甘肃省委省政府调查组关于天水市麦积区褐石培心幼儿园幼儿血铅异常问题调查处置情况的通报

7月12日，甘肃省成立省委省政府调查组，提级调查天水市麦积区褐石培心幼儿园幼儿血铅异常问题。调查组由省委省政府主要负责同志为组长，省纪委监委、省教育厅、省公安厅、省生态环境厅、省卫生健康委、省市场监管局等部门参加，并请生态环境部、国家卫生健康委等部委专家参与。国务院食安办派出工作组指导督办。现将调查处置情况通报如下。

据新华社

看通报原文请扫描二维码

借用电话手表、群发短信能赚钱、买游戏装备下载App……

暑期诈骗套路多 学生群体被盯上

暑假期间，青少年上网时间大幅增加，网络诈骗犯罪分子也趁机“上线”，通过同城交友、游戏福利、兼职刷单等诱饵实施诈骗。近期，全国各地已有多名学生遭遇不同类型的电信网络诈骗，部分家庭遭受较大财产损失。

案例1
手机没电+借用电话手表

近日，湖南省怀化市溆浦县公安局兴隆派出所成功破获一起专门针对小学生的电话卡盗窃案，该案中被盗电话卡被用于电信诈骗等犯罪活动。

经查，4名犯罪嫌疑人流窜至溆浦县，在学校周边活动。他们以“手机没电联系家人”或“借用导航”等借口，向小学生“借用”电话手表。得手后迅速拆解，盗取其中的电话SIM卡。

6月30日，该团伙在溆浦县某学校附近连续作案，骗取了20名小学生的电话卡，并立即转交上线。部分被盗电话卡当天即被用于实施电信诈骗，导致相关号码被通信运营商冻结。

接家长报警后，警方迅速行动。一方面联系运营商协助受害学生注销涉案号码，另一方面联合县反诈中心通过技术手段追踪嫌疑人。7月3日，警方在湖南省郴州市桂阳县将4名犯罪嫌疑人抓获归案。

目前，4名犯罪嫌疑人因涉嫌盗窃罪已被依法采取强制措施，案件正在进一步侦办中。

案例2
自称“警察”+诱导偷拿父母手机

7月4日，湖北黄石阳新高二女生石某加入一个群聊后，被一名自称“卧底警察”的人添加好友，之后掉入陷阱，3天被骗25万元。对方精准报出她的姓名和身份证号，声称“你涉嫌网络诈骗，已立案调查”。

石某又怕又慌，按要求先将自己5000多元生活费转入“安全账户”。紧接着，对方又报出其母亲马女士的信息，威胁“不转母亲银行卡里的钱，就立刻抓你去派出所”。被逼无奈的石某偷偷拿过母亲手机，用短信验证码破解支付密码，将两张银行卡里的25万余元全部转出。

对方还反复警告“这事必须保密，告诉家长就按抗拒调查处理”。直到7月7日，马女士接到警方提醒电话，才发现两张银行卡余额清零，石某这才哭着说出真相。目前阳新警方正在调查此案。

案例3
轻松高薪兼职+群发指定短信

14岁的中学生小雨（化名）想赚点零花钱，很快被一则“急招线上客服助理”的信息吸引，对方许诺“发一条短信一块钱，日赚150元”，工作内容仅是群发指定短信。

小雨信以为真，按对方提供的教程和号码，用父母手机号发送了内容为“你的物件已经到一个半小时了……”的引流短信。发送了几十条后，小雨察觉异常，及时停止了操作。

北京反诈中心发出警示：暑假期间，已发现多名11至17岁的未成年学生被诱骗发送此类诈骗引流短信，且呈现蔓延趋势。

反诈民警强调，学生一旦参与此类“兼职”，不仅可能影响自身电话卡使用，更严重的是已涉嫌违法犯罪，需承担法律责任。从受害者变成“帮凶”，往往仅一步之遥。

案例4
购买游戏装备+添加客服下载App

7月6日，浙江省衢州市一名学生小杨（13岁）在线下购买卡游徽章后，在某App上发帖转售，随后便有人私信联系称想要购买，并让小杨下载另一个App进行交易。

交易过程中，对方称已将钱付给交易平台，让其添加平台“客服”进行收款。随后小杨将自己的收款码发送给“客服”，“客服”称小杨是未成年人，要求其通过父母手机“垫付押金”才能发货。

在对方诱导下，小杨通过视频电话拍摄其母亲手机，并按对方远程指导操作其母亲手机进行汇款。对方以“退押金”为由，反复要求小杨扫码。直至母亲手机无钱支付后，仍未能退回押金，小杨意识到被骗，共计损失3.74万元。

近日，江苏的小张同学放假在家申请了一款新游戏的内测资格，申请失败后不甘心，又到网上搜索，进入了一个声称能办理内测资格的直播间。

对方称，官方内测期间充值可享受返利优惠，还能折上折，小张就按要求进行了多轮充值共计3600多元，还把充值账号密码告诉了对方。对方承诺内测资格和充值金额会在3天内生效，可第二天小张想联系却发现对方失联，意识到被骗赶紧报了警。目前，案件正在侦办过程中。

反诈提示

“三不”原则：不点“免费领”链接，不加陌生好友，不说验证码、密码。

“两立即”铁律：遇恐吓立即关屏幕，被威胁立即喊家长。

务必牢记：真警察不会通过QQ/微信办案，不会要验证码，不会让你用家长手机操作，不会让你共享屏幕。

据央视新闻微信公众号

“万能遥控器”随意开道闸 违法商品何以公开售卖？

在很多单位、小区、学校，或者停车场，进出大门通常需要走道闸。有些无人停车场通过识别车牌的方式，自动抬杆落杆；有些则需要保安通过无线遥控给车辆放行。这样的操作原本是为了保障出入安全，然而却有人打起了这些“道闸”的主意。

在网络购物平台，一种叫作“万能遥控器”的产品在公开销售，只有巴掌大小，号称能打开所有小区的道闸、卷帘门，畅通无阻，轻松实现出入自由。

记者发现此类万能遥控器在网络购物平台种类繁多，介绍产品的视频显示，万能遥控器使用方便简捷，没有复杂的操作。

记者发现，网络上销售的万能遥控器多款产品销售量超过了一万，一款万能遥控器的销量甚至达到了20万。购买者的评价中出现了“保安根本不会发现，太方便了、真不错，能给我省不少钱”等字样。

实测
可以打开小区、学校道闸

记者随机购买了一款销量较高的“万能遥控器”，前往多个小区和学校，按照使用说明进行实地测试。

经过测试，记者可以轻松打开小区的道闸。记者随后测试了多家小区大门和停车场的抬杆，发现大部分均可复制信号并成功开启抬杆。

随后记者来到一所小学，在保安的配合下，共同测试万能遥控器能否开启小学的伸缩大门。测试结果是，网上购买的价值70元的遥控器竟真的能开启学校大门。

揭秘
“万能遥控器”工作原理

无论是校园还是小区，拥有这种万能遥控器，道闸可能形同虚设。万能遥控器的工作原理是什么，为何能轻松实现遥控功能？网络安全专家进行了解析。

网络安全专家王媛媛介绍：“市面上那些能用万能遥控开启的门禁系统，多数采用无线射频中的固定码技术开启。这种方式通过无线发送一组固定的ID和按键码数字，接收端验证ID正确即可开门。”

专家表示，固定码遥控器采用单向明文广播方式，传输特定频段的无线电信号。设备通常不验证信号来源，并采用固定码方式对信号编码。避免信号被截获的最简单方式，是将固定信号更改为滚动式信号，一些重要场所可使用更高级别的二次验证方式或人工按钮开门方式。

王媛媛表示：“滚动码在每次触发开锁时产生的数字不同。即便有人截取其中一组数字，也无法在下一次开锁时使用，因为每次产生的滚动码都不同。”

王媛媛说：“对于重要单位和部门，建议采用整套技术和管理手段进行监控和全面管理。尽量使用二次认证方式部署和使用门禁系统。此外，安全级别要求高的部门或单位，也建议使用人为按键、手工开门方式。这样就不会被不法分子截取无线信号进行破解。”

支招
如何从源头堵住安全漏洞？

道闸设置的核心是保障安全。一个小小遥控器即可随意复制信号自由进出，对居民人身财产安全、校园安全等构成威胁。如何从源头上堵住这一安全漏洞？我们来听听专家的建议。

专家介绍，固定码无线遥控器被广泛使用的原因如下：生产成本很低，生产线较简单；封闭场景，如车库门、家用插座，在距离较短的非联网环境下使用广泛；用户安全意识不足，普通用户并不了解无线信号可被监听和复制。

针对万能遥控器，专家建议：1.制定相关的国家或行业强制标准，对其使用提供分级分类的安全指导。例如对相关设备生产厂家提出要求，注明安全风险和建议使用范围。2.加强相关技术的科普宣传，从教育、博物馆展示、科普宣传等层面，提高人们对这类技术的了解深度和广度。

这种万能遥控器在网络平台公开售卖，其安全问题引起关注。法律专家表示，万能遥控器本身属于违法产品，在网上公开销售，平台也应担责。

中国政法大学副教授朱巍表示：“该产品本身即属违法产品。生产此类违法产品的行为，情节严重可能构成刑事犯罪，如非法经营罪。生产完成后，该产品可能更换名称在网店销售，这是典型的利用电子商务平台从事违法活动。电子商务平台发现销售此类违法产品时，应立即下架制止并进行举报，向公安机关报案。但平台上仍出现大量此类产品，说明电商平台存在失责失察。”

据央视网