以案为鉴说骗局　筑牢反诈防火墙

本版策划：省公安厅宣传处、刑侦总队

◇编者按◇

当前电信网络诈骗手段迭代翻新，呈现高发态势，严重威胁人民群众财产安全。为筑牢全民反诈防线，全省公安机关正深入推进《山东省防范电信网络诈骗主题宣传活动方案》(即“防骗你我他 全民共反诈”集中宣传活动)，以案说法、以宣促防，全力挤压犯罪空间。

面对网络游戏虚假交易、虚假投资理财、冒充公检法等层出不穷的骗术，提升每一位公民的辨别与防范能力，是拧紧“安全阀门”的关键。以下是各地市真实案例与警示，旨在以案为鉴，帮助广大群众更加直观地识别骗局、增强防范意识，筑牢反诈防骗的防火墙。

济南公安提醒：

勿点不明链接　守住养老钱

案情回顾▶▶▶

9月17日，济南市某辖区老人张某海紧紧握着民警的手，后怕不已：“多亏你们及时上门，我差点就把养老钱‘送’给骗子了！”当天，济南市反诈中心通过精准预警与高效联动，仅用十分钟便成功阻断一起抖音直播扣费类诈骗，为老人守住50600元养老钱，以“速度与温度”筑牢群众财产安全防线。

当日，济南市反诈中心监测系统弹出高危预警：张某海老人疑似遭遇抖音直播扣费类诈骗，银行卡资金面临盗刷风险。民警第一时间尝试致电提醒，却发现电话被“呼叫拦截”——诈骗分子已操控老人手机设置，切断外界干预通道。情况紧急，民警迅速查询到老人亲属张某的联系方式，电话中亮明身份说明险情，可家属因不了解96110反诈专线心存疑虑，不愿提供具体住址，处置陷入僵局。

“每一秒都可能造成损失！”民警当即调整方案，根据预警关联的小区范围，紧急联系社区网格员与邻居协助上门。很快，邻居传来消息：已敲开老人家门，发现其正按对方指示准备下载涉诈App。民警一边驱车赶往现场，一边让邻居打开免提，指导老人关机、拔手机卡、关闭网络，彻底切断诈骗分子远程操控通道。几分钟后，民警抵达现场核实，银行卡交易记录显示资金分文未少，从预警触发到成功止损，全程仅10分钟。

民警支招▶▶▶

近年来，针对老年人的冒充抖音客服诈骗频发。诈骗分子通常以开通直播会员、账号异常、违规操作为由，通过电话或短信发送虚假链接，诱骗老年人下载涉诈App，利用屏幕共享功能，套取银行卡号、验证码等重要信息，进而盗刷资金。此类诈骗危害极大，不仅让老年人蒙受经济损失，还会引发焦虑、自责等负面情绪，影响身心健康，部分老人被骗后甚至独自承受痛苦。

为防范此类诈骗，子女应多关心老人，普及防骗知识；老人遇到自称平台客服的情况，务必通过官方渠道核实；抖音等平台也需加强安全提示，共同营造安全网络环境。

96110是全国统一反诈预警劝阻专线，接到来电说明机主或家人正遭遇电信网络诈骗，务必及时接听听从劝阻。此外，接到电商、物流客服电话时，需到官方平台核实，切勿随意开启屏幕共享、点击陌生链接，更不能泄露银行卡密码、短信验证码等信息。

济宁公安提醒：

家长管孩子防　共筑反诈防火墙

案情回顾▶▶▶

10月9日，11岁的侯某在手机上玩“回森”唱歌软件时，一陌生人发来私信称有很重要的事情，随后将侯某拉入聊天房间，对方自称北京市公安局的，谎称侯某的手机号被不法分子利用，需要其配合调查。对方诱导侯某拿来其母亲手机，并在自己手机上下载腾讯会议软件，通过该软件的视频通话功能与其通话，侯某在对方诱导下一步步扫码转账，直至手机没电，共计被骗1.4万元。

9月14日，13岁的郝某在手机上玩“小红书”时，刷到一个“美团零元购”的帖子，郝某在帖子下评论后收到一陌生人私信，对方发来一个二维码，郝某扫码进入一标有“红十字会”字样的网页，网页客服称转10元可返188元，郝某扫码支付10元后手机被下载一“海鸥”软件，该软件客服诱导郝某拿来家长手机，并用家长手机扫描二维码、提供短信验证码，随后其银行卡内余额被全部转走，共计被骗12万元。

民警支招▶▶▶

近期，济宁市任城区相继发生针对未成年人电诈案件，骗子紧盯孩子社会经验不足、警惕性弱的特点，套路层出不穷，警方提醒，务必高度警惕。

针对未成年人的常见诈骗套路需认清，高发的有三种，一是冒充公检法恐吓，谎称“违规需罚款”“家人涉案”，用“不配合就抓你”恐吓孩子，诱导共享屏幕、修改支付密码转账。要记住，公检法从不上网办案，更不会要你转账！二是游戏相关诱惑，以“免费送皮肤装备”“解除防沉迷”为饵，套取家长银行卡、验证码，甚至诱导孩子操作家人手机转账，单笔被骗最高超万元。三是兼职刷单陷阱，打着“轻松赚零花钱”“免费送礼品”幌子，先让交“违约金”，或骗孩子当“人肉中转站”，使其沦为诈骗工具人。

家长防护“三要点”：一是管好手机与密码，关闭免密支付，不向孩子透露支付密码；二是多讲真实案例，教孩子保护隐私，不扫不明二维码；三是发现资金异常立即断网冻卡，带着转账记录报警。

小朋友防骗“四牢记”：未知链接不点击，陌生来电不轻信，个人信息不透露，转账之前问家长！

禹城公安提醒：

警惕虚假投资理财　守好“钱袋子”

案情回顾▶▶▶

虚假投资理财类已成为当前高发的电信网络诈骗类型之一，诈骗分子精心设计圈套，让受害人在“高收益”的诱惑下遭受重大财产损失。

近期，投资理财类诈骗案件频发，犯罪分子利用人们对财务增值的渴望，设计出各种令人防不胜防的骗局。从虚假投资平台到线下现金交易，从黄金投资陷阱到情感诱导的“杀猪盘”，诈骗手段不断升级换代，让不少人辛苦积攒的财富顷刻间化为乌有。

虚假网络投资理财类诈骗通常通过社交软件、短视频平台等渠道，以“内幕消息”“高额回报”为诱饵，精心布置骗局。近日，禹城市居民郭女士在网上认识一名“现役军官”，对方每日嘘寒问暖，很快与郭女士建立起情感联系，见时机成熟，对方便让郭女士管理自己的理财账户，当郭女士看到账户每天都能收入数千元到上万元的收益而心动时，主动投入资金，当郭女士想提现时，却被平台告知需要收取手续费才能提现，先后共计被骗20余万元。

民警支招▶▶▶

核实机构资质。购买投资理财产品前，要通过国家企业信用信息公示系统查询企业是否登记注册，在证监会、国家金融监督管理总局官网查询金融机构业务资质。

警惕高收益承诺。年化收益超过6%要打问号，超过8%有风险，超过10%很可能就是骗局。任何承诺“保本高息”“稳赚不赔”的投资都是诈骗。

不下载未知App。不点击陌生链接下载投资App，更不要向陌生对公账户或个人账户转账，诈骗分子往往要求下载小众聊天软件进行沟通。

保持理性思考。主动询问资金投向、盈利模式，对于回答模糊或夸大其词的立即终止。遇到高收益诱惑，多征求家人意见。

投资有风险，入市需谨慎。不轻信、不透露、不转账，守好自己的“钱袋子”，在投资理财前多一份警惕，就能少一份损失。如遇可疑情况，请立即拨打全国反诈专线96110进行咨询。一旦发现被骗，请及时拨打110报警。

桓台公安提醒：

警惕高额回报　投资陷阱

案情回顾▶▶▶

近日，桓台县公安局少海派出所上演了一场反诈“竞速赛”。民警与电信网络诈骗分子争分夺秒“赛跑”，及时为群众挽回了10万元，守住了群众“钱袋子”。

近日，少海派出所接到反诈中心预警，辖区刘女士有被涉诈软件诈骗的风险。民警立即上门劝阻，据刘女士描述，其下载了某车友App，并加入一个微信群。群内一男子主动联系刘女士，以高额回报为诱饵，引导其在某软件进行小额“投资”，并给予返利，成功返利后刘女士与对方建立了信任。随后对方以“做大项目”“更高收益”为由，诱导刘女士提取10万元现金并以“网上转账不便”等借口，要求她亲自将现金送往指定地点。

经民警分析，刘女士意识到已踏入骗子精心设计的“高回报”陷阱。“谢谢警察同志！帮我保住了这10万元啊！”刘女士激动地说道。随后民警向刘女士详细讲解了电信网络诈骗的作案手法及预防措施，并耐心叮嘱其要提高警惕。

民警支招▶▶▶

日常生活中，当发现遭遇电信网络诈骗后，应立即拨打110报警，进行紧急止付。紧急止付机制是公安机关通过警务平台与各大银行合作，对涉案账户进行快速止付和紧急冻结，最大限度地减少和挽回群众损失。

如果不慎被骗应该怎么办？

1.及时记录转账时间、转账金额和诈骗分子的银行账户名称、账号及开户行。

2.第一时间拨打110报警，描述被骗的简要过程。当被确认为遭遇电信网络诈骗后，将由反诈部门进行紧急止付操作。

3.收集被骗过程中的汇款凭证、通话记录等相关信息，前往当地派出所进行后续处理。

千万不要做什么？

1.千万不要擅自寻找网络上所谓的“网警”报案或“黑客”自行调查。这些“网警”“黑客”往往是诈骗分子伪装的，很有可能会导致再次被骗。

2.千万不要直接删除相关证据信息，以免影响警方对手机数据进行提取、固定。

千万不要盲目与诈骗分子周旋，试图要回被骗钱财，不仅可能导致钱财无法追回，甚至可能再次陷入诈骗圈套，造成更大的损失。

青岛公安提醒：

网上交易须谨慎　提高警惕勿上当

案情回顾▶▶▶

网络游戏虚假交易诈骗：

近日，青岛市区一名13岁的初中生在手机上玩“迷你枪战精英”游戏时，有人联系其称，可以免费教游戏技术及赠送装备，在领取期间对方称“由于其是未成年人，领取需要家长手机辅助验证”，并下载了一个名为“商小信”的社交App，按照对方要求，使用其奶奶微信绑定银行卡并向对方提供二维码，套取家长银行卡验证码后，将家长银行卡内的钱从10月1日至6日转账68笔，共计损失2万余元钱。

民警支招▶▶▶

1、家长要保管好自己的手机和银行卡，不要让孩子知道支付密码，不要将支付App设置为免密支付。

2、家长要加强对孩子的反诈骗宣传教育。日常中多与孩子交流，分享这些真实的网络安全知识和诈骗案例，让孩子深刻认识到网络并非绝对安全，天上不会掉馅饼面对诱惑要保持警惕。

3、留意孩子手机里新安装的App，查看聊天记录和浏览历史，若发现孩子与陌生人频繁联系，或涉及金钱账号信息等敏感内容，要及时过问并引导。

案情回顾▶▶▶

交取暖费要擦亮眼睛：

近期，有不法分子通过闲鱼网、微信群、朋友圈、短视频平台等社交网络平台，以“供热费打折”“低价代充”等名义发布虚假信息，诱导用户交费，从而实施诈骗，严重损害用户财产安全与个人信息安全。

民警支招▶▶▶

对所谓“九五折”“九折”“八五折”等折扣信息务必提高警惕，不要轻信陌生人推荐的付款二维码、链接或转账账户。

要务必通过供热单位官方渠道交纳热费保障资金安全。如有疑问，可拨打自家签约的供热公司官方咨询电话进行咨询核实。

枣庄公安提醒：

切勿向陌生账户转账汇款

案情回顾▶▶▶

10月28日，枣庄市中区市民李某收到一个不明快递，内装一张刮刮卡，李某刮中某知名品牌洗衣液一桶和20元红包，但是刮刮卡上写明“如兑奖需扫描二维码”。李某扫码联系上所谓的“客服”后，对方要求其提供手机号和获奖刮刮卡的照片，并告诉李某要加入商家微信群才能领奖，群内还会开展现金抽奖、生活电器试用等活动。

抱着试试看的心理，李某扫描客服提供的二维码加入了微信群。随后，群主“商家活动员”发消息称，这是由多家平台成立的商家联盟，并给每位“中奖者”发送了20元现金红包，不一会的工夫，李某就在群里领取了近60元现金红包和一台空气炸锅。

这时，群主“商家活动员”又下发了新任务，通知群内人员可以参与关注淘宝订阅号赚取佣金活动，关注一个订阅号佣金为3.5元，并在群里下发任务。群里“中奖者”争相做任务，做了几单后，现金立即到账，大家沉浸在“赚佣金”的喜悦中，群内气氛高涨……“商家活动员”利用这个时机告诉大家，下载官方App，可以长期做任务赚取佣金，并且下载App后就会立即收到38.88元现金红包。

李某根据群主的链接下载了一个App，领到了38.88元现金红包。此后，有一位专职“助理”提供“保姆式”服务，全流程引导李某订阅接单、进任务群、添加任务“结算员”。

李某所进的App任务群内有1000多人，群内公告明确任务发布20分钟一次，每单关注价4.6元到16.9元不等，工作时间从9点到21点30分，每天9点签到领18.88元现金红包，连续签到3天可以领取288.88元现金红包……仅仅几个小时，李某就“赚到”了1000余元现金，从而使其放松了警惕，觉得这是一个业余赚钱的好机会。这时，有“助理”联系李某升级代理，并告知其可以赚更多佣金，享受更多福利，但是升级后需要凭运气和手速抢单做任务，不是谁都能抢到的。抢单金额为1000元、3000元、5000元、10000元、15000元、30000元(对应的本佣金返现为1300元、4200元、7000元、15000元、24000元、48000元)。

面对高额返利，李某犹豫再三，最终还是决定继续尝试，并“很幸运”地中单了。在李某按照“助理”要求将1000元转给商家做任务后，其被一位“金牌导师”拉入了一个5人群，此时App账户也显示1300元本佣金到账，但是“金牌导师”在群里强调需要继续做联单，做完联单才能把之前的任务佣金一起提现，联单金额为A8526、B17865、C38503。此时李某表示没有钱，放弃联单任务，却被告知如果不做联单之前的1300元本佣金不能提取，App账户金额会被捐赠到某爱心基金会，而且影响征信。

正当李某迟疑不决时，手机铃声响起，显示96110来电，李某瞬间明白自己遭遇了电信诈骗，等其挂断电话，发现自己已经被移出任务App，而且无法再登录进去。

半小时后，民警找到李某，向李某详细询问了相关情况并进行取证。随后，李某跟随民警到辖区派出所报案，因为民警的及时预警劝阻，李某没有继续被骗。

民警支招▶▶▶

100%刮刮卡、现金红包、0元领礼品……电信网络诈骗花样多、手法多变，而且为了诱人上当，骗子也会投入大量成本，但万变不离其宗的是要把钱从你的口袋转到骗子手中，一切以各种理由需要向陌生账户转账、汇款，或者以各种方式向对方提供银行账户、密码、验证码的，大家务必提高警惕，对于无法鉴别的，可以第一时间拨打96110(全国反诈预警劝阻专线)进行咨询，同时建议广大市民安装“国家反诈中心”App，进行实名注册，开启预警保护，及时预警，防止被骗。

山东法制报文化传媒有限公司出版　社址：济南环山路41号　邮编：250014　全年报价360元　山东大众华泰印务有限责任公司印刷　地址：济南市长清区玉皇山路1678号