随着暑期临近，学生放假、市民出行旅游及休闲娱乐活动增多，电信网络诈骗犯罪也进入高发期。结合历年暑期发案规律及近期新型骗局特点，记者采访了银川市反诈中心民警，梳理出暑期高发诈骗类型，提醒广大市民群众，特别是学生及家长群体提高警惕，谨防上当受骗。

“日进斗金”是骗局 “保录取”是陷阱

诈骗分子“暑期档”来袭 你准备好了吗？

记者 王辉

A 暑期学生兼职需警惕『高薪』骗局『刷单返利』陷阱

“目前银川高发的电信网络诈骗中，刷单类诈骗依然居高不下。”银川市反诈中心民警说，暑期是学生寻找兼职和社会实践的高峰期，但由于社会经验不足，他们很容易落入刷单返利的骗局。

诈骗分子通过短信、微信群、QQ群、短视频平台、快递包裹广告以及街面小广告等渠道，大肆散布“足不出户、日进斗金”“动动手指、轻松赚钱”“高薪兼职”等极具诱惑性的虚假信息。一旦受害人关注并添加联系方式，就会被拉入所谓的“任务群”。

诈骗分子首先会以小额返利骗取信任，让受害者完成关注公众号、点赞等简单任务，或进行小额垫资购物（通常金额在百元以内），并按时返还本金和少量佣金（5~20元不等），以此制造“诚信”假象。

在获取信任后，骗子会以“升级任务”“组合单”“高佣金单”为名，诱导受害者下载指定的诈骗APP（这些APP常伪装成正规电商或社交平台）。同时，群内的“托儿”会不断晒出虚假的高额收益截图，营造投入越多赚得越多的假象。

当受害者投入大额资金完成“任务”后，骗子会以“操作失误导致账户冻结”“系统检测到刷单需解冻金”“任务未完成需补单”“提现需缴纳个人所得税”等借口，要求受害者继续充值转账。如果受害者犹豫，骗子还会以“无法提现”“放弃则前期投入全部损失”等话术施压，直至受害者耗尽资金或最终醒悟。

B 藏在生活里的隐形『黑手』蹭热点设局

“您好，这里是宁夏教育厅。经AI监考系统判定，您孩子在6月8日高考数学科目中存在作弊行为，成绩将被取消。请立即点击链接确认申诉。”高考结束不到一周，李女士就收到了这条短信，顿时惊慌失措。就在她颤抖着手准备点击链接时，儿子及时制止了她。

“孩子说自己根本没有作弊行为，而且就算真有问题，也不会等到考完才通知。”李女士告诉记者。当她仔细查看来电号码时，这才产生怀疑：“后来我专门咨询了教育部门，确认这个虚拟号码根本不可能是教育部门的电话。”

在李女士经历这场虚惊的同时，金凤区的张先生也遭遇了诈骗。“人人保险客服”来电称：“您的医保补贴今天到期，请立即登录社保网站确认信息。”毫无防备的张先生按照对方指引进入钓鱼网站，输入银行卡号后，2万元存款瞬间被转走。

这些令人痛心的案例并非个例，而是当前诈骗犯罪日益猖獗的缩影。骗子们专门瞄准人们生活中的重要节点，教育、医保等民生领域已成为诈骗重灾区。

C 当心『共享屏幕』盗走你的钱 招生季+医保诈骗双重陷阱

银川市反诈中心最新通报显示，近期医保类诈骗案件持续高发，犯罪手段不断翻新。诈骗分子通过冒充“人人保险”等医保机构，利用群众对医保政策的信任，编造“补贴到期”“报销未确认”等虚假事由，通过短信发送含有钓鱼链接的通知，诱导受害人点击进入仿冒的社保中心网站。一旦受害者填写身份证号、银行卡号及验证码，或按要求下载屏幕共享软件，账户资金就会在不知不觉中被盗刷。

随着中高考结束进入招生季，针对考生及家长的诈骗也呈现高发态势。银川市反诈中心民警介绍，目前主要存在以下几类骗局：

一是“AI作弊指控”诈骗。不法分子冒充“宁夏教育厅”“宁夏教育考试院”等官方机构，发送“AI监考发现作弊违规行为，成绩将取消”等恐吓短信，利用家长对考试成绩的重视心理，诱导点击链接或回拨电话实施诈骗。

二是“招生黑幕”诈骗。骗子以“内部指标”“提前查分”“保录取”“改分数”甚至伪造录取通知书为诱饵，利用家长望子成龙的心理，索要“保证金”“操作费”等，得手后立即失联。

三是“共享屏幕”诈骗。以“协助申诉操作”等为由，诱导受害人下载屏幕共享软件，借此实时窃取银行卡密码、短信验证码等敏感信息，最终盗取资金。

D 电信诈骗的『心理操控术』 你的恐惧正在被明码标价

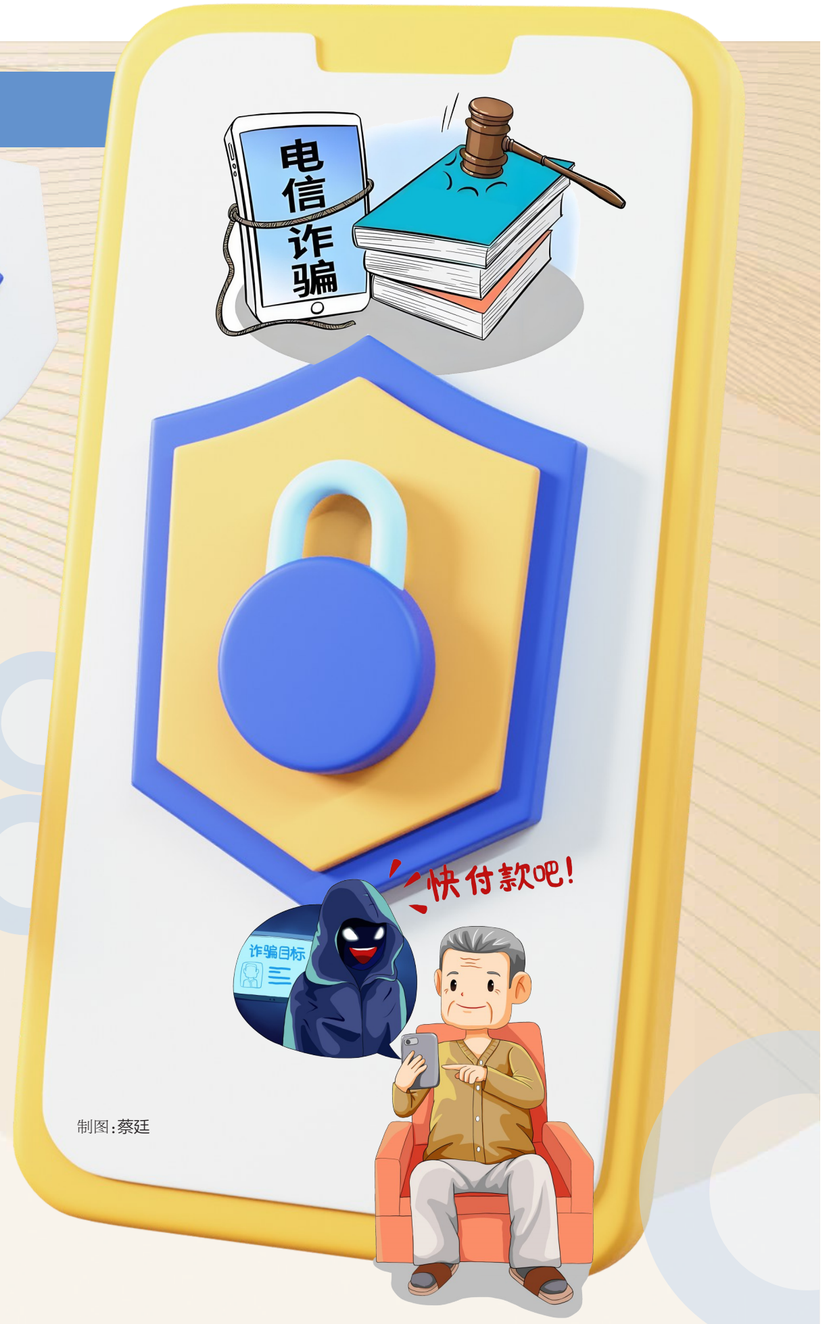
银川市反诈中心民警分析指出，当前各类电信诈骗虽然形式多变，但核心套路高度一致，每一步都经过精心设计，直击受害者的心理弱点。

首先，诈骗分子会精心伪造权威身份。他们冒用“社保中心”“教育厅”等具有高度公信力的官方机构名称，甚至利用技术手段仿冒官方短信号码。这种伪装让受害者在毫无防备的情况下放松警惕，轻易相信诈骗信息。

其次，犯罪分子深谙心理学，善于制造紧迫危机感。“补贴到期”“成绩将被清零”“名额有限”等话术如同紧箍咒，精准抓住人们对金钱损失、前途尽毁的恐惧心理。在这种高压状态下，受害者往往丧失理性判断能力，盲目听从骗子指令。

最关键的是，诈骗分子会通过各种话术诱导受害者主动交出关键信息。一旦获取身份证号、银行卡号、密码和验证码等敏感信息，特别是验证码，受害者的资金防线就会彻底崩溃，账户资金将被肆意转移。

值得注意的是，在公安机关持续高压打击下，诈骗分子也在不断升级手段。除了频繁更换“剧本”和“话术”外，他们还借助技术手段窃取信息。所谓的“屏幕共享软件”实际上是植入木马的程序，能让骗子实时监控受害者手机屏幕上的所有操作，包括输入的密码和收到的验证码，甚至能远程操控手机，实现精准盗取资金。



制图：蔡廷

防诈全攻略

官方教你见招拆招护住血汗钱

近期，针对电信网络诈骗案件高发态势，宁夏移动、宁夏教育厅、公安厅及通信管理局联合发布重要提醒。银川市反诈中心为广大市民总结出一套实用有效的防诈策略：

认准官方渠道

办理业务时务必通过正规途径：医保业务请通过当地医保局官网、官方APP、政务服务大厅或定点医院、药店窗口办理；中高考相关信息（查分、录取、政策等）仅以宁夏教育考试院官网、考生所在学校通知或省级教育部门发布为准。对非官方渠道信息保持高度警惕。

严守“三不”原则

- **不点击**：拒绝点击陌生短信、邮件、社交消息中的可疑链接；
- **不透露**：绝不向不明身份者提供身份证号、银行卡号、密码及验证码；
- **不安装**：拒绝下载来源不明的APP，特别警惕“屏幕共享”类软件。

保持冷静核实

收到涉及金钱、处罚等信息时：

保持冷静，避免恐慌；

通过官方渠道查询核实（如12333社保热线、教育考试院电话）；

切勿回拨短信提供的号码。

警惕转账要求

正规业务不会要求向个人账户转账；

任何“保证金”“手续费”的要求都是诈骗，坚决拒绝转账要求。

应急处置措施

- **如遇诈骗**：立即冻结银行卡，拨打银行客服挂失；
- **保存证据**：截图留存短信、通话记录等；
- **及时报案**：拨打110或96110反诈专线。

记者手记

十个被骗九个还以为自己是“幸运儿”

采访中一个令人深思的现象反复出现——许多受害者在事发前都信誓旦旦地说：“这种事绝不会发生在我身上。”然而当他们真正陷入骗局时，却难以识破诈骗分子精心设计的连环圈套。

诈骗分子精心设计的骗局，正是利用了人们最本能的信任——对“官方”标识的敬畏、对子女前程的焦虑、对医疗保障的依赖。他们借助技术手段伪装身份，利用人性弱点制造恐慌，在信任的缝隙中肆意行骗。“AI监考作弊判定”等新型话术的出现，更显示出诈骗分子对热点技术的敏锐嗅觉。从医保到教育，他们不断变换诈骗场景，唯一不变的核心目标就是诱导转账。

除了对“权威”的盲目信任外，当出现“提前查分”“保录取”“高额补贴”等字眼时，部分受害者潜意识里期待“特殊通道”。骗子深谙人性中的贪念，将诈骗包装成“仅限少数人”的机会。一位办案民警直言：“十个被骗的，九个都以为自己是‘幸运儿’，天真地相信天上会掉馅饼。”

请牢记这些永恒的原则：天上不会掉馅饼，所有“特殊渠道”“内部操作”的承诺都是陷阱。在涉及重大利益时，尤其要警惕“仅限今天”“过期不候”的话术施压——真正的官方流程都会留有合理缓冲期。

在这个数字时代，保持对“权威”的审慎态度，或许是保护家人最坚实的盾牌。正如民警所说：“骗子最怕你做的两件事：停下来想一想，打官方电话问一问。这两秒钟的停顿，能守住你99%的财产。”

责编/李林惠 编辑/梁莉薇 版式/蔡廷 校对/杨进峰 马骞