目 录

《中华人民共和国反电信网络诈骗法》于9月2日经十三届全国人大常委会第三十六次会议通过，并于2022年12月1日起施行。

法律解读

反电信网络诈骗法

反电信网络诈骗法共七章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、附则等。

专家普遍认为，反电信网络诈骗法坚持以人民为中心，统筹发展和安全，立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑。

对电信网络诈骗的定义

根据《中华人民共和国反电信网络诈骗法》第二条，“本法所称电信网络诈骗，是指以非法占有为目的，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”。通常犯罪分子会冒充他人及仿冒、伪造各种合法外衣和形式，通过电话、网络和短信等方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账，如冒充公检法，伪造和冒充招工、刷单等形式进行诈骗。

法律明确打击的范围

在中华人民共和国境内实施的电信网络诈骗活动。

中华人民共和国公民在境外实施的电信网络诈骗活动。

境外的组织、个人针对中华人民共和国境内实施电信网络诈骗活动的，或者为他人针对境内实施电信网络诈骗活动提供产品、服务等帮助。

明晰防电诈工作机制及职责

国务院建立反电信网络诈骗工作机制，统筹协调打击治理工作。

地方各级人民政府组织领导本行政区域内反电信网络诈骗工作，确定反电信

网络诈骗目标任务和工作机制，开展综合治理。

公安机关牵头负责反电信网络诈骗工作，金融、电信、网信、市场监管等有关部门依照职责履行监管主体责任，负责本行业领域反电信网络诈骗工作。

人民法院、人民检察院发挥审判、检察职能作用，依法防范、惩治电信网络诈骗活动。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任，建立反电信网络诈骗内部控制机制和安全责任制度，加强新业务涉诈风险安全评估。

如何做好前端防范?

•各级人民政府和有关部门应当加强反电信网络诈的宣传，普及相关法律和知识，提高公众对各类电信网络诈骗方式的防骗意识和识骗能力。

•教育行政、市场监管、民政等有关部门和村民委员会、居民委员会应加强对老年人、青少年等群体的宣传教育，增强反电信网络诈骗宣传教育的针对性、精准性，开展反电信网络诈骗“五进”（进学校、进企业、进社区、进农村、进家庭）宣传活动。

•各单位应当加强内部防范电信网络诈骗工作，对工作人员开展防范电信网络诈骗教育。

•单位、个人应当协助、配合有关部门依照本法规定开展反电信网络诈的工作。

•新闻、广播、电视、文化、互联网信息服务等单位，应当面向社会有针对性地开展反电信网络诈骗宣传教育。

•建立预警劝阻系统，根据情况及时采取相应劝阻措施。

对电信治理的要求

1.电信业务经营者

•依法全面落实电话用户真实身份信息登记制度，承担对代理商落实电话用户实名制管理责任；

•对经识别存在异常办卡情形的，有权加强核查或者拒绝办卡；

•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；

•建立物联网卡用户风险评估制度和物联网卡的使用监测预警机制；

•规范真实主叫号码传送和电信线路出租，对改号电话进行封堵拦截和溯源核查。

2．任何单位和个人不得非法制造、买卖、提供或者使用用于实施电信网络诈骗等违法犯罪的设备、软件。

3．电信业务经营者、互联网服务提供者应当采取技术措施，及时识别、阻断非法设备、软件接入网络，并向公安机关和相关行业主管部门报告。

对金融治理要求

•银行金融机构、非银行支付机构建立客户尽职调查制度，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。

•金融、电信、市场监管、税务等有关部门建立开立企业账户相关信息共享查询系统，提供联网核查服务。

•中国人民银行统筹建立跨银行业金融支付机构、非银行支付机构的反洗钱统一检测系统；会同国务院公安部门完善反洗钱可疑交易报告制度。

•银行业金融机构、非银行支付机构应按照国家规定，完整、准确提供交易信息，保证交易信息的真实、完整和支付全流程中的一致性。

•国务院公安部门会同有关部门建立完善电诈涉案资金紧急措施制度。银行业金融机构、非银行支付机构应当配合公安机关依法采取相关措施。

对互联网治理要求

互联网服务提供者对监测识别的涉案异常账户应当重新核验。

设立移动互联网应用程序应办理许可或备案手续，为应用程序提供封装、分发服务的，应当登记、核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途。

公安机关办理电诈案件依法调取证据时，互联网服务提供者应及时提供技术支持和协助。

电信业务经营者、互联网服务提供者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。

任何单位和个人不得为他人实施电信网络诈骗活动提供支持或者帮助。

相关救济措施的要求

对电信网络诈骗案件应当加强追赃挽损，完善涉案资金处置制度，及时返还被害人的合法财产。对遭受重大生活困难的被害人，符合国家有关救助条件的，有关方面依照规定给予救助。

多办几张手机卡？不能超量

反电信网络诈骗法明确，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。

反电信网络诈骗法还规定，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。

多办几张银行卡卡？不能超量

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。

到境外参加涉诈活动？限制出境！

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。

买卖、出租、出借两卡？纳入信用记录

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、账号等功能和停止柜面业务、暂停新业务、限制入网等措施。

制贩猫池，GOIP？涉嫌违法！

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网络设备、软件。

卖个人信息？帮转账？涉嫌违法！

但可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。

用户不提供真实身份信息

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。

违反了《反电信网络诈骗法》的后果

1.刑事责任：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。

2.行政责任：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。

3.民事责任：造成他人损害的，按照《中华人民共和国民法典》等法律的规定承担民事责任。

4.惩戒措施：对经设区的市级以上公安机关认定的实施相关违法行为的单位、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。

5.限制出境：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，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，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。

会被处罚的各类行为

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。

电信业务经营者：

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；

未履行电话卡、物联网卡实名制登记职责的；

未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；

未对物联网卡用户进行风险评估,或者未限定物联网卡的开通功能、使用场景和适用设备的；

未采取措施对改号电话、虚假主叫或者具有相应功能的非法设备进行监测。

银行业金融机构、非银行支付机构：

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。

电信业务经营者、互联网服务提供者：

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；

未履行网络服务实名制职责，或者未对涉案、涉诈电话卡关联注册互联网账号进行核验的；

未按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，或者记录并留存所提供相应服务的日志信息的

未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；

未履行对涉诈互联网账号和应用程序，以及其他电信网络诈骗信息、活动的监测识别和处置义务的；

拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关违法犯罪线索、风险信息的。

反电信网络诈骗工作有关部门、单位的工作人员滥用职权、玩忽职守、徇私舞弊，或者有其他违反本法规定行为，构成犯罪的，依法追究刑事责任。

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相关帮助的违法犯罪人员，除依法承担刑事责任、行政责任以外，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等违反本法规定，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

综合自《反电信网络诈骗法》及国家反诈中心、公安部刑侦局、中国警察网、新华网、澎湃新闻等相关报道

防诈知识

牢记“六个一律”“八个凡是”

牢记六个“一律”——

只要陌生人一谈到银行卡要转账一律挂掉；

只要陌生人一谈到中奖了要先交税一律挂掉；

只要陌生人一谈到“电话转接公检法”一律挂掉；

只要陌生人一谈到让人点击不明网址链接一律挂掉；

微信不认识的人发来的链接一律不点；

一提到“安全账户”一律删掉。

牢记八个“凡是”——

凡是自称“公检法”要求汇款的都是骗子；

凡是叫你汇款到“安全账户”都是骗子；

凡是通知中奖领奖要你先交钱都是骗子；

凡是通知“家属”出事要先汇款或转账都是骗子；

凡是电话中索要银行卡信息及验证码都是骗子；

凡是让你开通网银接受检查都是骗子；

凡是自称领导要求汇款或转账都是骗子；

凡是陌生网站要登记银行卡信息都是骗子。

来源：国家反诈中心、公安部刑侦局

电信诈骗的五大套路

一、取得信任

诈骗分子会在添加好友后频繁与你聊天，让你对其产生信任，有些诈骗分子甚至会对你关怀备至，与你确定恋爱关系，让你对他（她）的信任更深。

二、怂恿投资

等到关系稳定，诈骗分子便开始怂恿你在他们自制的平台赌博或购买股票等投资产品，大多数人就会试着小额投入几笔，诈骗分子会通过后台操作，让你小赚几笔。

三、大量投入

当你尝到甜头之后，诈骗分子会声称自己已经掌握了这个平台的规律，只要跟着他（她）投资稳赚不赔。这时，你已经深信不疑，便往平台里面大量投入。

四、无法提现

等到受害人投入大量金额之后，看到平台上金额增加，准备将里面的金额提现，却发现无法提出。

五、销声匿迹

再想与对方交涉时，诈骗分子已经消失得无影无踪。等到受害人恍然大悟，发现自己上当受骗后，钞票已经进入诈骗分子的口袋了。

据中国新闻网，互联网信息领域专家何立人提醒：“诈骗团伙会请一些有心理学背景的人士帮忙研究、撰写话本，针对受害人年龄、性别、职业等特点，塑造契合其心理需求的人设，“有的甚至有受害者隐私信息，比如快递、学历、医疗等等，来增加他们话术的可信度。”（摘自：境外团伙诈骗 5.1 亿余元，2600 多人上当！谨防电信诈骗五大套路，互联网信息专家提醒……）

来源：每日经济新闻　2022-08-23

警惕海外五大高发类型电信诈骗

一、冒充使领馆工作人员实施诈骗

一些犯罪分子会冒称其是中国驻外使领馆工作人员，通过可伪装的网络电话谎称当事人有包裹需要到使馆领取、或者以使馆名义通知其证件过期，骗取当事人下载第三方软件，或者以各种理由引导当事人进行转账汇款，从而达到骗取钱财的目的。

提醒：中国驻外使领馆不会电话通知取快递或处理国内案件。自称“大使馆”“总领馆”把电话转接到某部门一定是诈骗！

二、冒充公检法工作人员实施诈骗

犯罪分子冒充公检法人员，谎称当事人涉嫌洗钱、卷入国际金融诈骗案、重大刑事案件，须冻结账户，并要求当事人将自身银行卡里所有资金转账至“安全账户”，从而达到骗取钱财的目的。

提醒：自称“公检法”让你把钱转移到“安全账户”一定是诈骗！

三、“杀猪盘”诈骗方式

犯罪分子冒充“美女”在一些交友网站上与人聊天交友，逐步建立信任后遂向当事人提出借钱请求，或者以高收益高返利方式逐步诱骗当事人参与“投资理

财”。

提醒：陌生人加好友要小心，投资理财须谨慎，警惕虚假理财投资网站、APP。

四、“虚拟绑架”（主要针对留学生）

犯罪分子通过网络等各种渠道事先获取留学生联系方式并与其联系，谎称其在国内涉案被通缉，要求其拍摄图片或视频，配合调查取证，并和家人“切断联系”。这时候利用留学生与家人失联时间，联系留学生国内亲属并谎称留学生被绑架，利用信息不对称和恐惧心理进行诈骗。

提醒：拒绝“提供个人信息”、拍摄图片或视频、“与家人、朋友”切断联系；家长接到“孩子被绑架”电话切勿盲目轻信“支付赎金”!

五、其他新型电信诈骗

犯罪分子假借新冠肺炎疫情防控、疫苗接种、反诈等事由实施诈骗，非法获取当事人个人信息，或要求当事人转账汇款。

提醒：提高防范意识，牢记“不轻信”，千万“别转账”，绝对“不汇款”!（原标题：警惕海外五大高发类型电信诈骗——驻泰国使馆防范网络电信诈骗宣传周系列提醒之二）

来源：中国驻泰使馆教育组　2022-05-29

常见的八类60种电信网络诈骗手段

一、仿冒身份欺诈：

通过冒充伪装成领导、亲友、机构单位等身份进行欺诈。

1.冒充领导诈骗：犯罪分子获知上级机关、监管部门单位领导的姓名、办公电话等有关资料，假冒领导秘书或工作人员等身份打电话给基层单位负责人，以推销书籍、纪念币等为由，让受骗单位先支付订购款、手续费等到指定银行账号，实施诈骗活动。

2.冒充亲友诈骗：犯罪分子利用木马程序盗取对方网络通讯工具密码，截取对方聊天视频资料后，冒充该通讯账号主人对其亲友或好友以“患重病、出车祸”等紧急事情为名实施诈骗。

3.冒充公司老总诈骗：犯罪分子通过打入企业内部通信群，了解老总及员工之间信息交流情况，通过一系列伪装，再冒充公司老总向员工发送转账汇款指令。

4.补助救助、助学金诈骗：冒充教育、民政、残联等工作人员，向残疾人员、学生、家长打电话、发短信，谎称可以领取补助金、救助金、助学金，要其提供

银行卡号，指令其在取款机上将钱转走。

5.冒充公检法电话诈骗：犯罪分子冒充公检法工作人员拨打受害人电话，以事主身份信息被盗用、涉嫌洗钱、贩毒等犯罪为由，要求将其资金转入国家账户配合调查。

6.伪造身份诈骗：犯罪分子伪装成“高富帅”或“白富美”，加为好友骗取感情和信任后，随即以资金紧张、家人有难等各种理由骗取钱财。

7.医保、社保诈骗：犯罪分子冒充医保、社保工作人员，谎称受害人账户出现异常，之后冒充司法机关工作人员以公正调查、便于核查为由，诱骗受害人向所谓的安全账户汇款实施诈骗。

8.“猜猜我是谁”诈骗：犯罪分子打电话给受害人，让其“猜猜我是谁”，随后冒充熟人身份，向受害人借钱，一些受害人没有仔细核实就把钱打入犯罪分子提供的银行卡内。

二、购物类欺诈：

通过以各种虚假优惠信息、客服退款、虚假网店实施欺诈。

9.假冒代购诈骗：犯罪分子假冒成正规微商，以优惠、打折、海外代购等为诱饵，待买家付款后，又以“商品被海关扣下，要加缴关税”等为由要求加付款项实施诈骗。

10.退款诈骗：犯罪分子冒充淘宝等公司客服，拨打电话或者发送短信，谎称受害人拍下的货品缺货，需要退款，引诱求购买者提供银行卡号、密码等信息，实施诈骗。

11.网络购物诈骗：犯罪分子通过开设虚假购物网站或网店，在事主下单后，便称系统故障需重新激活。后通过 QQ 发送虚假激活网址，让受害人填写个人信息，实施诈骗。

12.低价购物诈骗：犯罪分子发布二手车、二手电脑、海关没收的物品等转让信息，事主与其联系，以缴纳定金、交易税手续费等方式骗取钱财。

13.解除分期付款诈骗：犯罪分子冒充购物网站的工作人员，声称“由于银行系统错误”，诱骗受害人到 ATM 机前办理解除分期付款手续，实施资金转账。

14.收藏诈骗：犯罪分子冒充收藏协会，印制邀请函邮寄各地，称将举办拍卖会并留下联络方式。一旦事主与其联系，则以预先缴纳评估费等名义，要求受害人将钱转入指定账户。

15.快递签收诈骗：犯罪分子冒充快递人员拨打事主电话，称其有快递需签

收但看不清信息，需事主提供。随后送“货”上门，事主签收后，再打电话称其已签收须付款，否则讨债公司将找麻烦。

三、活动类欺诈：

通过微信、微博等社交工具发布各种虚假活动，引诱用户参与进行诈骗。

16.发布虚假爱心传递：犯罪分子将虚构的寻人、扶困帖子以“爱心传递”方式发布在网络上里，引起善良网民转发，实则帖内所留联系电话是诈骗电话。

17.点赞诈骗：犯罪分子冒充商家发布“点赞有奖”信息，要求参与者将姓名、电话等个人资料发至社交工具平台上，套取足够的个人信息后，以获奖需缴纳保证金等形式实施诈骗。

四、利诱类欺诈：

以各种诱惑性的中奖信息、奖励、高额薪资吸引用户进行诈骗。

18.冒充知名企业中奖诈骗：冒充知名企业，预先大批量印刷精美的虚假中奖刮刮卡，投递发送，后以需交个人所得税等各种借口，诱骗受害人向指定银行账号汇款。

19.娱乐节目中奖诈骗：犯罪分子以热播栏目节目组的名义向受害人手机群发短消息，称其已被抽选为幸运观众，将获得巨额奖品，后以需交保证金或个人所得税等各种借口实施诈骗。

20.兑换积分诈骗：犯罪分子拨打电话，谎称受害人手机积分可以兑换。诱使受害人点击钓鱼链接。如果受害人按照提供的网址输入银行卡号、密码等信息后，银行账户的资金即被转走。

21.二维码诈骗：以降价、奖励为诱饵，要求受害人扫描二维码加入会员，实则附带木马病毒。一旦扫描安装，木马就会盗取受害人的银行账号、密码等个人隐私信息。

22.重金求子诈骗：犯罪分子谎称愿意出重金求子，引诱受害人上当，之后以缴纳诚意金、检查费等各种理由实施诈骗。

23.高薪招聘诈骗：犯罪分子通过群发信息，以月工资数万元的高薪招聘某类专业人士为幌子，要求事主到指定地点面试，随后以缴纳培训费、服装费、保证金等名义实施诈骗。

24.电子邮件中奖诈骗：犯罪分子通过互联网发送中奖邮件，受害人一旦与犯罪分子联系兑奖，犯罪分子即以缴纳个人所得税、公证费等各种理由要求受害人汇钱，达到诈骗目的。

五、虚构险情欺诈：

通过捏造各种意外不测、让用户惊吓不安的消息实施欺诈。

25.虚构车祸诈骗：犯罪分子以受害人亲属或朋友遭遇车祸，需要紧急处理交通事故为由，要求对方立即转账。当事人便按照犯罪分子指示将钱款打入指定账户。

26.虚构绑架诈骗：犯罪分子虚构事主亲友被绑架，如要解救人质需立即打款到指定账户并不能报警，否则撕票。当事人往往不知所措，按照犯罪分子指示将钱款打入账户。

27.虚构手术诈骗：犯罪分子以受害人子女或父母突发疾病需紧急手术为由，要求事主转账方可治疗。遇此情况，受害人往往心急如焚，按照犯罪分子指示转款。

28.虚构危难困局求助诈骗：犯罪分子通过社交媒体发布病重、生活困难等虚假情况，博取广大网民同情，借此接受捐赠。

29.虚构包裹藏毒诈骗：犯罪分子以事主包裹内被查出毒品为由，要求事主将钱转到国家安全账户以便公正调查，从而实施诈骗。

30.捏造淫秽图片勒索诈骗：犯罪分子收集公职人员照片，使用电脑合成淫秽图片，并附上收款账号邮寄给受害人进行威胁恐吓，勒索钱财。

31.虚构小三怀孕做流产：犯罪分子冒充儿子发送短信给父母，充分利用老年人心疼儿子的特点，诱惑受害者转账。

六、日常生活消费类欺诈：

针对日常生活各种缴费、消费实施欺诈骗局。

32.冒充房东短信诈骗：犯罪分子冒充房东群发短信，称房东银行卡已换，要求将租金打入其他指定账户内，部分租客信以为真，将租金转出方知受骗。

33.电话欠费诈骗：犯罪分子冒充通信运营企业工作人员，向事主拨打电话或直接播放电脑语音，以其电话欠费为由，要求将欠费资金转到指定账户。

34.电视欠费诈骗：犯罪分子冒充广电工作人员群拨电话，称以受害人名义在外地开办的有线电视欠费，让受害人向指定账户补齐欠费，部分群众信以为真，转款后发现被骗。

35.购物退税诈骗：犯罪分子事先获取到事主购买房产、汽车等信息后，以税收政策调整可办理退税为由，诱骗事主到 ATM 机上实施转账操作，将卡内存款转入骗子指定账户。

36.机票改签诈骗：犯罪分子冒充航空公司客服，以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

37.订票诈骗：犯罪分子制作虚假的网上订票公司网页，发布虚假信息，以较低票价引诱受害人上当。随后，以“订票不成功”等理由要求事主再次汇款，实施诈骗。

38.ATM 机告示诈骗：犯罪分子预先堵塞 ATM 机出卡口，并粘贴虚假服务热线，诱使用户在卡“被吞”后与其联系，套取密码，待用户离开后到 ATM 机取出银行卡，盗取用户卡内现金。

39.刷卡消费诈骗：犯罪分子以银行卡消费可能泄露个人信息为由，冒充银联中心或公安民警设套，套取银行账号、密码实施犯罪。

40.引诱汇款诈骗：犯罪分子以群发短信的方式直接要求对方向某个银行账户汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，往往未经核实，即把钱款打入骗子账户。

七、钓鱼、木马病毒类欺诈：

通过伪装成银行、电子商务等网站窃取用户帐号密码等隐私的骗局。

41.伪基站诈骗：犯罪分子利用伪基站向广大群众发送网银升级、10086 移动商城兑换现金的虚假链接，一旦受害人点击后便在其手机上植入获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

42.钓鱼网站诈骗：犯罪分子以银行网银升级为由，要求事主登录假冒银行的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施诈骗。

八、其他新型违法类欺诈：

43.校讯通短信链接诈骗：犯罪分子以“校讯通”的名义，发送带有链接的诈骗短信，一旦点击链接进入后，手机即被植入木马程序，存在银行卡被盗刷的风险。

44.交通处理违章短信诈骗：犯罪分子利用伪基站等作案工具发送假冒违章提醒短信，此类短信包含木马链接，受害者点击之后轻则群发短信造成话费损失，重则窃取手机里的银行卡、支付宝等账户信息，随后盗刷银行卡，造成严重经济损失。

45.结婚电子请柬诈骗：犯罪分子通过电子请帖的方式诱导用户点击下载后，就能窃取手机里的银行账号、密码、通信录等信息，进而盗刷用户的银行卡，或者给用户通讯录中的朋友群发借款诈骗短信。

46.相册木马诈骗：犯罪分子冒充“小三”身份激怒受害人点击“相册”链接，种植木马病毒获取用户网银信息等。

47.金融交易诈骗：犯罪分子以证券公司名义，通过互联网、电话、短信等方式散布虚假个股内幕信息及走势，获取事主信任后，又引导其在自身搭建的虚假交易平台上购买期货、现货，从而骗取事主资金。

48.办理信用卡诈骗：在媒体刊登办理高额透支信用卡广告，事主与其联系后，以缴纳手续费、中介费等要求事主连续转款。

49.贷款诈骗：犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以预付利息、保证金等名义实施诈骗。

50.复制手机卡诈骗：犯罪分子群发信息，称可复制手机卡，监听手机通话信息，不少群众因个人需求主动联系嫌疑人，继而被对方以购买复制卡、预付款等名义骗走钱财。

51.虚构色情服务诈骗：犯罪分子在互联网上留下提供色情服务的电话，待受害人与之联系后，称需先付款才能上门提供服务，受害人将钱打到指定账户后发现被骗。

52.提供考题诈骗：犯罪分子针对即将参加考试的考生拨打电话，称能提供考题或答案，不少考生急于求成，事先将好处费的首付款转入指定账户，后发现被骗。

53.盗用账号、刷信誉诈骗：犯罪分子盗取商家社交平台账号后，发布“诚招网络兼职，帮助淘宝卖家刷信誉，可从中赚取佣金”的推送消息。受害人按照对方要求多次购物刷信誉，后发现上当受骗。

54.冒充黑社会敲诈类诈骗：犯罪分子先获取事主身份、职业、手机号等资料，拨打电话自称黑社会人员，受人雇用要加以伤害，但事主可以破财消灾，然后提供账号要求受害人汇款。

55.公共场所山寨 WiFi：犯罪分子设置与山寨信号，这类信号就是一些盗号者在公共场合放出的钓鱼免费 WiFi，当连接上这些免费网络后，通过流量数据的传输，黑客就能轻松将手机里的照片、电话号码、各种密码盗取，对机主进行敲诈勒索。

56.捡到附密码的银行卡：犯罪分子故意丢弃带密码的银行卡，并标明了“开户行的电话”，利用了人们占便宜的心理诱使捡到卡的人拨打电话“激活”这张

卡，并存钱到骗子的账户上。

57.账户有资金异常变动：犯罪分子首先窃取了受害者网银登陆账号和密码，通过购买贵金属、活期转定期等操作制造银行卡上有资金流出的假象。然后假冒客服打电话确认交易是否为本人操作，并同意给用户退款骗取用户信任，要求受害者提供自己手机收到的验证码，受害者一旦把短信验证码提供给了对方，对方就得手了。

58.先转账、再取现、后撤销：犯罪分子利用银行转账新规中转账和到账时间的“时间差”来设置圈套。采取先转账、后给现金的诈骗套路，在骗取到受害人现金后，撤销转账。

59.补换手机卡：犯罪分子先用几百条垃圾短信和骚扰电话轰炸手机，以掩盖由 10086 客服发送到手机号码上的补卡业务提醒短信；然后，拿着一张有受害者信息的临时身份证，去营业厅现场补办手机卡，使得机主本人的手机卡被动失效，从而接收短信验证码把绑定在手机 APP 上的银行卡的钱盗走。

60.换号了请惠存:这属于冒充熟人的电信诈骗的“升级”。犯罪分子通过非法渠道获得机主的通讯录资料后，假冒机主给手机里的联系人发短信，声称换了新号码，然后向其手机里的联系人进行诈骗。

来源：中国警方在线　2020-02-19

反网络电信诈骗的五大利器

一、国家反诈中心 APP

国家反诈中心 APP 是一款官方手机防骗保护软件，主要有以下功能：一是当用户收到涉诈电话、短信或登录涉诈网址时，及时进行预警提示。二是当用户发现涉诈线索时，可以一键举报。三是用户可以通过 APP 对可疑网友的真实身份、社交账号、交易账号进行涉诈风险验证，大大降低网络交易风险。四是 APP 每日发布不法分子的最新诈骗手法，剖析典型案例，协助用户学习防骗知识、了解诈骗套路，提升识骗能力。

二、96110 预警劝阻专线

96110 预警劝阻专线，目前已在全国 29 个省区市的公安机关开通。

96110 预警劝阻专线是反诈专用号码，主要有以下功能：一是预警劝阻，发现群众正遭遇电信网络诈骗或者属于极易受骗的人员，公安机关将通过该专线及时预警劝阻。二是防骗咨询，如果遇到疑似电信网络诈骗活动，群众可以拨打

96110 进行咨询。三是涉诈举报，如果发现涉诈线索，群众可以通过该号码进行举报。

公安机关提醒：96110 是官方预警劝阻专线，如接到“96110”号码来电，说明机主本人或其家人正遭遇电信网络诈骗，请一定及时接听并耐心听取民警的劝阻提示，避免上当受骗。

三、12381 涉诈预警劝阻短信

工信部联合公安部推出 12381 涉诈预警劝阻短信系统，首次实现对潜在被骗用户的短信实时预警，上线以来已成功发送预警信息 1.49 亿条，预警劝阻准确率达 60%以上。

12381 系统可根据公安机关提供的涉案号码，利用大数据、人工智能等技术自动分析发现潜在被骗用户，并通过 12381 短信端口第一时间向用户发送预警短信，提示用户可能面临“贷款”“刷单返利”“冒充公检法”“杀猪盘”等 9 类高发电信网络诈骗情况。

公安机关提醒：如果收到来自 12381 的预警短信，说明很可能遭遇了电信网络诈骗，要保持高度警惕，牢记“三不一多”原则：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，谨防上当。

四、全国移动电话卡“一证通查”服务

针对部分群众身份信息被诈骗分子冒用办理涉案电话卡等情况，工信部推出全国移动电话卡“一证通查”服务，截至今年 4 月底，用户查询量已累计突破 6700 万次。同时，集中排查处置涉诈高危电话卡 7760 余万张、行业卡 1930 余万张，清理关联互联网账号 5700 万余个，对全国物联网卡开展拉网排查，一大批存量高危号卡得到全面清理。

诈骗分子冒用他人身份开办电话卡严重侵害用户本人合法权益，广大群众对此深恶痛绝。“一证通查”服务打通了 93 家省级基础电信企业和 39 家移动通信转售企业相关数据，群众只需要使用自己的居民身份证，即可通过线上线下多种渠道查询本人名下持有的全国移动电话卡数量，专用短信端口 10699000 将在 48 小时内向预留手机号反馈结果，真正实现了全国移动电话卡的统一便捷查询。

五、云闪付 APP“一键查卡”

为解决群众对于跨行银行卡账户查询的诉求，2021 年 12 月，人民银行指导中国银联股份有限公司联合商业银行基于银行业统一 APP 云闪付试点“一键查卡”功能，打造统一查询途径，向公众提供银行卡数量、每张卡的银行名称、借贷记

属性、脱敏卡号等信息的查询，在确保信息安全的前提下，便利公众直接掌握个人名下银行卡信息，强化自身银行卡管理。目前，“一键查卡”实行“16+16”试点应用，向上海、云南、北京、重庆等 16 个地区的用户，提供工商银行、农业银行、中国银行、建设银行、交通银行等 16 家全国性商业银行的银行卡查询服务。

自“一键查卡”功能试点上线以来，已累计生成超过百万份查询报告。后续随着试点逐步完善、推广，中国银联将不断扩大查卡范围和服务地区，优化查卡功能。（原标题：用好反网络电信诈骗五大利器——驻泰国使馆防范网络电信诈骗宣传周系列提醒之六）

来源：中国驻泰国大使馆官网　2022-06-08

公安部：电信网络诈骗犯罪出现了一些新变化、新特点

一是新型网络犯罪已成为主流犯罪。近年来，随着信息社会快速发展，犯罪结构发生了重大变化，传统犯罪持续下降，以电信网络诈骗为代表的新型网络犯罪已成为主流犯罪，成为公安机关面临的严峻挑战。尽管一年来此类案件在严打高压态势下出现下降趋势，但发案仍在高位运行，形势依然严峻复杂。当前，世界主要发达国家的电信网络诈骗发案也呈迅猛增长态势，特别是新冠疫情背景下，人们生产生活加速向网上转移，进一步加剧了案件的高发，电信网络诈骗犯罪已成为全球性的打击治理难题。

二是诈骗手法加速迭代变化。诈骗集团紧跟社会热点，随时变化诈骗手法和“话术”，迷惑性强，人民群众很容易上当受骗。诈骗集团针对不同群体，根据非法获取的精准个人信息，量身定制诈骗剧本，实施精准诈骗。公安机关发现的诈骗类型现在已经超过 50 种，其中网络刷单返利、虚假投资理财、虚假网络贷款、冒充客服、冒充公检法是 5 种主要的诈骗类型。

三是攻防对抗不断加剧升级。诈骗集团利用区块链、虚拟货币、AI 智能、GOIP、远程操控、共享屏幕等新技术新业态，不断更新升级犯罪工具，与公安机关在通讯网络和转账洗钱等方面的攻防对抗不断加剧升级。从通讯网络通道看，利用虚假 APP 实施诈骗已占全部发案的 60%，开始大量利用秒拨、VPN、云语音呼叫以及国外运营商的电话卡、短信平台、通讯线路实施诈骗。从资金通道看，传统的三方支付、对公账户洗钱占比已减少，大量利用跑分平台加数字货币洗钱，尤其是利用 USDT（泰达币）危害最为严重。

四是跨国有组织特征日趋明显。诈骗集团组织严密、分工明确，呈现出多行业支撑、产业化分布、集团化运作、精细化分工、跨境式布局等跨国有组织犯罪特征。集团头目和骨干往往躲在境外，打着高薪招聘的幌子，诱骗招募涉世未深的年轻人赴境外从事诈骗活动，目前在柬埔寨、菲律宾、阿联酋、土耳其、缅北等国家和地区，仍有大量犯罪团伙向我公民实施诈骗活动，跨国有组织犯罪特征日趋明显。

综合自新华网、第一财经相关报道

全国人大常委会法工委权威解读反电信网络诈骗法亮点

全国人大常委会法制工作委员会刑法室主任王爱立、公安部刑事侦查局副局长姜国利和全国人大常委会法制工作委员会刑法室处长张义健等就反电信网络诈骗法立法修法的亮点和人民群众关心的热点问题进行权威解读。

亮点一：“小切口”立法坚持人民至上

王爱立介绍，目前，与电信网络诈骗相关的法律规定较为分散，不够明确，针对性不强；实践中一些好的经验做法和政策文件需要上升为法律规定；在行业治理和制度建设方面还需要进一步完善，形成协同打击治理合力。在这样的情况下，急需有一部专门立法满足实践需要。

反电信网络诈骗法是“小快灵”立法的重要立法实践，是对全国人大常委会立法形式的进一步丰富，对关键环节、主要制度作出规定，建起四梁八柱，条文数量不求太多，立法进程快，体现急用先行。

亮点二：加强有针对性、精准性的宣传教育和防范预警

王爱立介绍，反电信网络诈骗法明确规定各级政府和部门的宣传教育职责，要普及相关法律和知识，提高公众的防骗意识和识骗能力；规定有关部门和基层组织，加强对老年人、青少年等重点易受害群体的宣传教育，开展反诈宣传教育进学校、进企业、进社区、进农村、进家庭的“五进”活动；规定行业企业的反诈宣传职责，对本领域新出现的诈骗手段要及时向用户作出提醒，在业务过程中对非法买卖“两卡”的法律责任作出警示；规定有关新闻单位面向社会广泛开展宣传教育活动；规定举报电信网络诈骗的奖励和保护；规定社会面上的单位和个人也要加强内部防范，提升自身防范意识。

特别规定了公安机关要会同有关部门、企业建立预警劝阻系统，对发现的潜在被害人及时采取相应劝阻措施。

亮点三：多部门联动，全链条治理

电信网络诈骗分子实施诈骗活动，离不开金融、通信、互联网等业务，他们利用这些技术和服务实施骗术、转移资金等。因此，加强对这些行业领域的治理是防范电信网络诈骗活动的关键和重点，也是难点。

“与传统的诈骗相比，电信网络诈骗利用技术手段钻管理上的漏洞，呈现组

织化、链条化、精准化等特征，实现跨部门、跨行业、跨地域协作犯罪。因此，非常有必要加强部门联动，形成打击治理合力。”全国人大常委会法制工作委员会刑法室处长张义健说，反电信网络诈骗法对地方政府的属地责任、行业主管部门的监管责任、政法部门的惩治责任、企业的防范责任、公民提高防范意识等作出了全面规定，组合出拳，形成合力。

反电信网络诈骗法明确规定国务院建立反电信网络诈骗工作机制，地方政府组织领导反电信网络诈骗工作，开展综合治理；公安机关牵头负责反电信网络诈骗工作，加强依法打击，金融、电信、互联网等主管部门负责本行业领域反诈工作；法院、检察院依法防范、惩治电信网络诈骗活动，人民检察院依法提起公益诉讼；政府部门间打击治理电信网络诈骗的协同配合和联动机制；金融、电信、互联网部门对有关企业的监督检查、管理防范职责；部门工作人员在反电信网络诈骗工作中滥用职权、玩忽职守的法律责任。

王爱立强调，反电信网络诈骗法注重从人员链、信息链、技术链、资金链等进行全链条治理，从前端宣传预防，中端监测止付，后端教育惩治进行全流程治理，强化部门监管主体责任，压实企业责任，对电诈分子规定了有效预防惩处措施，严厉打击各类涉诈黑灰产行为，构筑了反电信网络诈骗立法的“法网恢恢”。

亮点四：加强打击治理跨境电信网络诈骗

目前，境外实施电信网络诈骗犯罪占比高，境外电信网络诈骗犯罪也是打击的重点和难点。反电信网络诈骗法在管辖方面，规定中国公民在境外实施电信网络诈骗活动的，或者境外的组织、个人针对中国境内实施电诈活动或者为对境内实施电诈活动提供帮助的，适用反电信网络诈骗法的规定；在出境限制的措施方面，规定对前往涉诈严重地区且出境活动存在重大涉诈嫌疑的，或者因电信网络诈骗受过刑事处罚的，可以根据情况采取出境限制措施。

张义健表示，法律规定的条件是明确的，实践中要注意精准适用，依照有关规定确定的标准和程序，结合具体情况对重大涉诈活动嫌疑作出判断和决定，同时对于前科人员也要结合犯罪情况和预防再犯罪的需要进行判断，决定是否限制出境。

此外，反电信网络诈骗法特别规定公安机关要会同有关部门，通过开展国际警务合作等方式，提升信息交流、调查取证、侦查抓捕、追赃挽损等方面合作效能，坚决有效打击遏制跨境电信网络诈骗。

亮点五：个人信息保护双重发力

个人信息泄露为实施电信网络诈骗提供了“牵线搭桥”的便利，特别是在投资理财杀猪盘、冒充领导、快递物流类等诈骗案件中，精准锁定了诈骗对象。

“反电信网络诈骗法对个人信息保护双重发力，既要从上游阻断信息源，也要防止在反电信网络诈骗工作中个人信息的二次泄露。”张义健强调。

与个人信息保护法衔接，反电信网络诈骗法规定个人信息处理者要建立个人信息被用于电信网络诈骗的防范机制。特别是对与实施电信网络诈骗密切相关的物流信息、贷款信息、交易信息、婚介信息等要重点保护。规定公安机关在办理电信网络诈骗案件时要“一案双查”，对犯罪所利用的个人信息的来源进行查证溯源，并依法追究提供、泄露个人信息人员的法律责任。

此外，反电信网络诈骗法对于出售、提供个人信息，为实施电信网络诈骗提供支持帮助的黑灰产行为明确禁止，规定相应法律责任。同时，强调在反诈工作中对个人信息的保护。

亮点六：加强追赃挽损，提出申诉救济措施

随着互联网金融的发展，诈骗分子利用三方四方支付、跑分平台、数字货币、贸易对冲等多种方式，不断改变转账洗钱手法，转账速度快、隐蔽性强、追踪溯源难，给公安机关追缴赃款工作带来很大困难，此项工作还面临诸多挑战。

“反电信网络诈骗法的出台，为公安机关处置涉诈资金提供了法律支撑。”公安部刑事侦查局副局长姜国利表示。

反电信网络诈骗法明确规定对电信网络诈骗案件应当加强追赃挽损，完善涉案资金处置制度，及时返还被害人的合法财产。对遭受重大生活困难的被害人，符合国家有关救助条件的，有关方面依照规定给予救助。

公安部正在研究制定《涉诈资金处置规定》，进一步明确涉诈资金处置的工作流程和措施，确保有关工作依法高效开展。

来源：人民公安报　2022-09-07

反电信网络诈骗法的特点

01、“快”

立法技术上是“小快灵”，体现“小切口”，对关键环节、主要制度作出规定，建起四梁八柱，条文数量不求太多，立法进程快，体现急用先行，将进一步丰富全国人大常委会的立法形式。

02、“防”

强化系统观念，立足源头治理、综合治理，侧重前端防范。关于电信网络诈骗违法犯罪分子的法律责任，刑法已做出多次修改完善。关于依法打击电信网络诈骗，刑法已多次做出相关修改完善，可以说打击的法律手段总体上较为充足。本法主要是按照完善预防性法律制度的要求，针对电信网络诈骗发生的信息链、资金链、技术链、人员链等各环节，加强防范性制度措施建设，深入推进行业治理，强化部门监管责任和企业社会责任，变“亡羊补牢”为“未雨绸缪”，变重“打击”为“打防管控”并重。

03、“准”

反电信网络诈骗法是新型领域立法，立法过程中始终坚持问题导向和结果导向，作为一部专项急需立法必须立足实践需要，采取各项有力措施，赋予执法机关职权和企业责任，同时也要必须坚持精准防治，防止“一刀切”措施，依法保护公民和组织合法权益。（摘自：反电信网络诈骗法 12 月 1 日起施行）

来源：光明网　2022-11-25

《反电信网络诈骗法》施行后重点关注的 3 类群体

奇安信集团旗下奇安盘古反诈业务专家韩冲表示，反诈法施行后主要影响群体大致可划分为 3 类，即以互联网企业为代表的生产经营类企业、以电信运营商和银行、保险公司为代表的运营服务类机构、以公安和网信为代表的监管执法类单位，不同群体所承担的反诈治理责任及义务各不相同。

生产经营类企业须确保业务合规开展

以互联网公司为代表的生产经营类企业，其技术平台优势、企业品牌效应、客群资源覆盖等常常被电信诈骗分子进行扩大化间接渗透。如：借助名企名品背书下的“李鬼式 APP”生产、以技术外包或联合开发为由下的诈骗产品开发、围绕用户信息采集交易下的精准诈骗实施等都是较为常见诈骗开展形式。

虽然生产经营类企业未直接参与端对端的诈骗实施过程，但是在技术支撑、资源服务、人力组织方面等间接帮助了诈骗分子的诈骗实施开展，即构成了电信网络诈骗帮信事实（根据《中华人民共和国刑法》第 287 条之二规定）。因此，各类互联网企业应加强所经营业务的合规性内部审计以及外部风险漏洞排查工作，做到合法合规化业务开展。

运营服务类机构落实有效审查覆盖

以电信运营商、银行保险公司为代表的运营服务类机构，作为整个电信网络

诈骗的运作核心链（即通信链、资金链）。在整个反诈治理过程中除了面向基础用户侧开展“两卡 ”管控、诈骗域名&APP 监测外，其与自身运营服务相关的审查工作也应并行覆盖考虑。如：运营商侧应开展基于 IP 租售下的滥用及恶意网站投放监测、面对 VPN 建设下的绕行屏蔽访问行为检测等，银行、保险侧应开展金融欺诈交易侦查、互联网洗钱平台监测等。

监管执法类单位加强打击整治投入

以网信、公安、通管等为代表的监管执法类单位，需要进一步压实受害人预警劝阻、诈骗团伙侦查打击、行业统一监管等工作的开展，并按周期性诈骗态势、地域地缘特征等进行差异化分级治理投入。

随着反诈法的正式施行落地，各行业机构需尽快完善反诈相关基础建设并提升自身技术储备，充分发挥大数据和人工智能等技术作用，打造企业协同链路，更好适应新时期下的反诈工作形势及要求。（原标题：《反电信网络诈骗法》12 月 1 日起施行 这 3 类群体须重点关注）

来源：新京报　2022-12-01

最高检公安部：依法从严合力打击跨境电信网络诈骗犯罪

为依法严厉打击跨境电信网络诈骗犯罪，全力推进“拔钉”“断流”等专项行动，切实维护良好社会秩序和人民群众合法权益。

近年来，各级检察机关、公安机关深入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，按照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部署，密切配合、多措并举，始终坚持以人民为中心，依法、从严、全链条打击电信网络诈骗及其关联犯罪，深挖电信网络诈骗集团幕后“金主”，打击惩处工作取得明显成效。今年 6 月“拔钉”行动开展以来，国务院联席办先后将 470 余名电信网络诈骗集团头目和骨干纳入重点缉捕范围。截至目前，公安机关已抓获其中 240 余名，检察机关已逮捕 150 余名、起诉 80 余名。

为依法严打跨境电信网络诈骗犯罪集团嚣张气焰，最高检、公安部联合挂牌督办了第一批 5 起特大电信网络诈骗案件，相关地方检察机关、公安机关加强研判分析，强化协作配合，推动打击工作取得阶段性重大进展。如，浙江“12·30”电信网络诈骗案已抓获 11 名主要犯罪嫌疑人，判决 4 名。主要组织者葛某一审被判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产，其余 3 名主要犯罪嫌疑人均被判处十年以上有期徒刑。

工作中，最高检、公安部建立常态化挂牌督办工作机制于近日联合挂牌督办第二批 3 起特大跨境电信网络诈骗案件。这 3 起案件分别是浙江桐乡“3·03”电信网络诈骗案、湖北咸宁“3·03”电信网络诈骗案、四川南充“4·01”电信网络诈骗案，这是今年以来“拔钉”“断流”等专项行动中的重点案件，涉案金额巨大，社会危害严重，目前仍有部分犯罪分子畏罪潜逃、逍遥法外。

最高检、公安部有关负责人表示，全国检察机关和公安机关将深入学习贯彻党的二十大精神，认真贯彻反电信网络诈骗法，坚持以“零容忍”的态度，全力抓捕、从严惩治跨境电信网络诈骗犯罪集团头目和骨干，坚决“打财断血”，有力斩断犯罪链条，全力追赃挽损，切实守护人民群众合法权益和财产安全。（摘自：依法从严合力打击跨境电信网络诈骗犯罪最高检公安部联合挂牌督办第二批 3 起特大跨境电信网络诈骗犯罪案件）

来源:中国警察网　　2022-12-13

电信诈骗套路翻新迷惑性增强需警惕

电信网络诈骗犯罪分子依托新型电信网络技术手段，利用非法获取个人信息、网络黑灰产业交易等实施精准诈骗。此类新型电信诈骗犯罪呈现三大特征应予警惕：

其一是犯罪分子从单兵作战的“小窝点”向分工明确的“大集团”转变，部分团伙以公司招募“业务员”的方式，诱骗新人加入犯罪组织，形成“信息搜集-话术配合-交叉诱导-转移赃款”多环节流程，内部精细化分工，境内揽款、境外洗钱，犯罪链条延长，呈跨域化、组织化特征。

其二是施骗手段迭代，新型电信诈骗利用 AI 智能、区块链等新技术，借助虚拟机、VPN、云呼叫等方式，使犯罪事实难以立刻察觉，犯罪分子多通过虚假投资 APP，诱骗被害人购买虚拟货币等理财产品，将诈骗行为伪装成“投资活动”，犯罪工具隐蔽、技术新颖。

其三是受骗群体特定，新型电信诈骗从“广泛撒网”转向“重点捕捉”，针对学生、老年人、单身青年等特定群体，为其量身定制“剧本”，引导被害人一步步落入犯罪分子的圈套。

与传统模式相比，新型电信诈骗隐蔽性强、涉案金额大、被害人数多，容易造成更为严重的危害后果。因犯罪分子聚焦的年轻学生与老人为相对弱势的群体，部分被害人因难以承受大量资金被骗而猝死或自杀身亡。又因新技术的运用使被

害人信息极易被储存、运用，导致大量个人信息外泄，滋生信息窃取倒卖“黑色产业链”。

广大群众应提高警惕，不轻信“天上掉馅饼”类噱头、不透露个人信息、不向陌生人转账。公检法应加大电信诈骗打击力度，升级犯罪甄别预警工具，开展专项电信诈骗普法活动，营造“全民反诈”良好氛围。

来源：中国法院网　2022-12-13

【权威解读】我们认知中，电信网络诈骗的四大误区！

误区一：被骗的都是中老年人

中老年人这个群体，因为岁数较大，记忆力、智力、思维能力都有不同程度的减退。最重要的是，老年人对新鲜事物了解不足，特别是对电信网络诈骗犯罪了解欠缺，这是老年人在日常生活中被骗较多的原因。与此同时，该群体往往积累了一定的家庭财富，使得他们便成为一些电信网络诈骗犯罪嫌疑人青睐的对象。这样的人一旦被骗，一辈子的积蓄就会付诸东流。

但在实际情况中我们发现，老年人并不是唯一的被骗高危群体，被电信网络诈骗的事主，年龄构成呈“哑铃”状，也就是说，年龄两极化现象比较严重。除了中老年人以外，高校学生以及刚刚步入社会的青年也是易被侵害群体。因为这些人的社会阅历少，对社会风险的认知预估不足，并且又急于追求成功和积累财富，盲目地尝试新鲜事物，所以非常容易掉进骗子设定的陷阱。与中老年受害群体有所区别的是，青年受害群体在个案案值上损失不大，但整体发案数量高。

除了这两类人群外，企事业单位的财会人员也是此类犯罪嫌疑人的重点关注对象。他们往往掌管着企业的大量资金，一旦被骗，整个企业就会遭受巨大的损失，甚至会导致企业直接破产，这样的后果可谓相当沉重。

误区二：都是因为贪财、智商低，才会上当

关于电信网络诈骗，普遍存在一大误区，人们普遍认为：只有贪财之人，才会上当；上当受骗的，都是傻瓜。可是，实际上并非如此，电信网络诈骗在早期，的确是利用人们心中的贪念来实施犯罪（特别是台湾地区），比如“六合彩”等，但随着这种犯罪手段的普及，诈骗种类和花样也在不断翻新。现在，警方从侦查角度将电信网络诈骗归为四十多个大类、一百多个小类。这种种诈骗手段，对人们心理的利用也各不相同，大致可分为贪、怕、慌、缺、善几类，稍微不注意就会中招。

这些中招的受害者中，不乏高学历人士，甚至有个别民警也曾经上当受骗，并向犯罪嫌疑人汇过款。所以，对于电信网络诈骗，我们要重视起来，无论你认为自己社会阅历有多丰富，认为自己智商高还是学历高，如果不能及时了解一些防范资讯，很容易就会成为下一个受害者。

误区三：反电信网络诈骗，都是警察的事

很多人认为，案件的发生和破获与自己没有任何关系，破案抓人是警察的事，跟我没有关系。其实，这是一个很严重的误区，电信网络诈骗造成的损失，绝对不像我们所看到的那么简单。被诈骗的事主以及家人遭受了财产损失和精神打击，他们是第一受害者；那些接到电话但没有被骗的民众受到了骚扰甚至恐吓，这些人是第二受害者；第三受害者，则是我们置身其中的社会。

实施电信网络诈骗时，电话是经常用到的工具，犯罪嫌疑人往往冒充公安机关、法院、检察院的工作人员，冒充各级政府部门、公司（企业）的客服以及其他各种身份，来进行诈骗。他们摧毁的是整个社会的信任体系，导致人与人之间不敢随意相信他人，互相打电话、发信息时都不能确定对方到底是谁。

面对电信网络诈骗肆意横行，我们每一个人都是受害者，任何人概莫能外。由于电信网络诈骗的远程非接触性、隐蔽性特点，仅仅依靠警察一家，是难以完成对案件的侦查、破案以及防范工作的。常规的侦查需要金融部门、通讯运营商以及各个职能部门及企事业单位共同配合与支持，警察才能成功将这些犯罪嫌疑人绳之以法。

打击电信网络诈骗需要多警种、多部门、多方面的参与配合。而在防范此类犯罪的方面，更需要整个社会全员参与，共同编织一张防范电信网络诈骗的法网。

误区四：骗子实名使用银行账号和电话号码，为何不予逮捕

很多事主被骗后报警，都能向警察提供对方的账户信息以及电话号码。实实际上，这些账户和电话的开户人和犯罪嫌疑人没有一点关系。那么，账户又是怎么来的呢？基本上有两个途径：一个途径是，一些社会底层人员或没有经济来源的高校学生为了蝇头小利，主动用自己的身份证办理银行卡，然后以每张卡几十至几百元的价格卖给一些收售银行卡的“卡头”；另一个途径就是，这些“卡头”组织社会人员利用他人（一般是事主丢失）或者伪造的身份证件去办理银行卡。虽然我国“断卡”行动一直在高压状态，但是仍然有很多为了蝇头小利出卖自己身份证银行卡的“法盲”。

之后，这些银行卡会批量贩卖给诈骗团伙。电话号码除了有着和银行卡同样

的来源外，一些设备、软件都可以对来电予以伪装或者隐蔽。所以，光凭电话号码无法找到真正的犯罪嫌疑人。

此外，诈骗团伙为了逃避打击，基本上都是采取跨区域甚至跨国犯罪，这给警察的侦查工作造成了很大的难度。此类案件的犯罪侦查工作极具专业性，一般的基层派出所根本不具备开展此类案件侦查的能力。为了应对这种局面，各地成立了反电信网络诈骗中心，以便集中开展对此类案件的侦查工作。

综合自防骗每日电讯、反诈防诈骗中心相关报道

国外电信网络诈骗治理举措

从国际上看，为进一步防范治理电信网络诈骗，全球主要国家和地区立足本国国情，结合本国电信网络诈骗特点规律，多措并举，纷纷加强个人信息保护，强化重点人群以及弱势群体管理，持续提升技术防范能力，不断畅通用户举报投诉等渠道，同步配套宣传引导与警示教育等，有效遏制电信网络诈骗活动的蔓延。

强化立法保障，打好诈骗治理的法制基础。在立法方面，美国政府为打击电信网络诈骗、防范骚扰电话，先后发布《电话消费者保护法案》《控制非自愿色情和推销侵扰法》《真实电话主叫身份法案》等多项法规政策。在执法方面，根据美国法律规定，未经用户同意向“拒绝电话名单”注册用户推送商业推销、产品推广、服务广告等垃圾短信的，将面临 500 美元至 1500 美元的处罚。日本通过的《日本刑法典》规定“欺骗人而使其交付财务的，处十年以下徒刑”。

加强组织保障，高站位推进治理工作落地实施。一方面设立专门负责机构。2019 年，美国成立了网络安全局，专门向其合作伙伴提供关于大规模网络诈骗的相关线索。泰国成立网络犯罪调查科，负责处理泰国境内各种形式的网络犯罪，并受理各类投诉，同时由科技罪案调查科处理与科技有关的电信网络诈骗案件。另一方面建立跨部门协调机制。2018 年，英国金融业协会与英国财政部、伦敦市警察局、大都会警察局联合成立专用卡和支付欺诈专案组，专职打击欺诈类犯罪。

关注重点人群，筑牢电信网络诈骗防火墙。美国于 1994 年制定发布了《打击针对老年人的营销骗局法》，加强了对于老年人的保护；2019 年，美国司法部宣布，将对诈骗老年人的欺诈行为进行大规模打击。德国于 2018 年成立了专项调查小组，定向打击针对老年人的电信网络诈骗犯罪；开展“老年人告知老年人”项目，招募退休警官为志愿者，定期面向老年人组织各类讲座，分享最新的诈骗案例和防范手段。

强化技术能力建设，提升事前事后精准治理能力。在诈骗电话拦截方面，德国联邦刑事犯罪调查局联合其他单位成立了专门机构，用技术手段加强对骗术的甄别，对诈骗行为进行前期拦截。美国通信业巨头，如 AT&T、苹果、谷歌等联合成立了“反自动呼叫电话打击行动组”，开发了主叫号码 ID 识别技术，能够

屏蔽虚假号码拨出的诈骗电话。在诈骗电话提醒方面，自 2013 年起，日本政府每年拨款约 10 亿日元，专门用于在老人的家庭电话上安装电话录音机，当有疑似诈骗的海外电话或网络电话拨入时，警方的诈骗电话检测系统会自动启动。2020 年，英国监管机构推出欺诈广告警告系统，对互联网上的诈骗广告进行监测与拦截，同时，通过该系统用户可以举报欺诈性广告。在诈骗钱财转账止付方面，日本欧姆龙公司开发出一款装有人工智能识别设备的 ATM 机，如果 ATM 机摄像头捕捉到操作者正在用手机通话或是戴着口罩、墨镜的画面，该 ATM 机就会在屏幕上发布警告，要求操作者摘下口罩和墨镜。在诈骗资金追踪方面，英国金融协会和英国零售支付服务提供商 Pay.UK 联合开发了账户追踪方案，能够跟踪可疑交易，还能在交易确认前检查收款账户背景信息的真伪，防止支付欺诈。

加强社会监督与宣传引导，织密群防群控安全网。在畅通社会监督渠道方面，美国成立了网络诈骗投诉中心，用于受理各类网络诈骗投诉，并利用大数据分析和比对技术打击网络诈骗。澳大利亚政府设立了专门的举报网站，以受理民众举报诈骗电话等。在提升民众防范能力方面，美国、俄罗斯、英国、新加坡等国家均在其官方网站发布近期常见的电信网络诈骗手法，并为用户提供信息核查验证渠道；澳大利亚举办系列活动，展示当前电信网络诈骗新技术以及防范措施，同时编印《诈骗小黑书》，详细介绍了最常见的诈骗手法以及防范措施，并翻译成 10 种语言供大家参考学习。（摘自：国外是如何治理电信网络诈骗的？）

来源：人民邮电报　2021-02-01

英国网络犯罪防范与治理

（一）网络风险防范

在英国，一些网络犯罪活动团伙通常冒充被害人的熟人、同事和社区警察等身份实施犯罪。“精准式”作案的网络犯罪团伙通常花费数小时研究侵害对象，以确定特殊的话术，使被害人放松警惕。在各式各样的网络诈骗已构成重大威胁的背景之下，英国金融行业机构与英国警方、保险机构等一系列合作伙伴共同建立了“冷静五分钟”（Take Five）组织，旨在为公众提供最为可靠直观的防范网络犯罪与诈骗建议，帮助每个人免受可预防的金融类诈骗。该组织对冒充类网络诈骗提供了“三步走”的应对策略：第一步，停下来（Stop），即在向对方发送信息或转出资金之前，花点时间停下来想一想，这样是否是安全的操作；第二步，多琢磨（Challenge），即对特殊情形下的犯罪问题进行冷静思考，对相关情

形的真伪性予以辨别，拒绝或忽略非法的网络请求；第三步，及时保护（Protect），如果认为已经上当受骗，可立即联系有关银行或向英国反诈骗行动局报告。

此外，英国民众还可通过多种途径开展网络犯罪报告与安全防范工作。例如，国家网络安全中心提供了丰富的学习与防范网络安全风险专门知识，民众可访问其官方网站进行网络安全专业知识学习；如果民众遭遇了网络犯罪，既可以到当地警局报案，也可以通过英国反诈骗行动局官方网站和“03001232040”24 小时专门服务电话进行报案，还可通过上述专门电话就网络犯罪防范问题咨询专家；如果对一些问题有顾虑或为了进一步保护个人隐私，还可通过“犯罪终结者”提供的“0800555111”24 小时服务电话及专题网站栏目进行举报。同时，英国政府还与“犯罪终结者”联合设立了涉新冠肺炎疫情类诈骗举报电话“08005875030”，促使公众对不断演变的网络诈骗提高警惕。

需要说明的是，英国反诈骗行动局是专门针对欺诈和网络犯罪的国家报告中心，是英国唯一的国家犯罪报告系统，亦称“英国反欺诈和网络犯罪报告中心”，该机构诞生于 2005 年，其前身隶属于国家反欺诈局（NFA）。2014 年 4 月，反诈骗行动局正式转隶到伦敦警察厅，而后者是负责打击经济犯罪的全国警察领导机构，因此，转隶后的反诈骗行动局管辖权限与各项打击网络诈骗犯罪的职能得到了巩固和增强。如今，反诈骗行动局通过与国家反欺诈情报局合作，为诈骗和网络犯罪的受害者提供更紧密的点到点服务，这一工作制度已为个人和企业提供了许多至关重要的处置对策，增强了英国执法机关查处网络犯罪的能力。

（三）网络犯罪治理

2016 年以来，为了遏制网络诈骗犯罪与其他网络犯罪不断蔓延的趋势，英国制定了一系列打击治理网络攻击类、网络侵财类犯罪的制度，组织包括行业部门、行政机构、监管机构、执法机构和海外相关组织在内的成员参与英国网络犯罪治理。成立于 2016 年 10 月的英国国家网络安全中心，即是网络犯罪治理的专门机构，其总部位于伦敦，隶属于英国政府通讯总部（GCHQ）。该中心汇集了来自英国政府通讯总部信息保障部、网络安全评估中心、国家网络安全应急响应团队以及国家基础设施保护中心的专家学者，可以为中小企业、各类大型组织、政府机构、社会公众和社会部门提供专门性的网络犯罪防范治理帮助。该中心还与英国其他执法部门、国防机构、情报与安全机构以及国际合作伙伴开展相关合作，以促进英国形成安全的网上办公和互联网生活环境。

此外，英国还在网络安全案件处置与风险防范、专门机构与辅助机构协同治

理等方面开展了积极的犯罪防范与治理工作，成立了包括“犯罪终结者”“冷静五分钟”在内的各类网络犯罪协同治理机构。通过“犯罪终结者”平台，公众可以通过电话或网络的方式全天候进行网络犯罪信息的匿名举报。举报信息将被分析、研判，随即发送至英国犯罪打击与犯罪治理机构，包括举报者所在地的警察局、边境管理局、税务海关等部门，进而由相应的机构承担犯罪调查、嫌疑人逮捕和提起刑事诉讼的法律责任。各类网络犯罪协同治理机构在其官网和各类媒体平台上分享了众多免受网络犯罪侵害的专业建议，以增强英国群众的网络安全防范意识。（摘自：【特别策划】外国防范打击网络犯罪|英国网络犯罪现状及治理）

来源：现代世界警察杂志　2022 年第 8 期