新办的手机号为何频频收到骚扰信息

“你名下贷款逾期2300天”“尽早处理避免风险升级”……西安市民彭女士不久前办理了新手机号码，却频频收到针对前任机主的催债信息，“我解绑了好几个应用平台，还是每天收到这类信息。”最终，她无奈地换掉了手机号。明明是新办的号码，为何用户却会遭遇催债、垃圾信息骚扰等问题？

号码易主，旧信息难清

记者发现，黑猫投诉等平台上，与新手机号相关的投诉达上千条。一些用户在注册互联网应用时发现号码已被占用，有的还发现平台上留有前任机主订单，不支付就无法继续使用相关应用。

北京市民王先生告诉记者，办理新手机号后，他经常收到某出行平台发来的不属于自己的酒店订单信息，内容十分详尽，入住人姓氏、酒店名称、房型、入住日期、金额等信息一览无遗。

有网友曾发帖称，自己使用新办的手机号注册一家音乐平台时，输入收到的验证码后，居然自动登录上了已故知名歌手的账号。对此，该平台客服反馈，这一情况是艺人账号绑定的手机号被“二次放号”导致的。

所谓二次放号，指的是老用户注销手机号后，运营商将注销号码经过一段时间的冷冻期后，重新投放市场供新用户使用。电信服务规范规定，号码冻结时限最短为90日。

“二次放号最重要的原因，是号码资源紧张。”中国移动相关业务负责人表示，业界公认号码利用率超过50%即为号码资源紧张，而当前号码利用率已超过50%。

与此同时，部分新号码因用户偏好、文化习俗等原因从未被选用，易记、寓意好的号码往往曾被使用，因此新投放市场的号码不少为二次号码。

为何不能有效拦截？

去年以来，工业和信息化部推动“二次号码焕新”服务，主要包括由运营商为用户提供“批量焕新+主动焕新”服务。

批量焕新，是指把即将投放市场的回收号码提前批量推送给互联网应用方，在重新放号前完成解绑；主动焕新是指为使用二次号码的用户提供焕新服务入口，用户可自主操作，一键解除手机号码开户前已经存在的互联网应用绑定和号码标记。

工业和信息化部今年1月发布的数据显示，基础电信企业在放号前批量焕新二次号码超2.5亿个，解绑互联网应用超10亿件次；在官方APP和小程序上线主动焕新服务入口，支持解除与239款常用互联网应用的历史绑定，为580多万用户处理解绑申请超3.6亿件次。

随着各方采取行动，当前，应用解绑难题得到一定程度缓解，但前任机主遗留的催债、营销等骚扰信息“轰炸”仍无法根除。

“在二次放号过程中，部分前用户绑定过非常用应用和网站，此类应用和网站数量庞大，运营商难以一一核实并通知相关应用、网站运营主体进行解绑。”中国移动相关业务负责人表示。

那么，运营商能否通过抓取已注销号码信息中的关键词等前置手段，鉴别、筛选风险号码，从而避免将其释放给新用户？

中国移动、中国联通相关业务负责人均向记者表示，用户销户后，运营商与用户的电信服务合同即告终止，不能随意抓取信息并进行分析，否则将涉嫌违反个人信息保护法。不过，对经权威部门标记的涉诈、骚扰营销等高风险号码，运营商可按照上级主管部门规定，执行延长号码冷冻期、暂缓重新投放等措施，最大限度降低新用户承接风险。

进一步构筑权益保护墙

如何进一步降低二次放号对用户的负面影响？

“为更好保护用户权益，运营商应在分配号码时以显著方式告知新用户该号码是否属于二次号码，确保用户的知情权和自主选择权利。”北京市华泰律师事务所高级合伙人邓佩说。

记者了解到，已有运营商设立明确规定，要求营业人员在为用户办理新号码入网时，明确告知所办理号码是否为重新投放市场的二次号码，以确保用户知情权。

彭女士告诉记者，自己在办理新手机号时，并未被告知号码是否曾被使用。“营业人员只是拿出一本号码册，告诉我上面的号码都可以选。”也就是说，一些基层营业网点在履行告知义务方面仍存在瑕疵，需要进一步强化指导、压实责任。

从用户选号、使用角度来看，业内人士建议，用户在办理销户或过户前，主动检查并解绑个人常用互联网应用账号，避免因号码流转造成个人信息或账号资产泄露。

如遇到二次号码相关骚扰、信息错发等问题，可优先通过“二次号码焕新”服务申请解绑相关应用。如遭遇违法催收或骚扰，建议保留证据并向12378银行保险消费者投诉维权热线、公安机关或网信部门投诉举报，依法维护自身权益。

通信运营商表示，下一步将会协同主管部门，进一步扩大“二次号码焕新”服务应用范围，与各企业加强互认体系建设，推动更多互联网应用平台接入解绑平台。

新华社“新华视点”记者 张千千 高亢
（新华社北京4月9日电）

利用AI抓热点，炮制“爆款”博流量

起底新型网络“水军”犯罪手法

利用AI抓取热点，一键生成“黑稿”……近年来，网络“水军”犯罪呈现新动向，一些不法分子利用网络平台的算法逻辑，使用AI等技术故意炮制负面信息，操控海量“水军”账号同步炒作，借流量牟利。

近期，山东烟台警方抓获两个专门炒作新能源汽车负面信息的新型网络“水军”团伙，关停网络账号8000余个。这些“黑稿”是如何炮制出来的？背后存在怎样的利益链？

操纵“水军”炒作负面信息博流量

2025年7月以来，理想汽车、华为鸿蒙智行、小米公司等知名企业先后向烟台市公安局报警称，某知名网络平台出现大量涉及相关品牌新能源汽车质量、企业负责人的负面文章。

这些文章有的以耸动的标题抓人眼球，如“M9交付遥遥无期，尊界投诉榜遥遥领先”“雷军这次真的摊上大事了”；有的歪曲事实误导公众，如“偷偷减配，给消费者一个答复”“理想死鸭子嘴硬，月销量没突破过四位数”。

警方研判发现，发布这类文章的账号数以千计，不仅IP地址集中，发文时间、内容也较为集中。针对这些异常现象，警方经过数月侦查查明，网络“水军”团伙注册多家公司，利用MCN机构操纵数千个平台账号发布文章。

相关内容呈现出高度的组织化特征：有的串联炒作、歪曲解读，对企业进行恶意诋毁；有的伪装身份、虚构场景，冒充消费者发布不实体验；有的搬运洗稿、批量炮制，将个别问题放大渲染。表述各异但指向相同的海量负面信息短时间内集中发布，瞬间占领网络空间。

山东烟台警方查处的网络“水军”团伙办公窝点。**图据新华社客户端**

有受害企业表示，曾以为这是同行攻击或敲诈勒索，但警方查明，网络“水军”的牟利模式为利用大量账号发文的转发和评赞数量，获取平台支付的流量收益。

利用AI批量生成“黑稿”推送

办案民警介绍，相较于过去以“造谣引流”“舆情敲诈”“有偿删发帖”等为目的的网络“水军”案件，新型网络“水军”不敲诈、不收费、不引流，利用AI技术等批量炮制“黑稿”，“量大管饱”，只挣平台流量费。

——使用AI写稿，实现规模化“生产”。新型网络“水军”通过AI软件对抓取的热点词汇和内容进行重组、改写，伪装成个人体验或观点进行发布，实现了内容的批量、快速生产。

——搭建账号矩阵，形成流量积累效果。由于平台规则是流量收益与账号的发帖量、浏览量成正比，单个账号赚钱微乎其微。因此，新型网络“水军”为了扩大影响、获取不法收益，往往搭建规模惊人的网络账号矩阵。

经查，团伙核心人员于某等人使用30多个MCN账号，操控了8000多个个人账号，达到规模化、地毯式推送同质化内容，人为制造舆情。

这些账号都是批量买来，1个MCN账号一般要上万元，实名注册的个人账号则几十元1个，有的号主本人对买卖不知情甚至不知道注册过账号。

——多种工具助力，“小作坊搞起大流量”。新型网络“水军”从管理账号到找素材、发文章均使用自媒体管理软件完成。这些软件中，有的可以提高内容分发和账号管理的效率，有的可以批量管理母账号、子账号，查看收益、发文情况，还能搜集全网热点话题、潜在爆款素材，并有现成创作模板。

“这些工具大大降低犯罪门槛，让缺乏专业技术的小团队也能吃上‘流量饭’。”烟台市公安局经济技术开发区分局网络安全保卫大队大队长陈天胜说，一个团伙的主犯仅受过小学教育，另一成员待业在家。他们租了个房子、买了几台电脑、找了几个员工，就开始“低成本创业”。他们专门炒作负面信息，什么火就发什么，1个月能赚二三十万元。

平台守牢责任 监管仍需完善

据悉，本案中的9名犯罪嫌疑人因涉嫌侵犯公民个人信息罪，现已被依法采取刑事强制措施。

“新型网络‘水军’眼里只有流量，今天炒作新能源汽车，明天就可能涉足其他热门领域，危害不容小觑。”受访专家建议，网信、公安、市场监管等部门加强联合执法，严打包括账号买卖、工具开发、资金结算在内的“黑产链”，推动刑事司法衔接。

办案民警表示，平台流量分发主要依赖点击率、点赞数等指标，新型网络“水军”犯罪利用了平台的自媒体流量扶持计划，借助平台对MCN机构的倾斜，实现一个母账号操控成千上万个子账号。

中国人民大学法学院教授刘俊海认为，平台应全面改造流量奖励机制和账号监管机制，从“唯流量”的奖励机制，转向社会价值、安全发展等多维价值取向；此外，加强个人信息比照、内容原创、互动真实、账号活跃等方面的账号真实性核查。

新华社记者 王阳
（据新华社济南4月8日电）