育儿补贴还没领到“奶粉钱”骗局已精准送达
诈骗剧本紧跟政策更新 谁在贩卖母婴信息？

9月8日，国家卫生健康委召开新闻发布会宣布，育儿补贴的申领正式全面开放，对3周岁以下婴幼儿按每孩每年3600元标准发放。

一些年轻父母发现，诈骗剧本的更新速度，几乎和政策同步。短短几周内，量身定制的诈骗电话已经瞄准新手父母对育儿补贴的期待，精准锁定目标家庭。对方不仅能准确报出孩子的姓名、出生日期，甚至连申领金额都一清二楚。在层层诱导中，有人差点被骗输入银行卡密码，有人眼睁睁看着“奶粉钱”被划走。

资料图 （北京日报）

“与时俱进”的电诈剧本

36岁的林尧（化名）今年刚迎来二胎，6月底顺利生下宝宝后，听闻有育儿补贴政策，她在支付宝完成了申请。

9月5日上午，她接到四通来自香港的电话。平时习惯拒接境外电话的林尧，心里不免生出一丝疑虑：“连打这么多次，应该是有重要的事吧。”电话那头的男子自称“育儿补贴发放工作人员”，核对宝宝出生日期和申领金额，并告知补贴3600元需分三次领取，如果三个月未提取，第四个月可一次性领取。林尧并不了解流程，便按照对方要求，在手机浏览器输入一串数字网址。

林尧记得，打开网页显示的是“国家卫健委网站”，填写完个人信息和账户信息提交后，网页显示“账户未开通企业收款功能”，需通过线上会议开通。对方又让她改用微信收款，询问她的手机是“苹果还是安卓”，并指引安装“TestFlight”和“办公e服务”两款软件。

她被引导进入一个“线上会议”，另一名“工作人员”接手对话，还提醒她不要接听其他电话。此时对方要求她打开微信钱包，林尧突然发现手机上方的录屏小红点，心里一惊，迅速退出了线上会议。

而王峰（化名）就没那么幸运。

王峰也接到归属地为香港的来电，对方报出他和爱人的姓名及身份证号码，引导他打开支付宝“查询育儿补贴金额”，同样以“没有开通企业收款”为由指引他登录指定网站并下载陌生应用。随后，王峰的手机屏幕出现“白屏”。他看不到对方在做什么操作，直到他收到银行卡金额转出提醒。

王峰这才意识到，在他输入验证码和密码时，银行卡上的5000元已经被迅速划走，对方甚至尝试办理网贷分期，将资金转入银行卡再准备转走。报警后，警方确认第一笔资金已被转入境内账户，第二笔因转向境外而被银行拦截。

信息泄露于何处？

年轻父母们都在疑惑，骗子们为何能够精准地叫出新生儿的姓名、出生日期，甚至连父母的身份证号和补贴金额都一清二楚？

2024年10月，上海市静安区检察院办理了一起侵犯公民个人信息案件。顾先生的孩子刚出生，他就接到一家摄影机构的电话，对方能准确报出妻子的姓名和孩子的出生日期，目的是推销婴儿百天照套餐。

警方追查发现，这些数据来自一家月嫂服务公司的内部人员倒卖。王某某系公司派驻某医院产科的文员，负责管理母婴信息，单独或伙同总公司文员刘某某，将近4万条新生儿母婴信息打包出售，三年间累计获利超过30万元。摄影机构法人邹某某购得信息后，再交给话务公司批量拨打推销电话。

行业“内鬼”是泄露公民个人信息的主要源头，上海市静安区人民检察院公益诉讼部门检察官刘国敏表示，这些人具有职务便利，在工作中可以接触到公民个人信息，继而利用职务便利非法获取公民个人信息，后将上述信息出售获利。

公安部今年公布的十大严打侵犯公民个人信息犯罪典型案例显示，信息泄露的方式多样。

除了“内鬼”，还有通过技术窃取，定向投放木马程序，非法控制内部计算机，进而窃取资料；还有非法采集，比如冒充地图类App工作人员，以“帮商户开通旺铺认证”为名，骗取个体工商户的身份证号和联系方式。

除了被恶意窃取，个人信息“被动泄露”也让公众难以防范：使用公共Wi-Fi时，数据可能被窃取；某些App内置SDK（软件开发工具包）偷偷收集设备信息、通讯录等，还可能读取剪贴板中的验证码、链接；甚至随意分享一张照片，照片的元数据里就可能包含地理位置、设备信息。

隐秘的个人信息交易生意

北京一家信息科技公司的网络安全负责人张鑫解释，在隐私泄露的黑色产业链上，上游为提供技术支持的黑客，或者泄露敏感个人信息的“内鬼”；中游是“贩卖环节”；下游从事诈骗、洗钱等黑产。

上中下游之间早已形成了密切配合：中游根据诈骗需求，分层提供不同精度的数据，下游则依照“剧本”精准出击；诈骗成功后，下游会将经验反馈回中游，推动数据进一步清洗、标签化。合作模式既有“一条龙”团队包办所有环节，也有松散的分工合作，以分成的方式获利。这一条看似松散的链条，借着分工协作，完成了对公民个人信息的“收割”。

记者在海外社交软件上检索关键词“新生儿信息”，很快链接出多个群聊中的内容。其中一个群聊中展示了一张表格截图，共有60条信息，包含“新生儿名字”“出生日期”“性别”“母亲姓名”“母亲身份证号”“联系电话”共六项信息。记者以买家身份联系了这位卖家，对方称一条数据5元，他目前只有四川、青海和广东三个地区的数据，在他展示的一张截图里有14份表格，将近2万条数据。

在另一个名为“实时网购，贷款等”的群组中，记者看到，其中也有多份新生儿数据，每个表格中至少有1000条数据。在这些表格中，每一条婴儿信息中都包含2~3个电话。9月12日，该群组更新表格时备注，目前的新生儿信息有河南、四川、青海、广东、浙江。

这些在群里被发出来的表格，叫作“样本”。按照“行规”，买家觉得样本可用，就会成百上千地购买，交易一般通过加密货币进行。

记者随机加入多个“黑产交流群”，除了交易数据，群中还有很多人寻找合作。有的成员专门撮合买卖，有的充当中间人“找车”（为数据找出路），也有“车找料”（为买家找合适的数据包）。

当诈骗完成，最后的洗钱同样迅速。上海市静安区检察院检察官周梦梦经手的一起案件中，出现了所谓的“三方平台”。这种平台既与境外电诈团伙保持联系，又能在境内迅速调配银行卡资源，安排“车手”完成取现。诈骗团伙一旦掌握受害人资金流向，平台便立刻介入，提供有效银行卡账户，接收转账，再通过层层过账或兑换虚拟货币，将资金转移出境。

防护体系需要多方发力

“当前，电信网络诈骗犯罪已成为数量上升最快的刑事案件类型。”公安部刑事侦查局副局长郑翔曾在《电信网络诈骗及其关联违法犯罪联合惩戒办法》发布会上表示，作为非接触性犯罪，电信网络诈骗犯罪之所以能够实施，是因为有庞大的支撑电信网络诈骗违法犯罪活动的黑灰产从业者，通过出租出售电话卡和银行账户、贩卖个人信息、推广引流、程序开发、“跑分”洗钱等为电信网络诈骗违法犯罪活动提供帮助。

近年来，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等重要法律中均涉及数据泄露问题。

但数据泄露从未停止。最高人民检察院数据显示，2024年全国检察机关起诉电诈犯罪7.8万人，同比上升53.9%；起诉利用网络实施侵犯公民个人信息犯罪2458人。

关于案件追查难点，周梦梦指出两点：一是个人信息出售与流通高度隐蔽，掌握与交易这类资源的通常是“高层”人员，交易多在境外平台或匿名渠道进行，线上身份难以溯源；二是取证与认定门槛高，很多案件需要委托司法鉴定恢复和去重数据。

2024年12月1日，由公安部会同国家发展和改革委员会、工业和信息化部、中国人民银行联合印发的《电信网络诈骗及其关联违法犯罪联合惩戒办法》正式施行。

周梦梦认为，育儿补贴类诈骗既是信息泄露问题的直接后果，也是电诈产业链高度组织化、跨境化的产物。司法机关既要在刑事端追究主犯与参与方责任，也需配合行政监管、行业合规与社会防范，才能从源头和链条两端形成合力遏制这类犯罪。

刘国敏强调，司法只是最后一道防线，防护体系需要行政、司法、行业和公众协同发力。

王峰觉得，自己的经历就是警示。他说，这次教训让他认识到，家长群体必须更加警惕：不要轻易接听陌生来电，不要下载来源不明的App；储蓄卡最好关闭境外交易权限，并设置每日转账限额。

（新京报）