中国移动 China Mobile

防范电信网络诈骗警示案例汇编

中国移动通信集团有限公司
网络安全领导小组办公室
2022年2月

目 录

前　言

2021 年 4 月，习近平总书记对打击治理电信网络诈骗犯罪工作作出重要批示，强调要坚持以人民为中心，全面落实打防管控措施，坚决遏制电信网络诈骗犯罪多发高发态势。集团信安中心坚决贯彻“第一议题”制度，落实党中央、国务院以及各上级单位要求，以习近平总书记“以技术对技术，以技术管技术”的重要指示精神为指引，在网信安全治理中创新引入舆情监测技术手段，聚焦治理业务需求、提升监测分析能力，综合运用大数据分析、人工智能、态势感知等新型技术手段，实现了对网信安全事件的全面采集和发展态势预测，重点针对各类诈骗事件开展了全面监测与深入分析，在有力支撑打击治理工作加快从“事后处置”向“事前预防”转变的同时，收集整理了大量互联网诈骗案例。

截至目前，依托舆情监测系统，中心主动监测发现热点诈骗事件近 200 起。为了更好地应对网络安全形势发展，纵深推进打击治理相关工作，我们选取了具有代表性、典型性的 7 大类 26 小类 93 个案例结集成册，供各单位参考。

第一章 公共服务类诈骗

（一）社保诈骗

1、社保卡被冻结诈骗

媒体时间：2021 年 6 月 22 日

摘要：近日，大量市民接收到 0065、0067 或 65（11 至 13 位数字）等开头的境外电话，要求市民到社保中心大厅办理相关业务，且大部分是以中老年女性群体为主。据了解，这些电话内容通常为：“您的社保卡（医保卡）异常，涉及某件刑事案件，公安机关正在调查，请配合……”“您的社保卡（医保卡）在异地被盗刷，已冻结！”“您的社保卡（医保卡）涉嫌诈骗……”。

链接：https://baijiahao.baidu.com/s?id=1703154001293740350&wfr=spider&for=pc

2、社保卡升级诈骗

媒体时间：2021 年 9 月 6 日

摘要：近期出现在线升级社保卡诈骗，主要内容是：全国社会保障卡统一升级电子版本，请于某月某日前打开 XX.XXX.CC（网址会有变化）在线办理。骗子冒充社保中心以“办理新版电子社保卡、社保账户未上传电子审核、社保卡业务被冻结”等理由向受害者发送包含链接的诈骗短信，有的还会要求受害人“限期”办理，否则“过

时将被注销账户”“逾期将停用您的社保”。

链接：https://weibo.com/ttarticle/p/show?id=2309404678356888322196&sudaref=www.baidu.com

3、医保卡更换诈骗

媒体时间：2022 年 1 月 14 日

摘要：近日，辽宁省医疗保障局官方微信发布消息称，辽宁省医保局接到部分群众反映，有不法分子向该省参保群众推送诈骗短信，相关内容为“【辽政通】你名下的医保已停用，请进 ****** 申换电子版使用”，内含虚假链接（实为木马病毒链接），诱导受害人点击该链接。点开链接后，跳转的页面与官方网页非常相似。如果按页面上的提示填写了身份证号、银行卡号、银行卡密码、预留手机号、验证码等信息，会导致受害人手机和银行卡等信息被盗，银行卡被盗刷受损。

链接：http://news.jcrb.com/shxw/202201/t20220114_2356394.html

4、医保卡停用诈骗

媒体时间：2021 年 10 月 18 日

摘要：10 月 5 日，厦门市民洪先生报警称当日 8 点多收到一条短信，内容是“闽政通”通知其名下医疗保障卡即将停用，需要点击某个网站查询，未升级的将统一暂停使用。洪先生相信这是“闽政通”发来的，于是点击查询，没想到按要求输入个人资料后还要进行所谓“验证”-- 即填写银行卡密码。随后洪先生按要求分三次提供了手机收到的银行发送的短信验证码后。银行卡账户便被扣款，

直到收到银行扣款短信洪先生才意识到上当受骗了。

链接：https://www.sohu.com/a/495732124_121106994

（二）ETC 诈骗

1、ETC 失效诈骗

媒体时间：2021 年 5 月 31 日

摘要：去年 10 月四川巴中的冯先生手机收到一条短信，提醒他的 ETC 账户将于 30 日内失效。冯先生按照链接页面要求，输入了自己的姓名、身份证号码、银行卡号、密码、手机号提交。然而，当他再次输入手机验证码进行提交时，短短几秒钟，冯先生接连收到 4 条短信，银行卡内的 11900 元被迅速盗取。

链接：https://baijiahao.baidu.com/s?id=1701260766907984558&wfr=spider&for=pc

2、ETC 通行证被锁定诈骗

媒体时间：2021 年 6 月 17 日

摘要：近日，不少北京市民向知道君反映，收到短信告知 ETC 通行证被锁定，要求立即进入一网址进行重新认证，以恢复使用。6 月 16 日上午，知道君从 ETC 发行公司处得到证实，此类信息为诈骗信息。

链接：https://www.sohu.com/a/473108370_103567

3、ETC 被封解冻诈骗

媒体时间：2021 年 9 月 14 日

摘要：据李先生介绍，今年 7 月 3 日，他收到了一条＋ 9181458596852 的电话号码发来的短信，短信内容为：车主您好，系统显示您的 ETC 状态已被禁用，请前往指定网站申请解除，延迟将被限制使用。“我当时并没有相信这条短信的内容，但是过了 15 天，我再次收到了一条短信，内容是我的电子 ETC 已经进入禁用状态，让我立即点击指定网址解除禁用，我就相信了，担心以后无法在高速公路上使用 ETC。”于是，李先生根据提示，打开网址，填写了自己的个人信息，其中包括办理 ETC 时使用的信用卡账号和密码，并且进行了人脸识别，得到了“ETC 成功激活”的提示。此后，李先生认为已经没有问题，直到 8 月 28 日，李先生收到一条短信称自己的信用卡在贵阳市南明区某珠宝行消费了 4999 元。恍然大悟的李先生意识到自己遭遇了电信诈骗，于是立即报警。

链接：https://news.qingdaonews.com/qingdao/2021-09/14/content_22882037.htm

4、车辆禁止高架通行诈骗

媒体时间：2021 年 9 月 18 日

摘要：近日，有群众收到“您的车辆已被禁止高架通行”“您的 ETC 卡处于禁用状态”短信，点开链接后发现跳转页面与官方网页非常相似，误以为自己车辆或者 ETC 卡真的出问题了，于是按页面上的提示填写了银行卡号、预留手机号、密码等信息。随后，你就会收到银行发送过来的钱款转走的信息。

链接：http://baijiahao.baidu.com/s?id=1711203804912317353

（三）票务（改退签）诈骗

1、航班改签诈骗

媒体时间：2021 年 4 月 28 日

摘要：陈先生近日收到了一条自称是航空公司发来的短信，称其预订的航班由于飞机故障取消了，要求陈先生拨打专线电话改签或退票，且每位旅客有 200 元误机补偿。短信上留有航空公司客服电话，于是陈先生通过上面的电话与对方联系。之后，“客服”告知陈先生要通过支付宝办理退款，并提供一个支付宝账号引诱陈先生按照提示操作，添加对方为好友，开通“亲密付”功能。由于陈先生不了解亲密付功能，所以并未对此产生怀疑，直到最后才发现自己支付宝被转走近一万元。

链接：https://new.qq.com/omn/20210428/20210428A0EF7A00.html

2、购买北京环球影城门票诈骗

媒体时间：2021 年 9 月 6 日

摘要：北京环球影城宣布试运行日期当天，小王在微博上查看环球影城的相关信息时，看到微博用户发布了有门票可出售的帖子，并配有环球影城内的照片。小王询问后对方表示，自己是官方授权渠道，可以出票，1000 元一张。购票需要填写姓名、身份证号、手机号等信息，填好信息后在官网下单，收到订单短信通知后，支付票款。之后对方称，“由于支付宝大面积风控，造成支付成功率大幅降低”，要求用手机银行转账，并给出了银行卡账号和收款人姓名。

小王付款 1000 元后，其又称购票流程出了问题，需要重新转账 1001 元，之前的 1000 元会退回。对方以各种借口，两次要求转账，小王觉察到可能是骗子。

链接：https://www.sohu.com/a/488100552_121117454

3、机票退票诈骗

媒体时间： 2021 年 12 月 29 日

摘要： 12 月 7 日，拉萨市民罗某（化名）通过某 APP 购买机票，后来罗某因故想要退票，于是在某浏览器中搜索该 APP 的客服电话，准备联系退票。罗某拨通了网络上显示的假客服电话，并按照这名假客服的提示操作，最终被骗 11021 元。

链接：https://baijiahao.baidu.com/s?id=1720495716061279827&wfr=spider&for=pc

4、【冬奥】购买门票诈骗

媒体时间： 2022 年 2 月 8 日

摘要： 1 月 18 日，北京奥组委发布通知：“鉴于疫情防控形势依旧严峻复杂，为保障涉奥人员和观众的健康安全，决定将原计划通过公开销售门票的方式调整为定向组织观众现场观赛”。打着“有票”“有渠道”的旗号找你卖票都是骗子。

链接：https://baijiahao.baidu.com/s?id=1724167734792136588&wfr=spider&for=pc

（四）医疗诈骗

1、HPV 疫苗预约诈骗

媒体时间： 2021 年 8 月 24 日

摘要：骗子通过微博、小红书等平台，发布“代抢”、“代预约”九价 HPV 疫苗的虚假消息，等待受害人主动联系。骗子作出“包预约、不打包退”等虚假承诺或出示相关接种九价疫苗手续后骗取受害人信任，获取受害人手机号、身份证等个人信息，发送预约成功的虚假短信。再以“手续费”、“转账超时”、“流水不足”等理由，要求受害人继续缴纳费用。收到钱款后，又利用疫苗的预约特性，不断拖延接种时间，继续蒙骗受害人，最后将受害人拉黑。

链接：https://www.163.com/dy/article/GI5UIEUI0534A4S1.html

2、“基因检测”“癌症筛查”诈骗

媒体时间：2022 年 1 月 4 日

摘要：该犯罪团伙先打造一个女性、生物科技公司工作人员的人设，然后加对方微信进行聊天。他们逐步把自己塑造成“暧昧对象”“专业人士”等形象，摸清目标对象的身份、职业、经济水平等关键信息，经过大量的话术铺垫，他们将“基因技术”“癌症筛查”等概念灌输到目标对象脑海中，同时利用普通人群对专业技术的认知差异，加剧目标对象对罹患癌症的恐慌心理，从而开始信任骗子。火候成熟后，骗子就会介绍自己“长期合作”的“实验室”，以“低于市场基因检测价格”的噱头吸引受害人前去检测。在受害人拿到“基因报告”并为此崩溃恐慌时，这伙诈骗分子便趁机推出了“自己公司研制的、专门针对高风险人群早期保养”的“益生菌”“钛”等保健品。

链接：https://baijiahao.baidu.com/s?id=1721001057760864158&wfr=spider&for=pc

3、献血保证金诈骗

媒体时间：2022 年 1 月 9 日

摘要：近日，上海一市民报案称被骗 30 元保证金。经调查，诈骗分子在微信群里发布“献血 400 毫升，补偿 1200 元”的信息，于是相关受害者加了诈骗分子的微信，按照诈骗分子的要求，每人转了 30 元保证金并发送身份信息。次日，受害者们赶到献血领取补偿的集合点，诈骗分子却解散相关微信群并删除受害者们的微信。

链接：https://www.sohu.com/a/516605029_120721950

4、【新冠】核酸检测登记诈骗

媒体时间：2021 年 6 月 11 日

摘要：近日，深圳警方发现一种新型的诈骗手法，不法之徒将诈骗短信包装成防疫提示来行骗。居住在龙岗区的邱先生就收到这样一条短信：要求他到福田区 3 小时内把核酸做了，否则承担法律责任。短信后面还附有输入银行卡等信息的链接。

链接：https://weibo.com/tv/show/1034:4646822518652962?from=old_pc_videoshow

5、【新冠】加钱快速出核酸结果诈骗

媒体时间：2021 年 8 月 30 日

摘要: 近期网络上有一些人声称，可以“快速出核酸检测结果”“加急最快半个小时就出结果”，不过需要额外收费。记者确认，核酸结果一定要由经卫健部门认证的具备资质的医院或第三方检测机构出具。根本没有所谓的私人渠道。不要轻信网络不实信息和所谓“私

人渠道”。这不仅可能影响自身正常出行，更有可能落入不法分子非法敛财的骗局。

链接：https://m.gmw.cn/baijia/2021-08/30/1302521733.html

第二章 金融类诈骗

（一）投资诈骗

1、投资共享充电桩诈骗

媒体时间： 2021 年 12 月 12 日

摘要： 受害人收到了一条短信，“2022 年赚钱新风尚，你投资，我建桩，坐在家里把钱抢。共享充电桩火爆来袭，机会有限欲购从速。”因受害人对电动汽车及充电桩有些了解，随后联系上了对方，并且约见了当面沟通。诈骗分子表示现在融资，只需要投入一部分资金，就可以在家里坐享其成。随后受害人投资近 20 万元。前几个月，受害人都顺利地收到了公司的转账，随后几个月就没有再收到每个月的返利，其公司业务员等联系不到。受害人才意识到自己被骗。

链接：http://baijiahao.baidu.com/s?id=1718848032119613246

2、网络关键词投资诈骗

媒体时间： 2021 年 12 月 23 日

摘要： 一名自称是高琴发展信息科技有限公司员工的人给他打电话，说可以通过网络推广服务让廖先生的钢材得到更高的销售量，在对方的劝说之下，廖先生最终花了 5 万块钱，购买了一个叫“江西钢材”的关键词。不久之后，有人打电话给廖先生，称愿意花 50 万购买其名下的关键词，廖先生当即便联系了高琴发展的工作人员，

在一连串的专业名词攻势下，廖先生同意让该公司帮忙为其代理代办，随后便通过微信转账、网银转账共支付给陈经理 1 万元的服务费。

交完钱后廖先生时常便会打电话询问，可对方总以“买方”找各种借口拖延不付款为由一直拖延，直到对方电话停机找不到人。廖先生向新余警方报警。经查证，廖先生手中注册关键词的凭证均为仿造并无实际作用。

链接：https://baijiahao.baidu.com/s?id=1719899404381864206&wfr=spider&for=pc

3、创业投资诈骗

媒体时间： 2022 年 01 月 26 日

摘要： 江苏常州，计算机专业的沈某某曾是学生会主席，在校期间他谎称自己在开发游戏软件，希望老师能投资，老师初期投资了约 4 万元。随后，沈某某谎称游戏已在平台售卖并盈利，该老师继续追加投资，到 2021 年 5 月共投入 400 余万元。沈某某用诈骗所得将自己包装成创业成功人士，骗取多位同学钱款共约 100 万元。沈某某获刑 11 年。

链接：https://weibo.com/2286908003/LcpuincXm

4、【冬奥】虚假奥运募捐诈骗

媒体时间： 2022 年 2 月 7 日

摘要： 犯罪分子利用群众对冬奥会的特殊情结，通过编造虚假感人故事或某运动员家庭贫困背景需要资助等，骗取市民同情，并以“网络募捐”形式骗取钱财。

链接：https://m.gmw.cn/baijia/2022-02/09/1302796394.html

（二）银行（卡）诈骗

1、冒充“晋商银行”诈骗

媒体时间：2021 年 4 月 20 日

摘要：从 4 月 19 日开始，有诈骗团伙向太原市晋商银行客户大量发送诈骗短信。不法分子冒充晋商银行工作人员以“手机预留信息即将停用”为由，诱骗市民点击虚假链接网站。此类短信皆显示在境外发送，且内容中还带有繁体字，当用户点开链接后，还会出现带有伪造晋商银行标识的虚假网页信息，诱导用户填写个人信息、银行卡号、密码甚至是验证码。不法分子一旦获取受害人的银行卡号、身份证号及密码、验证码等重要信息后，便可迅速通过银行快捷支付等功能盗刷受害人银行卡内存款。

链接：https://m.thepaper.cn/baijiahao_12296973

2、冒充 “农商银行”诈骗

媒体时间：2021 年 12 月 8 日

摘要：近期，青海省居民收到冒用“农商银行”名义发送的诈骗短信“尊敬的用户您可在我行申请一笔储备款”。一旦点击短信内的链接并填写个人信息，账户资金将被盗取。

链接：http://news.sohu.com/a/506476506_121123826

（三）贷款诈骗

1、网贷广告诈骗

媒体时间：2021 年 4 月 24 日

摘要：江苏的陈先生轻信网贷广告，30 万贷款没到手却被骗走近 16 万。经调查，此类诈骗广告系套用、伪造金融机构的资质，而平台审核不严，为赚钱睁一只眼闭一只眼。

链接：https://www.sohu.com/a/462850894_115060

2、网贷提现诈骗

媒体时间：2021 年 9 月 13 日

摘要：近日，苏州市民李先生报警，称自己被骗 10 余万元。一开始，李先生转账 8 万余元但网贷无法提现，此时他察觉到不对前往报警。但途中对方表示，李先生只要再打 2 万元解冻费，就可将所有钱退还至账户上。李先生抱着侥幸的心理，又转出 2 万元。

链接：https://weibo.com/1618051664/KxPYyEVuY?refer_flag=1001030103_&type=comment

（四）数字货币诈骗

1、虚拟币“杜鹃花”诈骗

媒体时间：2021 年 9 月 8 日

摘要：不法分子周行等人通过航空服务公司，自 2018 年起推出虚拟币“杜鹃花”，编造“购买‘挖矿机’就可将每日走路的步数转化为‘杜鹃花’在海外市场交易所交易”等谎言，在一年的时间内骗取全国多地 1000 余名被害人钱财 3.1 亿元。

链接：https://www.toutiao.com/i7005139275670929924/

2、虚拟货币投资诈骗

媒体时间：2021 年 6 月 29 日

摘要：目前利用虚拟货币、区块链等新技术产物进行电信网络诈骗案件更是越来越多。从以往的案例中发现虚拟货币诈骗者（团伙）大多利用各种各样的“空气币”，配合各类不法的网络交易平台收割用户。主要手法有诱导用户进行虚拟币投资，要求受害者转账；冒充交易平台客户，要求用户认证身份，骗取受害人账户信息等。

链接：https://www.jinse.com/blockchain/1119813.html

3、数字人民币电子支付诈骗

媒体时间：2021 年 12 月 29 日

摘要：近日，一名自称是公安局民警的人打来电话称受害人涉嫌骗保，称受害人涉嫌洗钱诈骗。对方不仅向她展示逮捕令，还恐吓她要坐牢。而且为了能够顺利实施诈骗，犯罪嫌疑人要受害人避开人群，去酒店单独开一间房进行通话。其间，骗子让受害人下载诈骗 app，远程操控受害人手机，并通过录制受害人与其谈话时全程的人像的图像，采集了受害人左右摇头、张嘴、眨眼的视频，在受害人不知情的情况下开通了她的“数字人民币”钱包，并迅速把钱转走。

链接：https://www.ersanli.cn/article.html?newsId=1212200948997 41&type=1

4、区块链投资诈骗

媒体时间：2021 年 9 月 16 日

摘要：“股票行情不好，投资区块链能获得几倍甚至几十倍的回报！”面对被区块链技术“精装修”的数字虚拟货币投资，数千名被害人趋之若鹜，但最终损失惨重。殊不知，拥有华丽外表的虚拟货币投资背后，是一个组织严密、分工明确、成员众多的庞大诈骗集团。陈先生在投资交流群中受“投资大佬”影响，决定申购 30 万元名为“BKC”的数字货币。 随后，陈先生收到一款名为“LKF”的平台链接。该平台看起来和平时炒股的 App 非常相似，赚钱心切的陈先生没有多想，就在该平台投资了 30 万元购买数字货币。转账后，陈先生发现该平台有 6 个月的锁仓期，锁仓期满才能交易。虽有些担忧，但陈先生每天看着平台上自己投资的数字货币涨势喜人，心里就踏实多了。 没过多久，平台忽然无法登录，平台工作人员也相继失联。陈先生意识到自己被骗，随即向公安机关报案。

链接：http://news.jcrb.com/jsxw/2021/202109/t20210916_2319985.html

（五）网络新概念诈骗

1、元宇宙区块链游戏诈骗

媒体时间：2021 年 12 月 13 日

摘要：记者发现，无论是何种形式的元宇宙区块链游戏，都需要用户将人民币兑换为 USDT 这种虚拟币，再兑换成该游戏所使用的虚拟币。而在 2017 年，央行等就明确指出，所谓“虚拟货币”，本质上是一种未经批准非法公开融资的行为。业内人士告诉记者，网

络上鼓吹的“元宇宙链游”，只是借着元宇宙概念炒作推广的骗局。许多区块链游戏本质是款网页小游戏，开发成本很低，对外宣传可以理财赚钱，其实只是拿后入场的人支付的资金来填补窟窿。

链接：https://weibo.com/2258727970/L5T5Qy0iN

2、元宇宙培训课程诈骗

媒体时间：2021 年 11 月 23 日

摘要：近来，“元宇宙”成为热门话题，越来越频繁地出现在人们的视野里，各类打着元宇宙旗号的套路与骗局已经有滋生的苗头。一些知识付费项目把元宇宙包装成一夜暴富的机会，声称“未来只有元宇宙这一条路”，以贩卖焦虑的方式借机敛财。一些人言必称元宇宙，没有任何与之相关的实体内容却热衷制造噱头，挖空心思从元宇宙概念中分得一杯“流量羹”。

近期开设元宇宙培训课程的平台越来越多。大致上内容也有不少雷同，其内容主要是邀请专家来分享如何通过大数据来对乡村经济进行更好地治理以及如何更好地实现乡村的信息化建设。这实在是一种“挂羊头卖狗肉”的行为。

链接：https://baijiahao.baidu.com/s?id=1717147318657389774&wfr=spider&for=pc

第三章 社交类诈骗

（一）游戏、APP 软件诈骗

1、“合成大西瓜”游戏诈骗

媒体时间：2021 年 2 月 7 日

摘要：2021 年 2 月 7 日，合成大西瓜被骗 19.9 元出现在微博热搜榜上第 7 位。诈骗手段：微博网友反映，在玩该游戏时，其页面右上角会出现宝箱图标，玩家选择点击后，会跳转至抽奖界面，其中的奖品为「100 元手机话费券」，逢抽必中。而如果玩家想要得到奖品，需支付 19.9 元购买。支付后，页面则弹出让你下载某款 APP，去该 APP 领取话费。可很多网友反映，根本就没有话费，退款也遇到阻碍，申请退款迟迟收不到退款，“在公众号申请客服也没有回应。”

链接：https://baijiahao.baidu.com/s?id=1691031297794659186&wfr=spider&for=pc

注：合成大西瓜是微伞游戏推出的小游戏，此前因核心玩法与娱乐圈「吃瓜」热点挂钩而爆红网络。

2、游戏账号交易诈骗

媒体时间：2021 年 6 月 28 日

摘要：市反诈骗中心提醒：暑假来临，游戏账号（装备）交易类诈骗进入高发期。游戏玩家们务必提高警惕，游戏开发商不支持

私人间的游戏账号装备买卖，不要相信网友提出的“官方交易平台”。凡是客服称账号被冻结，要交解冻金、保证金等费用的，都是诈骗。家长们也要注意，不要把自己的银行卡绑定在未成年人使用的微信、QQ 上，提醒子女注意用网安全，提高防范电信网络诈骗意识。

链接：https://appshare.hualongxiang.com/wap/thread/view-thread/tid/15615523

3、新型游戏诈骗

媒体时间：2021 年 10 月 25 日

摘要：近期出现了一种新型游戏诈骗。换汤不换药的是，他们依旧是利用虚拟交易平台来实施诈骗，只是骗子的准备更加充分。骗子假冒了买家、客服、警察等多重身份，融合了道德压制、恐吓等多种心理操控术，已然是一套成熟完善的话术。

新型游戏诈骗套路：

1、以“玩家”的身份购买游戏账号。

2、引导卖家进入虚假“游戏交易平台”。

3、伪造成功支付页面。

4、假冒客服，要求充值为资金解冻。

5、心理战术，道德压制。

6、假冒警察，威胁恐吓。

链接：https://baijiahao.baidu.com/s?id=1714554632300625600&wfr=spider&for=pc

4、色情软件购买诈骗

媒体时间：2021 年 12 月 20 日

摘要：2021 年 2 月，江苏无锡梁溪警方接到群众报警，称其因没有经受住诱惑，下载安装了一款色情软件 APP，按照软件内的提示付款 1 元开通会员，却收到银行卡消费 2271 元的短信提醒。几乎同一时期，当地警方又掌握了多条线索指向此类“灵异事件”，无锡市公安局网安支队遂会同梁溪分局立案侦查。经查，此 App 开通会员界面中显示：“仅需支付 1 元即可观看海量视频。”支付界面上也的确显示支付金额为 1 元，所以许多当事人却在扫码被扣数千元钱后浑然不知，只有部分开通短信提醒的当事人发现。

链接：https://baijiahao.baidu.com/s?id=1719653783804195726&wfr=spider&for=pc

5、微信红包封面诈骗

媒体时间：2022 年 1 月 20 日

摘要：最近有不少明星、公众号、游戏等发放红包封面，有些红包封面通常是限量发布，有些抢不到的网友就会考虑去买一个。最近一段时间微信安全发现了不少售卖红包封面序列号的骗子，声称自己有大量的红包封面，价格从数元到数十元不等。这些骗子会告诉买家，序列号属于虚拟商品，必须先付款，交易时骗子还会避开交易平台，收钱后就拉黑买家。

链接：https://baijiahao.baidu.com/s?id=1722440767292293016&wfr=spider&for=pc

6、“集五福”诈骗

媒体时间：2022 年 1 月 23 日

摘要：这两天，“敬业福”登上了热搜，今年新一轮的“集五福”

活动已经上线。不法分子通过网上二手交易平台、QQ、微信等社交软件，发布售卖福卡等信息，引诱受害者进行交易，不法分子在收到钱财后直接将受害人拉黑或失去联系。

链接：https://baijiahao.baidu.com/s?id=1722756897119538947&wfr=spider&for=pc

（二）杀猪盘诈骗

1、【新冠】接种护士加好友诈骗

媒体时间：2021 年 6 月 6 日

摘要：这是新出现的借助新新冠疫苗诈骗的手法，但与通常杀猪盘诈骗的套路一致，只是加好友的理由不同。有可能是新冠疫苗注射或登记信息被泄露，也有可能是因为新冠疫苗注射普及，诈骗分子群发撒网。建议对新冠疫苗诈骗短信策略进行加强，对“登记电话”“接种护士”等词进行策略配置观察，阻止不良信息传播。

链接：https://baijiahao.baidu.com/s?id=1701889495109265611&wfr=spider&for=pc

2、网络交友找“真爱”诈骗

媒体时间：2021 年 11 月 15 日

摘要：11 月 10 日，富春街道李某（化姓）报警称 :10 月初其在某视频软件上认识一名男子，添加微信联系一段时间后感情逐渐升温。近期，对方称有朋友在投资平台做后台维护，有内幕消息稳赚不赔，李某十分心动。在对方指导下李某发现投资平台确实能赚钱提现，放下警惕后加大投资金额，后平台无法提现，累计被骗 90 万

余元。

链接：https://m.thepaper.cn/baijiahao_15397557

（三）直播打赏诈骗

1、直播打赏被骗

媒体时间：2021 年 7 月 14 日

摘要：2021 年 2 月，浙江杭州“00 后”小伙杨某为要回给女主播小方刷的 80 万元礼物，以投资电商为由将小方拉到了一个三人微信群中。之后，杨某一人分饰两角，先后三次忽悠小方将 21.2 万元转入其提供的支付宝账号中。2 月 20 日，小方屡次要求还款未果，遂报警。近日，经杭州市富阳区检察院提起公诉，法院以诈骗罪判处杨某有期徒刑三年，缓刑四年，并处罚金人民币 3 万元。

链接：https://weibo.com/1896650227/KoFtpFJ3Y

2、诱导粉丝刷礼物诈骗

媒体时间：2021 年 8 月 3 日

摘要：近年来，网络直播持续火爆。在直播中，用户给人气主播刷礼物、冲榜是直播变现的重要手段之一，然而直播平台鱼龙混杂，主播诱导粉丝刷礼物的背后，实则暗藏着精心的骗局。今年 5 月份，黑龙江哈尔滨警方捣毁一个利用网络直播进行诈骗的犯罪团伙。

链接：https://tv.cctv.com/2021/08/03/VIDElnXTgdgYe2R4LeWykgh3210803.shtml

3、网恋刷礼物诈骗

媒体时间：2021 年 8 月 26 日

摘要：近日，浙江金华。据义乌公安，陪玩主播黄某用假照片和小傅谈恋爱，小傅为其刷礼物转账达 318 万元。黄某还与其他几名男子保持“恋爱关系”。目前，该主播涉嫌诈骗被刑拘。

链接：https://weibo.com/5044281310/Kvcw9iGIW

（四）共享屏幕诈骗

1、视频会议 APP 共享屏幕诈骗

媒体时间：2021 年 4 月 20 日

摘要：共享屏幕是把屏幕上显示的内容同步让对方看到，包括弹框显示短信、微信、其他 App 推送的内容。也就是说，你在手机上的任何操作，对方都能看到。国家反诈中心提醒，如果有陌生人给你打电话，并提到腾讯视频会议、共享屏幕等字眼，你要当心了，这很可能是诈骗。

链接：https://m.thepaper.cn/baijiahao_12309259

2、“假客服”+“共享屏幕”诈骗

媒体时间：2021 年 7 月 14 日

摘要：近日，受害人小燕前往当地公安机关报警，称自己接到一通陌生电话，对方说自己是某金融平台的客服人员，告诉小燕她在大学时使用过该平台的校园贷，如果不注销就会影响她之后的征信。小燕又陆续收到很多对方发来的邮件，看到里面有抬头是“中

国银行业监督管理委员会”之类的截图。于是按对方要求下载了一款 App，跟着指示操作了多个银行账户上的存款。在两个小时里，小燕分多次将 18 万元打到对方提供的账户上。小燕表示，骗子在诈骗时还使用了云会议软件。小燕在屏幕上的任何操作都在对方的监视下，但她自己当时却并没有意识到。

链接：https://www.toutiao.com/a6984617385290433063/?tt_from=weixin&utm_campaign=client_share&wxshare_count=1&timestamp=1626242278&app=explore_article&utm_source=weixin&utm_medium=toutiao_ios&use_new_style=1&req_id=2021071413575801021207521600C0C2E08&share_token=BA6A6520-B9D8-4483-B8CD-8E342C910763&group_id=6984617385290433063

（五）邮件诈骗

1、虚假工资补贴邮件诈骗

媒体时间：2021 年 9 月 18 日

摘要：近日，江苏南京市民徐女士收到了一封内容为“工资补贴通知”的企业邮箱邮件。徐女士点击进入页面，邮件显示只需扫描邮件内的二维码，按照流程如实填写信息便可获得补贴，徐女士按照提示输入了银行卡号、身份证号、手机号以及银行卡的可用额度，随后还收到了一条短信验证码，徐女士将相关信息全部输入，便受到银行卡扣款 10000 元的信息。

链接：https://www.12377.cn/aqyj/2021/dec1f73e_web.html

2、TikTok 钓鱼邮件骗局

媒体时间：2021 年 11 月 18 日

摘要：研究人员监测到一个针对 TikTok 用户的网络钓鱼邮件活动，主要涉及拥有大量粉丝的“网红”、工作室等账号。钓鱼邮件分为两种类型，但骗子都会冒充成 TikTok 的客服人员，一种是通过发送邮件告知用户账号因涉嫌违反平台规定将被立即封号，而另一种方式则截然相反，通过邮件告知用户账号已通过认证。TikTok 的认证机制能够提高账号的可信度和真实性，并在流量和推荐算法上给予更多扶持，让内容获得更多的曝光。用户收到这种邮件，都会欣然接受这种“认证”标签，因而后者的钓鱼方式显得尤为有效。如果用户点击邮件中伪装成验证账号入口的链接地址，会跳转至一个 WhatsApp 聊天室，骗子在此做局，伪装成 TikTok 客服，要求用户提供能绕过身份验证和重置密码所需的电子邮件地址、电话号码和验证码，从而顺利骗取用户账号的控制权。

链接：https://netsecurity.51cto.com/art/202111/691054.htm

第四章 消费类诈骗

（一）快递诈骗

1、团伙闲鱼低价卖二手苹果机诈骗

媒体时间：2021 年 9 月 2 日

摘要：近日，江苏南通抓获一个通过“闲鱼”销售廉价二手苹果手机的 19 人诈骗团伙。经查，该团伙用低价和其它正品苹果手机的外观视频和图片诱导，添加被害人微信私下交易，随后邮寄翻新、组装的廉价山寨苹果手机。如买家要求退货退款，团伙便发送虚假退货地址和物流单号拖延时间，最后将买家拉黑删除。

链接：https://baijiahao.baidu.com/s?id=1709772581017399295&wfr=spider&for=pc

2、【新冠】“快递检出新冠阳性需销毁赔付”诈骗

媒体时间：2021 年 11 月 23 日

摘要：近期某地一位吴先生接到自称某快递公司的电话，说他的快递在运输过程中被检出新冠阳性，整车快递都要销毁，要对他进行赔付，还跟他核对了快递单号等有关信息。对方让吴先生扫一个二维码，填写了银行账号、密码、验证码等信息，结果显示验证码超时，对方又让他下载一个 App，进行远程直播，指引他一步步操作。吴先生照做之后，发现他的账户出现 6 笔网络支付，总计超过 10 万元。

在上述过程中，吴先生的银行账户、密码、验证码都泄露给了对方，对方就可以用他的账号进行支付了。此为冒充客服的网购类诈骗，但是骗子更新了手段，利用疫情防控这个借口引人入局，隐蔽性很强。

链接：https://cj.sina.com.cn/articles/view/1893761531/70e081fb020028wyu

（二）电商诈骗

1、虚假好评电信网络诈骗

媒体时间：2021 年 7 月 14 日

摘要：哈尔滨市公安局道外分局捣毁一利用公民个人信息进行虚假好评的电信网络诈骗犯罪窝点。该团伙下设销售部、运营部、接号组三个部门，分工明确，环环相扣。“销售部”孙某云首先通过网站寻找好评少、评价低的商家，要求业务员按照话术以“包月 2188 元，包季度 4188 元，提升信誉为承诺”与商家进行联系。随后，“接号组”张某和胡某凡按照李某林下发的实名手机号到网上平台进行账户注册，再将注册好账户分发给“运营部”余某进行虚假好评，提升商家的评星等级。

链接：http://m.news.cctv.com/2021/07/14/ARTIxnDcXKtRRzKX8aGAzPcv210714.shtml

2、网店“代运营”诈骗

媒体时间：2021 年 8 月 18 日

摘要：今年 5 月份，温女士通过互联网广告联系上了一家网店代运营公司，并添加了该公司的“营销指导老师”王某。王某称公

司可以为温女士提供独家的优质货源、装修店铺、运营推广、电商实操指导与技术咨询，并向她展示了运营成功案例。温女士当即支付了 5998 元购买了“卓越版”代运营套餐。网店开起来之后，温女士却发现自己的网店订单一直没有明显变化，联系王某后，王某则以各种理由搪塞，称会继续帮助温女士经营，还向温女士推荐更加昂贵的套餐，就这样，温女士先后购买各类升级套餐数万元。但过了两个月后，网店销量依旧毫无起色，温女士意识到自己被骗，便向龙华公安分局龙华派出所报警。

链接：https://baijiahao.baidu.com/s?id=1708418973083066364&wfr=spider&for=pc

3、低价商品点对点交易诈骗

媒体时间：2021 年 11 月 10 日

摘要：广州市反诈中心发现，最近出现一种新的诈骗手法，不法分子在网购平台发布低价商品信息，之后引诱市民绕过第三方平台进行点对点交易。最近，事主林先生在网购平台上购买低价游戏机，商家以这款游戏机暂时缺货为由，客服将林先生介绍到其他平台购买。林先生信以为真并添加了对方的微信，对方指引他通过链接购买了游戏机，支付了 4200 元，后来林先生不但没有收到游戏机，还发现自己已被对方拉黑，才知道自己被骗。

链接：https://c.m.163.com/news/a/GOEDL1EH04179HVF.html

4、短视频虚假广告销售诈骗

媒体时间：2021 年 11 月 12 日

摘要：近日，上海警方捣毁一个利用短视频平台发布虚假购物广告进行引流，继而通过网络社交平台实施诈骗的团伙。受害人称，这款产品号称服用 60 天就能让白发直接反黑，并虚称是中医世家流传金方。没想到在被害人添加了网络社交平台账号后，犯罪分子便冒充专业医师以网上诊疗出具专业报告等方式，以被害人毛囊不畅、肝肾不好为由，陆续诱骗被害人购买所谓的中药膏、茶饮、理疗足贴等产品。经鉴定，这些产品都是没有任何治疗功效的食品，成本低廉。

链接：https://tv.cctv.com/2021/11/12/VIDEVFzi6jAq8oIQVrrZ92ig211112.shtml?spm=C22284.PKlANB2y5VO8.S63367.46

5、借微信号送苹果手机诈骗

媒体时间：2021 年 12 月 17 日

摘要：12 月 13 日，兰山公安分局刑侦大队在工作中发现市区有一伙人经营着一种看似亏本的神秘生意，这伙人在网络上拉拢网友，组建 QQ 群，发布临时租用微信号赠送 iPhone12 手机的消息，称使用一段时间后，再把微信号返还给当事人。同时，他们要求当事人使用的微信号必须是实名认证。据诈骗分子叙述诈骗方式为租用他人实名认证的微信号，再转卖给电信诈骗团伙使用，从中谋取暴利。一旦更改了绑定手机后，马上把这些经过实名认证的微信号里的内容清空，以高额的价格卖给电信诈骗团伙实施作案。刚开始，他们还批发来一些 iPhone12 手机的模型来蒙骗受害人，后来干脆连模型

也省掉了，直接从网上下载图片忽悠受害人。

链接：https://baijiahao.baidu.com/s?id=1719362460048938136&wfr=spider&for=pc

6、【冬奥】“冰墩墩”代购诈骗

媒体时间：2022 年 2 月 9 日

摘要：浙江绍兴市民张某在网络上认识了一名自称家在北京的男子徐某，男子称可以帮忙购买冰墩墩，张某向对方转账 1000 元。可钱到手后，徐某却说现在购买“冰墩墩”比较困难，要过段时间再看看。张某提出退款，不曾想自己的微信已被“好友”删除，张某这才发现被骗了，立即向派出所报案。

链接：https://hznews.hangzhou.com.cn/shehui/content/2022-02/09/content_8165498.htm

7、【冬奥】虚假中奖信息诈骗

媒体时间：2022 年 2 月 5 日

摘要：冬奥会期间，骗子会编造虚假的冬奥会中奖信息，市民在浏览网页或者网络聊天时会“幸运”地收到这样的“中奖”信息，告知你在冬奥会回馈抽奖活动中获得大奖，并编造吸引眼球的奖品。当信以为真的市民与兑奖方联系，对方都会以需要保证金、支付邮寄费用等各种借口，要求市民先汇钱。当汇去第一笔款后，骗子还会以手续费、税款等其他名目，继续欺骗市民汇款，直到“吃干榨尽”为止。

链接：https://baijiahao.baidu.com/s?id=1723870567156577566&wfr=spider&for=pc

8、【冬奥】推销冬奥纪念品诈骗

媒体时间：2022 年 2 月 7 日

摘要：此类诈骗蹭了冬奥会的热度，多有两种套路：一是“以次充好”，用不具收藏价值的纪念品冒充，骗取高额收购款；二是“空手套白狼”，仅仅以“冬奥纪念品”为幌子，收到转账之后就拉黑消失。

链接：https://baijiahao.baidu.com/s?id=1724089596902017370&wfr=spider&for=pc

（三）积分兑换诈骗

1、手机消费积分兑换奖品诈骗

媒体时间：2021 年 7 月 20 日

摘要：四川省绵阳市公安局涪城区分局日前破获了一跨川、闽、冀三省的“手机消费积分兑换奖品”电信网络诈骗案。涪城区公安分局副局长何跃介绍，诈骗团伙利用某电信运营商积分兑换奖品这种吸引客户的营销手段，轻而易举“吃掉”受害人话费积分，这种行骗模式新颖，极具隐蔽性。许多被骗的手机用户不关心自己的积分，也没有习惯主动使用积分，收到“科技公司”寄来的小礼品还很高兴，这给骗子们留下了可乘之机。

链接：https://baijiahao.baidu.com/s?id=1705800620169048256&wfr=spider&for=pc

2、积分换礼诈骗

媒体时间：2021 年 8 月 6 日

摘要：近日，刘女士手机接到一条来自“10086”的短信，短信称：“尊敬的用户：您已满足兑换 249.36 元现金大礼包，请登入移动商城 10086.yr8uk.pw，根据提示下载并安装点击允许，即可领取”。刘女士当时没有理会，隔天后刘女士的手机上再次收到相同短信。刘女士想到可以兑换现金，于是便点击下载安装并进入这一网站，随后网页上弹出要求输入银行账号、密码及身份证号等信息，刘女士按照要求进行输入。没过多久，她发现卡上 1.6 万余元被人通过网银分 5 次全部消费。

链接：https://mp.weixin.qq.com/s/zlQC4SNnd8km6fUbARmsrg

3、商家积分兑换诈骗

媒体时间：2022 年 1 月 19 日

摘要：临近春节，平台商家开始发送种活动短信，其中有商家推出积分清零活动，催促尽快去兑换平日各种消费积攒的积分，提醒再不及时兑换有的可能就会过期作废。点开短信中的网址链接，按提示输入了银行卡号、姓名、手机号、开户行以及银行密码等信息。

链接：https://baijiahao.baidu.com/s?id=1722351774613929750&wfr=spider&for=pc

（四）商业营销活动诈骗

1、新型“回扣”诈骗

媒体时间：2021 年 9 月 7 日

摘要：2021 年 8 月 2 日，江阴市一冷却器有限公司的销售员工

网上看见求购公司产品换热器的留言，阿秀与“客户”沟通，“客户”称自己的公司想购买 4 台换热器，但是在每台换热器基础加价，自己赚差价吃回扣。于是便收到“客户”发来的假冒银行到款短信，在“客户”的催促下，员工将回扣费通过老板的私人银行卡转至对方提供的银行卡上。老板之后点开了自己的手机银行，想再确认下到款，却惊讶地发现，自己银行卡上并未收到对方到款。

链接：https://www.toutiao.com/i7004992179412582948/

2、套路租车新型诈骗案

媒体时间： 2022 年 1 月 13 日

摘要： 2021 年年底以来，青浦、闵行等地区先后接报多起涉及车辆租赁纠纷的警情，集中反映出租赁合同短期内违约、租赁车辆短期内故障、出租方收取高额违约金押金等共性特征。犯罪团伙以高薪招聘司机为诱饵，签订隐含“陷阱条款”的租车合同，刻意制造违约后强占押金而非法获利。此类“套路租车”新型诈骗犯罪以“公司运作、签订合同”为伪装，呈现出作案手法更新快、隐蔽性强的特点。

链接：https://baijiahao.baidu.com/s?id=1721816501660286269&wfr=spider&for=pc

3、【冬奥】滑雪场优惠诈骗

媒体时间： 2022 年 2 月 8 日

摘要： 一些大型滑雪场的黄牛打着“冬奥合作单位能低价买卡”的幌子，实际上只为了骗取你的钱财。当你把钱转给对方之后，对

方反手一个拉黑，钱和卡你一个都没拿到。

链接：https://baijiahao.baidu.com/s?id=1724167734792136588&wfr=spider&for=pc

4、【冬奥】庆功红包诈骗

媒体时间：2022 年 2 月 7 日

摘要：每逢重大赛事，总是会出现名为运动健儿庆功的红包，可点开后却提示要将红包链接分享到 2 个不同的微信群即可领取，在这个链接中还包含不少广告内容，按照该提示操作，红包中的钱依然没有到账。所谓的“需要分享才能领取的红包”通常是一些伪造成微信红包进行恶意推广营销的手段，发布者利用送“红包”的方式吸引用户转发，实际上除了骗子增加了传播量之外，用户并不会得到任何好处，还极易造成个人信息泄露，甚至财产会受到损失。

链接：https://www.sohu.com/a/521524047_160447

第五章 求职类诈骗

（一）兼职诈骗

1、冒充求职者诈骗

媒体时间： 2021 年 9 月 9 日

摘要： 近几天有不法分子打着求职者的旗号，利用在线聊对企业方进行诈骗。具体的诈骗过程：首先在人才网注册个人简历，再以求职者的名义在平台给大量客户发送在线聊，广泛撒网抓住时机进行诈骗。聊到一半的时候会亮明自己是该家公司的法人以询问招聘情况、工作进度为由要求人事添加他们的 QQ 号码进行下一步的诈骗动作。

链接：https://new.qq.com/rain/a/20210909A02Y7200

2、高薪招聘兼职人员诈骗

媒体时间： 2021 年 12 月 6

摘要： 网络赌博相关的诈骗信息则会以丰厚的奖励诱骗受害人下载并使用赌博网站，受害人开设账号后也会将钱转入平台作为赌本，以为可以轻松获取高额回报。然而，受害人很快会收到通知，说账号被冻结，若要将赌本取出必须给更多的钱。一旦他们再次转账，骗子就会失联，网站也不能登陆了。

链接：https://weibo.com/5137261048/L4KMubKLY

3、【冬奥】当选志愿者押金诈骗

媒体时间：2022 年 2 月 8 日

摘要：奥组委在 1 月 24 日的时候已说明，志愿者招募工作已在 2021 年 10 月完成。近日声称被“选为”志愿者，需要垫付各种资金的都是骗子。

链接：https://baijiahao.baidu.com/s?id=1724167734792136588&wfr=spider&for=pc

（二）刷单诈骗

1、刷单返现诈骗

媒体时间：2021 年 4 月 21 日

摘要：2021 年 1 月，浙江省杭州市江干区的陈某在网上认识了一个陌生人，对方称可以带他“刷单”，并告诉陈某这生意稳赚不赔。在陌生人的“指导”下，陈某向平台充值 3100 元，顺利完成了第一个任务，没过多久就收到了本金和利息共计 4026 元。于是陈某又向平台充值了几笔钱，完成刷单任务后，很快就在平台上收到了佣金并且提现成功。有一天陌生人告诉陈某自己手头有一个“大单”，陈某二话没说就把钱充了进去，然而，任务完成后，陈某却发现从平台提现失败了。陈某联系上陌生人，陌生人回答称：“由于系统设置，你需要再转一笔同样数目的钱，才能提现。”陈某没有一错再错，反应过来对方在骗自己，于是立即报警。

链接：https://m.gmw.cn/baijia/2021-04/21/1302245295.html

2、鸿星尔克红包诈骗

媒体时间：2021 年 7 月 30 日

摘要：近期，鸿星尔克实业有限公司因捐赠 5000 万元物资驰援河南瞬间爆红，频频登上热搜。没想到连骗子都想来“蹭”热度，日前，有个别不法分子冒充鸿星尔克官方以“派送红包”为由诱导网友分享链接，实为刷单诈骗的引流。

链接：http://www.yidianzixun.com/article/OWDSYWQ4

3、下载 APP 做任务诈骗

媒体时间：2021 年 9 月 8 日

摘要：永修一名女子就因为想领一台免费的电扇，被骗 75321 元钱。首先，群主发布一条刷单广告，让翁某下载“米柚”APP 注册，并充值 28 元到这个 APP 里后，便能赚取本金 28 元加佣金 22 元，共计 50 元，还能领取一个免费的电饭煲。在成功领到 50 元钱后，9 月 2 日 14 时许至 9 月 3 日 16 时许，翁某按照群主（骗子）的要求，不断地充值现金进去投注刷单做任务。在对方的引诱下，翁某通过自己建设银行卡号分别向对方提供六张银行卡号转账现金，共计转账金额 75928 元，除提现的本金 428 元和赚取的 149 元，翁某实际被骗 75351 元。

链接：http://k.sina.com.cn/article_2022364304_788ad49002000upmo.html

4、评选投票、买票刷名次骗局

媒体时间：2021 年 10 月 13 日

摘要：郝先生是陕西华阴一家民营企业的负责人，他告诉记者2020年11月突然有人通过加好友的方式发给他一个投票链接，链接显示他的公司入围了当地行业优秀企业的评选活动。这个荣誉对企业来说尤其在招标的时候用处挺大的，人家说这可以买票，100块钱1000张票，这个落后多了，又买了200块钱的票，再买500块钱的票，再后来买1000块钱2000块钱的票。为了刷票赢得奖杯，公司通过微信转账向对方累计支付了3万多元人民币，但最终排名却不理想，郝先生才意识到被骗并选择报警。

链接：https://baijiahao.baidu.com/s?id=1706334936180270532&wfr=spider&for=pc

第六章 冒充身份类诈骗

（一）冒充公职人员诈骗

1、冒充移动公司人员诈骗

媒体时间：2021 年 4 月 8 日

摘要：该犯罪集团首先由一线成员冒充被害人所在地中国移动公司客服人员或通讯监管局工作人员，拨打被害人电话，谎称被害人个人信息泄露，被他人利用从事洗钱或诈骗等违法犯罪活动。

链接：http://m.mp.oeeee.com/oe/BAAFRD000020210408465004.html

2、冒充公司年检诈骗

媒体时间：2022 年 1 月 18 日

摘要：日前，西峡县某公司财务人员孙某来到五里桥派出所报警，称其接到一电话，对方以公司账户需要年检为由让其添加 QQ，在 QQ 群内有两人冒充公司法人和总经理，骗孙某向对方提供账户转入 8 万余元。接警后，民警立即对涉案账户进行止付、冻结，核实涉案账户信息，启动资金返还程序。最终在办案民警和银行工作人员的努力下，成功止付 8 万余元被骗款。

链接：https://baijiahao.baidu.com/s?id=1722258334793331579&wfr=spider&for=pc

3、冒充移动公司工作人员转账诈骗

媒体时间：2021 年 8 月 11 日

摘要：受害人朱女士对警察叙述称自己接到了一个自称移动公司工作人员的电话，对方称朱女士名下有一张电话卡被用作诈骗。朱女士表示自己没有办过这张卡，对方便称可能是朱女士丢失过身份证，被他人冒用了。朱女士还来不及回忆，对方又称要将北京公安的电话转给朱女士。随后，朱女士又接到了自称北京公安的电话，对方称朱女士与一起诈骗案有关，涉案金额高达 216 万，经过核实，朱女士未参与案件，但是对方冒用了她的信息，所以需要朱女士配合警方办案，将 216 万打到警方的“安全账户”，否则 2 小时后朱女士及其家人的银行卡、医保卡都会被冻结。

链接：http://k.sina.com.cn/article_7505202169_1bf584bf902000x9xq.html

4、冒充移动员工刷单诈骗

媒体时间：2021 年 8 月 27 日

摘要：8 月 22 日，蒙阴县李女士通过“伊队”相亲网站认识一男子，通过交流，该男子自称在济南移动公司工作，男子告诉李女士，自己利用工作便利可以在“全国话费充值采购平台”以 95 元的价格买进电话卡，100 元的价格在此平台卖出，刷单赚钱，一张充值卡能赚 5 元钱，李女士尝试在平台充值 950 元购买电话充值卡，从中获利 50 元，尝到甜头的李女士将此平台推荐给儿子小刘，男子又以“多买多赚”利诱李女士母子两人，李女士于是将自己的 2.3 万积蓄和儿子的 7.2 万元在此平台购买了电话卡。当准备提现时，发现平台

已无法登陆，才发现投入的 9.5 万元被骗。

链接：https://mp.weixin.qq.com/s/2I6gBFQBoG-ZDbYy14zHyw

5、冒充银行员工诈骗

媒体时间：2021 年 9 月 10 日

摘要：徐某某在印度尼西亚、马来西亚、印度等地参与一诈骗集团的境外电信诈骗活动，该诈骗集团冒充移动公司工作人员、银行工作人员、公检法工作人员，采用向被害人打电话的方式，虚构被害人银行卡透支、身份信息泄露或涉及重大案件需配合调查的事实，取得被害人信任，获取被害人姓名、身份证号码、银行帐户及密码等信息后，再将被害人银行卡中款项全部转走。

链接：https://www.12309.gov.cn/12309/gj/gs/lzs/lzsqlhq/zjxflws/202109/t20210910_10494331.shtml

6、【新冠】冒充“疫苗接种普查调查员”诈骗

媒体时间：2021 年 6 月 2 日

摘要：据人民资讯报道，近日各地广泛开展疫苗接种工作，有人收到“疫苗接种普查调查员”的好友申请，经查为诈骗分子假冒。警方发布提醒，涉新冠疫苗的主要骗局有：假冒预约链接、微信拉群交费、来电冒充疾控中心，都属于仿冒身份诈骗，套取个人信息或者诱骗转账。

链接：https://new.qq.com/rain/a/20210602A018PL00

7、【新冠】冒充预约疫苗接种诈骗

媒体时间：2021 年 6 月 6 日

摘要：诈骗分子谎称是疫苗中心主任，被害者根据指引需进群交付加急费、押金、做任务等方式才能安排打疫苗。预约新冠疫苗诈骗是不法分子利用人们的恐慌心理作案，骗子谎称自己“有关系”，是所谓的“内部人士”，只要支付一定的额外费用就可以帮你争取优先打到疫苗，进而索取金钱或者个人信息。

链接：http://bendi.news.163.com/guangdong/21/0601/17/GBE1RKF104179HVF.html

8、【新冠】冒充公检法对防疫人员诈骗

媒体时间：2021 年 11 月 9 日

摘要：11 月 7 日上午，湟中区一名疫情防控工作人员接到一自称是微信管理人员的陌生电话，称其微信有违法活动，有人举报该工作人员非法出售假冒伪劣口罩，必须进行微信账户封号处理，随后，对方将受害人的电话转接到一位自称是“北京市通州公安局办案民警”的诈骗电话上，对方称因“办案需要”，指示受害人通过网页下载“安全卫士”（诈骗软件），又以需要调查该工作人员银行账户资金为由，骗取 15 万元。

链接：https://www.toutiao.com/i7028407006113448481/

9、【新冠】冒充防疫部门流调诈骗

媒体时间：2021 年 11 月 17 日

摘要：近期，外地关于利用“核酸检测”实施诈骗的案件多发。其手法为：首先冒充防疫部门给你打电话，说你的核酸结果有问题。询问近段时间是否去过中高风险地区，接触过风险人群。然后说可

能系统问题，需要重新核实你的身份信息和行程信息然后给你发个链接，重新填写你的身份证信息和电话号码。等你把信息填写完之后，你就会收到一个验证码，让你把验证码发给他们，表示重新给你办理行程码。然后你就会上当，钱被骗走了。

链接：https://k.sina.com.cn/article_2107036715_v7d96d42b01900yhly.html

10、【新冠】冒充密接人员身份认证诈骗

媒体时间：2022 年 1 月 26 日

摘要：近期全国各地疫情不断，不法分子也在健康码上找到可乘之机。不法分子通过电话方式，谎称自己是某防疫部门的工作人员，称判断为密接人员，并发送钓鱼链接及验证码。如按照不法分子提供了详细个人信息和手机验证码，骗子就可通过网银把你钱直接划走。

链接：https://weibo.com/5149608258/Lcv1up5x5

（二）冒充客服诈骗

1、冒充网购客服称商品质量有问题诈骗

媒体时间：2021 年 11 月 05 日

摘要：2021 年 9 月 12 日，葛女士接到一个自称某网购平台客服的电话，对方称其在网上买的化妆品有问题，现在要对其给予双倍补偿 340 元。于是葛女士加了对方的 QQ 号并指引葛女士从支付宝里提取了 500 元钱。葛女士扫描对方发来的二维码，进入一个虚假的

“理赔通道”，接下来对方以注销帐户、缴纳保证金等种种理由，诱导葛女士在“拍拍贷”等 APP 里贷款，最终葛女士被骗走共计五万余元。

链接：https://baijiahao.baidu.com/s?id=1715572976541408349&wfr=spider&for=pc

2、冒充清除不良征信诈骗

媒体时间：2021 年 12 月 7 日

摘要：2021 年 11 月 28 日，李先生接到自称是第三方支付平台的“客服”人员的来电，称他曾在平台上因还款逾期，导致征信有不良记录。因为近期正有买房的打算，之前也的确有过逾期还款的情况，担心无法贷款购房，李先生便信以为真。“客服”告知李先生，如果想要消除征信问题，需要银行的流水记录把信用提升，让李先生把自己的全部存款转入到指定银行账户，等信用提升后，会予以退还。随后，李先生将自己的 75000 元存款全部汇入到对方账户。转账后，迟迟不见退款，李先生心生疑虑赶紧联系对方，“客服”只字不提退款的事情，还要求他继续下载其他手机软件进行操作，这时李先生觉得不对劲，赶紧报警求助。

链接：http://finance.sina.com.cn/money/bank/bank_hydt/2021-12-07/doc-ikyakumx2479812.shtml

3、【新冠】冒充客服谎称快递员感染新冠病毒诈骗

媒体时间：2021 年 10 月 26 日

摘要：10 月 23 日 16 时，新城区毫沁营红山口村白某某接到冒充电商客服的电话称，由于快递员感染新冠病毒，快递要集中销毁，

销毁后给被害人退款补偿。随后，犯罪嫌疑人让被害人提供银行账户并告知被害人该卡已被冻结，将钱转入安全账户后方可解冻。被害人按照其要求共转账四笔共计被骗 9.3 万元。目前，案件正在进一步侦办中。

链接：https://new.qq.com/rain/a/20211026A062RH00

（三）冒充熟人诈骗

1、男子凭头像昵称错加好友被骗

媒体时间： 2021 年 9 月 29 日

摘要： 今年 8 月，河北保定市顺平县的谭先生收到一条微信好友申请，对方微信名和头像是自己一个多年的好朋友，谭先生立即通过了申请。经过一段时间的嘘寒问暖后，这个好友以急需周转资金为由让谭先生马上转给他 40 万元钱。可钱打过去后，谭先生却被拉黑，这时，谭先生意识到自己被骗，赶紧报了警。骗子诈骗套路：①伪造他人头像，重新注册微信号②先不谈钱，当目标人群对骗子深信不疑时再说急用钱③拿到转账后立刻拉黑，逃之夭夭。

链接：https://weibo.com/3266943013/KArH4r0f6

（四）冒充网站诈骗

1、【冬奥】假冒冬奥会官方网站诈骗

媒体时间： 2022 年 2 月 5 日

摘要：不法分子通过搭建虚假的冬奥会官方网站，在网站上进行所谓的“幸运抽奖”“冬奥纪念品赠与”“冬奥限量版纪念邮票限时抢购”“冬奥纪念币抢购”等活动，诱骗进行在线注册。一旦市民按照网站设定的路径操作，就会落入诈骗分子的圈套，导致个人信息泄露，甚至银行卡中的钱财被转走。

链接：https://baijiahao.baidu.com/s?id=1723870567156577566&wfr=spider&for=pc

第七章 针对特定人群类诈骗骗

（一）针对未成年诈骗

1、12 岁女孩上网课被骗

媒体时间： 2021 年 8 月 3 日

摘要： 近日，苏州 12 岁女孩小孔在用妈妈手机上网课时，一个陌生人加她好友。对方自称是某地警官，小孔父母涉嫌诈骗，账户已被冻结，要在 30 分钟内解冻，否则其父母将坐牢。小孔赶紧按照要求先后给对方转账了 7000 多元。小孔的妈妈发现后报警。

链接：https://weibo.com/2286908003/KrHS4w7yw

2、小学生为要偶像签名被骗

媒体时间： 2021 年 8 月 13 日

摘要： 8 月 11 日，湖南常德。12 岁女孩小李刷短视频时，为领取偶像签名照和 888 元奖励，添加一自称是偶像工作人员的账号，先后被骗 19100 多元。小李的哥哥表示，信息是未经认证的偶像团体的其中一个队员账号发出，现已报警。@白鹿视频 据其家人提供的二维码添加所谓“工作人员”后，被告知需截图微信余额，不同金额可领取不同等级的红包，并有详细返款流程视频，根据流程付款后并未得到返款。

链接：https://weibo.com/1678528194/KteomaoqJ

3、注销支付宝学生账户骗局

媒体时间：2021 年 8 月 27 日

摘要：诈骗分子通过违法的渠道获取了很多学生的一些个人信息，他们给学生拨打电话，会告诉你的姓名，你的身份证号以及你学校的相关信息，目的就是为了能够跟你建立信任感。以教用户查询所谓的“学生账户”名义，查询“借呗”额度。所谓把“支付宝学生账户”清零，是将“借呗”里的贷款额度借贷出去，转成现金。

链接：https://weibo.com/1977460817/Kvn4IwkSo

4、小学生为解除游戏防沉迷限制被骗

媒体时间：2021 年 9 月 6 日

摘要：小贺是名未成年，根据最新要求游戏时长被限制。在登陆游戏时，看到游戏大厅中有人称能够帮助未成年人解除游戏限制。于是小贺就加了该陌生人的好友，并按照对方要求将妈妈的微信账号和密码发送给了对方。该陌生人在收到小贺母亲的微信账号和密码后，就将微信中的 100 元零钱转走了，还冒充孙女士向其亲朋好友借了 1150 元。

链接：http://baijiahao.baidu.com/s?id=1710118402455557696

5、女孩为看偶像直播回放被骗

媒体时间：2021 年 9 月 15 日

摘要：近日，河南南阳 13 岁女孩为了看偶像演唱会的回放，听信粉丝群网友的“指导”，用父亲手机转出 10 余万元，父亲信用卡

还款时发现银行卡余额异常，经过询问发现女儿被骗，遂报警。

链接：https://weibo.com/5658011035/KyfCYsqOB

6、初中生加偶像 QQ 被骗

媒体时间：2021 年 11 月 21 日

摘要：江苏苏州喜欢追星的初中生小雨，从同学处得知自己的“偶像”输了游戏后在网上公布了 QQ 账号，便添加了该 QQ 为好友。随后，小雨被拉进粉丝群，参加所谓的充值返现福利活动，用家长手机向对方指定的账户转账了 9 万多元。

链接：https://weibo.com/1796087453/L2yxVxnKQ

（二）针对老年人诈骗

1、假冒银行员工诈骗

媒体时间：2021 年 11 月 8 日

摘要：70 岁的张某 2020 年 3 月接到了一个自称天津市和平区 A 银行工作人员的电话，告知她在 A 银行透支了 11000 余元，在得知张某没有 A 银行卡后，建议其报警，并帮助其接通公安系统电话。接着，一位自称公安系统的人员告诉张某，她现在牵扯到大案要案，手机被人盗用，让张某更换手机，不要告诉他人，随时保持联系。于是张某购买了新手机和手机号，并将银行卡存款存成定期，办理了手机银行和电子密码器。当日下午，张某来到银行注销了原来的网银、手机银行等，并将卡内 40 万人民币定期存款 1 年，诈骗人员称公安局需要加密电子密码器，让张某多次输入密码，再将生成的动态密

码告诉他。反复多次后，诈骗人员表示银行卡已被银监会冻结，一周之内不要使用，并表示张某可以继续往这张银行卡里存钱。一周后，北京市海淀区民警打来电话，张某才知道自己被骗了。

链接：https://www.jiemian.com/article/6789659.html

2、假冒子女诈骗

媒体时间：2022 年 3 月 1 日

摘要：近日，王老先生在家里接到一通开头显示为”+00“的境外电话，电话那头的人声称是他的孙子小王，并声情并茂地讲述自己在美国加州上学时，被牵扯进了一起重大的交通事故中，请求王老先生帮他解围，王老先生回想起自己的孙子小王确在美国上学，便二话没说答应了。后来，其孙子“小王”便开始声情并茂的“诉说”着自己在美国遭遇的交通事故，要王老先生帮他垫付赔偿费、律师费、修理费以及医治费等，以骗取王老先生的信任，并通过王老先生的座机电话，告知了自己的收款账号，王老先生想也没多想，就匆忙的去了银行进行转账汇款。等到真正的孙子小王找到了王老，在谈话过程中，王老先生发现自己受骗了，便随即拨打报警电话求助。

链接：https://www.thepaper.cn/newsDetail_forward_16903870


中国移动
China Mobile
5G+