同数字和字母大小写的组合。
- 支付工具应从官方网站下载，不要随意扫描二维码下载。
- 登陆支付工具时将“自动登录”等选项取消。

※ 电子智能防护工具的使用

- 根据要求安装密码安全控件，保护密码安全。
- 设置安全保护问题防止盗号。
- 安装正规的防病毒软件，阻拦病毒、钓鱼网站等。
- 使用智能密码钥匙、动态令牌设备、短信验证码、动态挑战应答等身份认证方式。
- 设定消费限额。
- 按照自己的实际需求对各类认证方式进行限额设置。
- 设定消费限额，避免在信息泄露时遭受更大损失。
- 关闭支付工具的小额免密支付功能。

※ 置身安全环境

- 尽量使用本人的电脑、手机、电话等办理业务。
- 不使用公共场所中的电脑登陆网银等银行、支付类网站。

※ 妥善保管个人支付信息

- 手机做好安全防护，防止恶意程序入侵。
- 对 U 盾、手机动态口令等信息做好保护，不要向他人泄露。
- 不在不明链接中填写账户密码、动态验证码等支付信息。
- 发现账户异常，立即直接与银行联系。

2、安全提示

※ 妥善保管

妥善保管身份证、银行卡、网银 U 盾、手机等，不借给他人使用；不随意丢弃刷卡交易凭条；不向任何人发送带有银行卡信息和支付信息的图片等。

※ 有效防范

不点击短信、网络聊天工具或网站中的可疑链接，不登陆非法网站；慎扫不明来历二维码；不轻信陌生电话；使用资金较少的银行卡用于网络支付等。

※ 及时报警

如个人相关信息泄露或银行卡被盗刷，应尽快挂失银行卡，并及时向公安机关报案，提供有关证据配合公安机关开展案件调查。

3、出租、出借、出售账户的危害

“实名不实人”的卡，不但被犯罪分子用来搞电信诈骗，还会用来搞网络贩毒、网络赌博等犯罪。据新闻报道，每年网络赌博流出资金就达万亿级别，而这些钱大部分都是通过买卖的银行卡、对公账户

或者第三方支付账户走账，难以追查和打击。

非法买卖的银行卡、身份证等可能被用于洗钱、逃税、诈骗、送礼和开店刷信用等行为，扰乱了正常的社会秩序。同时，卡内存储了很多个人信息，如果贪图小便宜出售自己名下的卡，有可能被收卡人用来从事非法活动，给自己带来巨大的法律风险，甚至承担刑事责任。一旦所售卡出现信用问题，最终都会追溯到核心账户，导致个人信用受损，甚至承担连带责任。

四、账户风险防控

1、银行卡使用安全

- 树立安全用卡意识。银行发放的用卡提示，要认真阅读。领到信用卡后，应该立即在卡背面的签署栏上写下自己的名字。在为银行卡设置密码时，尽量不要使用简单的数字和容易被猜到的密码，并要定期更换。
- 在使用自助机具办理业务时，要留意是否有可疑的装置。刷卡时，要注意一下旁边是否有人偷看，同时用手或身体进行遮挡，保护自己的密码不会被泄露。
- 不管是消费还是转账等，都会产生交易凭条，千万不要随意一扔了事，应及时撕碎扔掉或者妥善保存。
- 刷卡时务必不要让银行卡离开视线，尤其不能把银行卡转交服务员或他人代刷，以免被不法分子盗取卡片信息，制作“克隆卡”。
- 尽量把银行卡和身份证分开放，避免发生银行卡和身份证同时丢失而被盗刷的可能。
- 可以给银行卡开通消费金额短信提醒功能（可能需付费），当消费后会第一时间将消费情况通过短信通知你。要注意的是，在申办银行卡时务必正确预留本人的手机号码，如果手机号码发生变动，也要到银行进行更新。这是通过电话申请冻结账户的必要条件。
- 若一旦发现本人银行卡被“盗刷”，应立即致电银行客服热线冻结账户，将损失降低到最小。若是担心记不住这些客服号码，可以

将已有的银行卡的银行客服电话存在手机里或记在一个笔记本上。

2、使用电子银行的注意事项

- 为了安全起见，申请开办全功能电子银行业务时，一般会要求本人携带有效身份证件及银行卡或存折到银行营业网点办理。
- 可以自主决定是否申请注册电子银行业务，自主选择注册电子银行的渠道种类，如网上银行、手机银行、电话银行等。
- 对涉及收费的电子银行业务，在最终提交银行业务处理系统前，应了解、知晓相关收费标准或具体收费金额，以便自主决定是否继续操作该项业务。
- 电子银行交易指令一经确认、执行，不能以与第三方发生纠纷为由要求变更或撤销。通过电子银行渠道办理相关交易后，可以在规定时限内到银行营业网点补登存折或补打交易明细。
- 电子银行使用者若发生数字安全证书丢失或密码泄露等情况，应尽快与银行联系，办理挂失补办手续。
- 如对电子银行服务有疑问、建议或意见，可拨打银行客服热线、登陆银行官方网站或到银行营业网点进行咨询或投诉。
- 如不再继续使用电子银行业务，可向银行申请终止相关电子银行服务，但在申请终止相关电子银行服务之前使用该服务的，仍应当遵守相关调整内容。

3、风险防控措施

为保护人民群众财产安全，各类金融机构积极推行多项账户风险防控措施，加强账户管理，防范打击违法犯罪活动。

1）客户身份识别

金融机构在与客户建立业务关系或者为客户提供规定金额以上的现金汇款、现钞兑换、票据兑付等一次性金融服务时，应当要求客户出示真实有效的身份证件或者其他身份证明文件，进行核对并登记。

客户由他人代理办理业务的，金融机构应当同时对代理人和被代理人的身份证件或者其他身份证明文件进行核对并登记。

与客户建立人身保险、信托等业务关系，合同的受益人不是客户本人的，金融机构还应当对受益人的身份证件或者其他身份证明文件进行核对并登记。

金融机构不得为身份不明的客户提供服务或者与其进行交易，不得为客户开立匿名账户或者假名账户。

金融机构对先前获得的客户身份资料的真实性、有效性或者完整性有疑问的，应当重新识别客户身份。

任何单位和个人在与金融机构建立业务关系或者要求金融机构为其提供一次性金融服务时，都应当提供真实有效的身份证件或者其他身份证明文件。

金融机构通过第三方识别客户身份的，应当确保第三方已经采取符合本法要求的客户身份识别措施；第三方未采取符合本法要求的客

户身份识别措施的，由该金融机构承担未履行客户身份识别义务的责任。

金融机构进行客户身份识别，认为必要时，可以向公安、工商行政管理等部门核实客户的有关身份信息。

金融机构应当按照规定建立客户身份资料和交易记录保存制度。

在业务关系存续期间，客户身份资料发生变更的，应当及时更新客户身份资料。

客户身份资料在业务关系结束后、客户交易信息在交易结束后，应当至少保存五年。

金融机构破产和解散时，应当将客户身份资料和客户交易信息移交国务院有关部门指定的机构的事项。

2）账户分级管理

银行应按照“了解你的客户”原则，采用科学、合理的方法对存款人进行风险评级，根据存款人身份信息核验方式及风险等级，审慎确定银行账户功能、支付渠道和支付限额，并进行分类管理和动态管理。银行可通过柜面、远程视频柜员机和智能柜员机等自助机具、网上银行和手机银行等电子渠道为开户申请人开立个人银行账户。银行通过自助机具和电子渠道提供个人银行账户开立服务的，开户申请人只能持居民身份证办理。

在现有个人银行账户基础上，增加银行账户种类，将个人银行账户分为Ⅰ类银行账户、Ⅱ类银行账户和Ⅲ类银行账户（以下分别简称

Ⅰ类户、Ⅱ类户和Ⅲ类户）。银行可通过Ⅰ类户为存款人提供存款、购买投资理财产品等金融产品、转账、消费和缴费支付、支取现金等服务。银行可通过Ⅱ类户为存款人提供存款、购买投资理财产品等金融产品、限定金额的消费和缴费支付等服务。银行可通过Ⅲ类户为存款人提供限定金额的消费和缴费支付服务。银行不得通过Ⅱ类户和Ⅲ类户为存款人提供存取现金服务，不得为Ⅱ类户和Ⅲ类户发放实体介质。

3）存量账户清理

存量人民币银行个人结算账户清理是指银行对存量的个人银行卡进行销户、暂停使用、封卡操作的一种处理方式，主要清理范围包括：单家银行个人账户数量超过了Ⅰ类、Ⅱ类和Ⅲ类银行账户的开户数量上限，或者个人银行卡账户属于长期未动账的状态。

具体清理范围视各银行公告而定。

五、教你防范诈骗新手法

当前，电诈犯罪形势严峻复杂。在电诈犯罪链条中，电诈分子往往将诈骗钱款分散转入多个层级的他人银行账户中，隐蔽诈骗钱款来源，逃避公安机关追查。除此之外，电诈分子还使用他人互联网账号，或冒用身份向亲友骗钱、发布违规广告、推广引流信息……为完成上述违法犯罪行为，电诈分子大肆收购、获取“两卡”和个人信息，发展“跑分”洗钱、推广引流等网络黑灰产，利用多种手段利诱蒙骗群众成为电诈“工具人”。面对花样百出、防不胜防的诱骗手法，为了提高公众反欺诈意识和能力，切实保护广大人民群众的财产安全乃至人身安全，应当学习生活中关于诈骗的防范知识，提高警惕。

1、出租、出借“两卡”

- “两卡”是指手机卡、银行卡。手机卡包括日常使用的四大运营商的电话卡、虚拟运营商的电话卡以及物联网卡；银行卡包括个人银行卡、对公账户及结算卡、非银行支付机构账户即支付宝、微信等第三方支付平台。手机卡可被用来拨打诈骗电话或群发诈骗短信，身在境外的犯罪分子还会利用 GOIP 设备，远程操控境内手机拨出诈骗电话，这种电话一般不会被标记为境外电话，具有极强的迷惑性。
- 常见形式：

（1）非法买卖、出租、出借电话卡、银行账户支付账户和互联网账号等，并以此牟利。

（2）非法购买、使用 Goip、Voip 等虚拟拨号设备，为境外诈骗分子搭设通话转接通道。

【典型案例】 老刘于 4 年前办理了一张银行卡，历经几次银行系统升级和卡片换代后，该张银行卡的使用频率不高，被搁置一旁。经邻居介绍，老刘加入了一个名叫“小王开卡”的微信群，通过群友牵线，银行卡很快找到买主。之后被他人用于实施电信网络诈骗。案发后，老刘因涉嫌帮助信息网络犯罪活动罪被公安机关刑事拘留。

[国家反诈中心提醒] 不论何种情况，在面对不法分子提出租借、收购手机卡、银行卡等要求时，一定要保持清醒头脑，法律不会因为你是受骗者而减轻惩罚。

2、“跑分”

- 在电诈实施过程中，诈骗分子为了保证自身和赃款的安全，需要把诈骗得来的钱“洗一洗”才能转入自己的账户，这个过程被称为“跑分”，大量租借或购买来的银行卡，就是“洗白”的工具。
- 常见形式：

使用自己或他人银行账户、第三方支付账户，为诈骗分子提供非法资金转移的“跑分”洗钱行为。

【典型案例】 2021 年 2 月至 4 月期间，被告人沈某某为非法获取佣金，招募被告人毕某某、来某某、李某某等人，组成收款转账团伙，并负责管理。上述被告人在明知账户接收的钱款来路不明，可能系电信网络违法犯罪所得的情况下，仍根据安排，提供各自名下银行卡及

支付宝、微信账户作为收款工具，并将收到的钱款从火币网等处购买虚拟币 USDT，再转入指定账户，帮助转移赃款，从而非法获利（俗称“跑分”）。2021 年 3 月，被害人叶某遭电信网络诈骗，被骗的部分钱款经上述部分被告人的账户流转。

[国家反诈中心提醒] 千万不要轻易被所谓“高额利润”诱惑，充当“跑分客”，结果就是自毁前程，务必引以为戒！

3、转账洗钱

- 围绕洗钱，电诈分子会编造出多种冠冕堂皇的理由引人上钩：高薪招聘兼职采购员；为了避税，需要兼职者持银行卡在工作人员配合下面对面刷脸转账;销售有业绩压力,希望代为转账冲业绩；因财务问题，想找人帮忙转账刷银行流水；高折扣慢充话费、电费、燃气费……
- 常见形式：

  （1）诈骗分子以高薪为诱饵招聘兼职“采购员”将涉诈资金转入“采购员”账户并要求取现，再以各种理由将购买实物或现金取走的行为。

  （2）诈骗分子冒充扶贫资金发放机构，以需要刷流水包装账户才能放款为由，要求扶贫金申请人出借或邮寄银行账户和密码，甚至帮助刷脸辅助验证来转移非法资金的行为。

  （3）诈骗分子以贷款账户需要刷流水包装账户才能放款为由，要求贷款者出借或邮寄银行账户和密码甚至帮助刷脸辅助验证来转

移非法资金的行为。

【典型案例】“您好，本基金由国务院扶贫办进行发放，全程无须缴纳任何费用……”今年 2 月，60 多岁的刘某突然收到这样一条短信。刘某根据短信链接加对方为微信好友后，对方自称是政府部门工作人员，刘某被确定为帮扶对象。之后，对方称要将刘某包装成“入不敷出”的样子，需要大量的银行流水以及最终清零的账户作为申请项。刘某在对方要求下先后将收到的多笔汇款汇到指定账户。很快，他的账户显示被冻结。当民警找上门时，他如梦方醒。

[国家反诈中心提醒] 规范收款流程，拒绝来历不明的货款；不随意提供银行账户或收款二维码；账户异常及时报警，聊天、交易记录保留好。

4、吸粉引流

- “引流”是诈骗开始的“前端服务”。受害人被各类“引流”方式诱导加入指定微信群、QQ 群或其他群组，而后被诈骗。其中，拉人进群环节费时费力，且不利于“隐蔽幕后”，所以许多电诈分子招募他人成为“引流”工具人。

  “线下引流”多以“扫码送礼”“支持创业”等方式出现，电诈分子在网上发布兼职广告，要求兼职人员以赠送礼品等为由吸引群众扫码进群或是拉人建群。

  “线上引流”的表现形式多为冒充客服给他人打电话并拉人进入指定聊天群。

- 常见形式：

（1）诈骗分子雇佣地推人员，印刷张贴带有二维码的涉黄小广告，引诱受害人下载涉诈 APP 实施诈骗的行为。

（2）通过传播虚假广告信息链接到微信群、朋友圈等，或是发送诈骗短信给指定电话帮助诈骗分子引流实施诈骗的行为。

（3）利用在路边赠送小礼品的方式，吸引行人扫码或者是拉人建群，帮助诈骗分子引流实施诈骗的行为。

（4）诈骗分子招募兼职“话务员”，要求以固定话术剧本，冒充客服人员拨打指定电话，并将受害者引流给诈骗分子的行为。

【典型案例】 云南陆良的丁某、吴某在微信朋友圈看到一则兼职广告，便按照要求到夜市做“地摊引流”，向不特定人群发放小礼品并将其拉进各种聊天群。丁某、吴某的行为被举报，民警很快将二人带回调查。

[国家反诈中心提醒] 如遇到邀请进群、转发可领取礼品等情况，务必要高度警惕；不要轻易添加来路不明的好友、点开来路不明的网址；年轻人特别是学生群体在网上找兼职时务必擦亮眼睛，特别警惕邀请进群、动动手指就可获得报酬的工作；受“不明人员”鼓动诱惑，批量拨打诈骗电话、群发诈骗短信或添加微信、QQ 好友，无论是否获得报酬，都涉嫌为违法犯罪活动提供帮助，将被依法追究相应责任。

5、网络黑灰产

- 网络黑灰产是指通过人工方式或者技术手段实施的操纵网络信息

内容，获取违法利益、破坏网络生态秩序的行为，包括搬运洗稿、恶意营销、撰写黑稿组成的“内容三黑”，以及黑账号、刷粉刷量推广作弊组成的 “运营三黑”。

【典型案例】 有黑产团伙流窜全国各地，在县级医保局联系称可以帮助医保局实名化数据，借此获取公民信息，非法注册账号，进行百家号账号实名、淘宝、微信小程序等注册，再将这些数据专卖获利。[国家反诈中心提醒] 提高个人意识，不轻信他人，不贪图小利。不参与网络赌博、不充当网络水军，一定要保护好个人的银行卡、身份证、不出售个人信息。警惕“黑灰产”，不“傻傻”做帮凶。

6、数字人民币诈骗

- 数字人民币是指与纸质人民币是具有同等价值特征和法偿性，由中国人民银行发行的数字形式的法定货币，具有国家信用背书，且同纸币使用场景相同，字母缩写为 e-CNY。数字人民币诈骗，是指诈骗分子以虚假的数字人民币优惠活动或保险、理财、投资等为借口，诱骗受害者进行绑卡、存钱等一系列动作，进而盗取受害者资金的违法犯罪活动。
- 常见形式：

（1）诈骗分子诱导受害人下载“微会议”、“全视通”等远程共享桌面 APP，代其进行数字人民币钱包开立、转账等操作；或者欺骗、威胁未成年人（寒暑假等节假日为高发期），诱导其使用家长信息开通数字人民币钱包，或泄露家长关键信息。

（2）诈骗分子以虚假的数字人民币优惠活动或保险、理财、投资等为借口，诱骗受害者进行绑卡、存钱等一系列动作，进而盗取受害者资金。

（3）诈骗分子以短信等线上形式发布钓鱼链接、二维码等，甚至伪造钓鱼网站，引诱客户填写关键个人信息，随后利用受害者信息开通数字人民币钱包并进行犯罪。

（4）诈骗分子冒充银行或小贷公司资质审核人员，利用客户急需贷款的心态，以“发放数字人民币贷款”“通过数字人民币钱包收取手续费”等为借口，骗取受害者关键个人信息或钱财。

（5）诈骗分子冒充公检法等公职人员，通过打电话等方式告知受害者涉及违法问题，要求受害者填写个人信息，随后利用受害者信息开通数字人民币钱包并进行资金转移。

（6）诈骗分子冒充客服以快递丢失等理由联系买家，诱骗消费者开通数字人民币钱包领取补偿金；或者以回馈客户赠送礼品等理由，要求客户提供身份证、手机号等关键个人信息，随后利用受害者信息开通数字人民币钱包并进行犯罪。

（7）诈骗分子借助微信、QQ 等社交软件群组，视频号、抖音、快手等短视频网站传播仿冒数字人民币 APP 软件，引诱受害者下载仿冒 APP，通过视频、录像等获取客户关键信息进行诈骗。

（8）诈骗分子冒充招聘人员，骗取受害者关键信息，随后利用受害者信息开通数字人民币钱包并进行犯罪；或者以工作保证金为理由，诱骗受害人进行开通数字人民币钱包、存钱、转账等一系

列操作，最终盗取资金。

【典型案例】 四川甘孜州炉霍县王某接到一陌生电话称：其在一网贷平台上有一笔高利息贷款，需要清除，否则将影响个人征信记录。王某因自身确实借有网贷，所以放松了戒备，让骗子有了可乘之机。其后，对方要求王某查询该平台上的信用额度并将该额度转至自己银行卡内。王某按照要求将”有钱花“贷款平台上的 10 万余元转到自己银行卡内。随后，对方要求王某下载“数字人民币”APP，通过“数字人民币”软件将卡内资金转入指定的数字账户内 。最终，王某被诈骗 10 万余元。

更多链接

1、反诈识诈 安全支付 | 一图读懂《中华人民共和国反电信网络诈骗法》

https://mp.weixin.qq.com/s/NbB4d9aRDIo9BzOkuWsSKw

2、国务院打击治理电信网络新型违法犯罪工作部际联席会议决定

https://www.mps.gov.cn/n2255079/n4876594/n5104076/n5104077/c7386967/content.html

3、《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发[2016]261号）

http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3154362/index.html

4、反诈识诈，安全支付——请收好这份宣传手册！

https://mp.weixin.qq.com/s?__biz=MzAwNjE1ODIxMA==&mid=2650397481&idx=3&sn=c9cfb3e562b7d6af8a094b5f3bf6490e&chksm=831cd9c4b46b50d20b8fed16d56bb453b8bb1a80735507f202d353cb0a2536ebff7a7415c4e4&scene=27

5、《中国人民银行关于改进个人银行账户服务 加强账户管理的通知》

http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/2995472/index.html

6、《中国人民银行 中国银行业监督管理委员会 公安部 国家工商总局关于加强银行卡安全管理、预防和打击银行卡犯罪的通知》

http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/2888073/index.html

7、《人民币银行结算账户管理办法》

http://www.pbc.gov.cn/zhifujiesuansi/128525/128535/128620/2898144/index.html

8、中央网信办（国家互联网信息办公室）违法和不良信息举报中心

http://www.12377.cn

9、老年人金融服务手册

http://www.pbc.gov.cn/jingrxfqy/145720/145735/4415862/index.html

10、公安机关呼吁公众提高警惕——诱骗手法“套路深” 莫成电诈“工具人”

https://mp.weixin.qq.com/s/wgcFoHZTGRsk7aOszqVyvA