

微信群里抢“红包”成“洗钱帮凶”

男子因犯掩饰、隐瞒犯罪所得罪被法院依法判处拘役4个月

□ 记者 沈媛 通讯员 汪百顺

添加微信群聊、输入口令、领取红包，简单操作几下就能轻松拿到“佣金”！然而，这些红包里装的却是电信网络诈骗分子骗来的钱。近日，经金山区人民检察院提起公诉，蔡某因犯掩饰、隐瞒犯罪所得罪被金山区人民法院依法判处拘役4个月，并处罚金3000元。

今年1月，待业在家的蔡某偶然发现一条赚钱的路子，上家（已另处）告诉他只要在微信群里抢“口令红包”，就能获得不少提成。在对方介绍完后，蔡某不禁怀疑，居然有这种直接领钱的“好事”，便询问上家“红包”的来路，对方称红包里的钱是“赌博”的资金。蔡某脑海里浮现出了“跑分”两个字，原来所谓的“兼职”是这种违法犯罪的事，但舍不得对方许诺的报酬，犹豫之下，蔡某还是抱着侥幸心理照做了。

很快，蔡某便抢到数千元的红包，并按照之前的约定，自己留下4个点的“佣金”，他算了算，一天竟然能挣四五百块，这样下来月入破万也并不是难事，如此“不劳而获”的赚钱方式让他暗自窃喜。

蔡某沉浸在“抢红包”赚钱的甜头里，一收到“口令”就意味着“工资”到

账，渐渐地，蔡某开始不满足于此。他找到上家称自己可以召集一些进群抢红包的朋友，由他来做“群主”发号施令，待所有人抢完红包后，蔡某将除去“佣金”的钱款汇总给上家。

对方则表示，蔡某在“上交”余款时，需要下载特殊的软件，将资金兑换成虚拟货币再转至专门账户，蔡某可以拿到更多报酬。收到上家发来“升级版”的“跑分”指示，虽然更加笃定对方在做违法的事，但是为了钱，他决定继续操作。

红包里的钱来源到底是谁呢？周先生就是其中之一。今年2月，周先生和网友在群聊内交流投资理财方面的心得，谈及虚拟货币时，对方向周先生推荐了一款专门用来投资的App。接着，周先生在其声称“回报快”“收益高”的诱惑下，逐步在App中充值9000余元，待到周先生要求提现时，却发现无法操作，意识到被骗后，遂报警。

经侦查，警方很快锁定了蔡某，原来蔡某等人抢的红包均是源于上游电信网络诈骗被害人的资金。今年4月，蔡某及其团伙悉数落网。

【检察官提醒】

《刑法》第312条规定：明知是犯罪所得及其产生的收益而予以窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金。

“轻松”且“高薪”的工作，背后暗藏的可能是违法犯罪的陷阱，诸如利用微信、支付宝等“抢红包”，或提供网上银行的登录密码、刷脸识别等，帮助上游犯罪转账。检察官提醒大家，千万不要为了蝇头小利，将银行账户、支付密码等提供给他人以谋取利益，切莫为了贪图挣快钱让自己成为不法分子的帮凶。

帮取手机、帮买黄金就能赚钱？

杨浦检察院办理两起涉嫌掩饰、隐瞒犯罪所得案

□ 见习记者 王葳然
通讯员 杜佳妮

本报讯 只要帮忙代取装有手机的快递，并将手机回收，就能获取高额报酬？只要帮忙到金店消费，并将所购黄金交给他人就能收到大量好处费？近日，杨浦区人民检察院办理两起帮取手机、帮买黄金涉嫌掩饰、隐瞒犯罪所得案。

今年上半年，李某在游戏软件中结识的网友向其介绍一份兼职，只需帮忙收取装有某品牌手机的快递并回收，再将钱款转给他人，就能获得高额报酬，李某欣然同意，该网友还邮寄了专门用于接听快递电话的手机给李某。

据李某供述，其在对方的指令以及邮寄手机、虚构

数名收件人等异常情况中知晓购买手机的钱款来源不当，是上游犯罪所得，但为了高额报酬，同时法律意识淡泊，认为自己没有参与上游诈骗，只是帮忙取快递，他人的犯罪行为与自己无关，故选择“铤而走险”。短短两周时间，李某代取快递的涉案资金就达到30余万元。

无独有偶，廖某从工友处得知帮忙代买黄金可以获得高额好处费，在知晓资金来源存在问题的情况下，仍根据上家的指示，用上家提供的银行卡到金店帮助购买黄金进行资金转移，涉案金额40余万元。

目前，犯罪嫌疑人李某已依法被杨浦检察院批准逮捕。被告人廖某因犯掩饰、隐瞒犯罪所得罪，经杨浦检察院提起公诉，被法院判处有期徒刑1年6个月，并处罚金1万5千元。

【检察官说法】

近年来，电诈犯罪、掩隐犯罪频频发生，二者之间相互关联。

对于掩隐嫌疑人来说，世上不存在不劳而获，付出与报酬不符的工作更不存在，切莫贪图那小小的“好处费”而搭上自己的人生，同时要增强法律意识，千万不要觉得自己未参与上游诈骗，只是帮个忙、跑个腿就不会涉嫌犯罪。

对于回收店铺员工来说，针对黄金、手机等高价值物品的回收，通过问询、登记、索要发票等方式，仔细甄别是否存在明显低于市场价、无法说明来源、不配合登记等异常情况，如发现不对劲及时报警处理，切莫贪图便宜而违规回收。

网页总是自动跳转？背后竟是“劫持流量”的猫腻

□ 记者 季张颖 通讯员 杨莹莹

瞄准互联网时代下“流量劫持”的“商机”，恶意利用静默插件，实现用户在访问某知名搜索平台时，自动添加或更改为被告单位的计费名从而获取流量费。近日，经闵行区人民检察院提起公诉，被告单位某信息科技有限公司犯非法控制计算机信息系统罪，被闵行区人民法院判处有期徒刑20万元；被告人王某、李某基、肖某、李某磊，犯非法控制计算机信息系统罪，被判处有期徒刑1年9个月至3年不等，均适用缓刑，各并处罚金。

程序员发现流量劫持敛财猫腻

周先生是一名程序员，闲暇之余喜欢上网浏览新闻。最近在家使用电脑时，他发现了一件奇怪的事情：每次自己在输入某知名搜索平台的域名后，总会自动跳转到别的网站。哪怕周先生重启浏览器或者清空浏览器cookies后，问题依旧没有解决。

周先生从事互联网行业颇久，他敏锐地意识到，这是一种流量劫持的方式。“应该是我的搜索网页被劫持到特定的渠道商那里了，只要我使用这个搜索平台就会产生流量，渠道商可能会从平台拿到一定的流量费用。”察觉到不对劲的周先生立即前去派出所报案。一个专门靠劫持流量敛财的信息科技公司随即进入警方的视野。

2015年末，被告人王某、李某基、李某磊、肖某从某互联网公司离职。经过深入沟通，四人决定合作创办一家信息科技有限公司，主要是做一些软件或小程序，比如桌面清理软件或者购物平台返利软件等。

生意不景气时，他们也会调整业务方向，做一些弹窗广告业务或者短视频动画等。王某回忆，创业之路“走偏”发

生在2022年的春天。那年的315晚会曝光了他们公司的软件推广渠道商，公司所做的软件安装量因此下降很多。

团伙分工明确，违法获利8万元

一边是业务的急剧收缩，另一边是公司日渐入不敷出。面对这些不利因素，王某等人有些“慌不择路”。偶然向他人了解到，可以通过静默安装插件，更改用户电脑中浏览器的计费名获得流量收益后，他们立刻召开内部会议进行讨论，决定开启该业务。

“计费名就是这个搜索平台公司给我的推广渠道号。我之前有通过商务推广渠道向某知名搜索平台申请过数十个计费名。如果用户使用的搜索平台的网站链接中带有我们公司的计费名，平台就知道是我们公司介绍来的客户，就会给流量费。”被问及如何实现替换电脑用户计费名时，王某供述道。每次用户安装完自家公司开发的软件后，就会静默在用户的浏览器中安装浏览器插件，实现浏览搜索平台时，自动添加或更改公司申请注册的计费名。

整个犯罪流程不仅环环相扣，涉案公司内部也层级严密、分工明确。在王某提出大概的业务框架后，肖某、李某磊负责开发电脑端的相关软件，李某基负责公司所有服务器的运营维护。

经鉴定，涉案公司的两款软件可进行静默安装浏览器插件，具有流量劫持功能，违法所得共计8万余元。

闵行检察院认为被告单位某信息科技有限公司、被告人王某、李某基、肖某、李某磊违反国家规定，采用技术手段非法控制他人计算机信息系统，其行为已触犯刑法相关规定，涉嫌非法控制计算机信息系统罪。法院经审理作出前述判决。