

起底手机维修诈骗套路

# 线上“挂羊头卖狗肉” 线下夸大故障骗钱

近日,一些不法分子利用人们急于维修手机的心态,线上精心制作以假乱真的网页“引流”;线下设计话术,虚构或夸大手机故障,甚至以次充好偷换零件,目的只有一个——骗取高额的维修费用。从开始表示 200 元维修费即可,到最终 3000 多元的实际付出,消费者就是在不法分子的“连环套”中,陷入被骗深渊。

上海警方日前成功打掉一个线上客服低价揽客、线下门店虚假维修的诈骗团伙,在全国多地抓获以吴某为首的 20 名犯罪嫌疑人,涉案资金超过 3000 万元。

## 200 元涨到 3200 元 高价换屏却维修“无痕”

今年年初,家住上海长宁区的倪先生不慎将手机摔落在地,手机屏幕摔出了几条裂痕,虽然手机仍能正常使用,但倪先生觉得它并不美观。于是,他通过网络搜索该手机的品牌维修商,浏览了“品牌维修商”网页后,他拨打了排名靠前的“客服电话”。

“当时客服人员详细地询问了我手机的型号、购买时间、故障问题等,然后表示仅需 200 元就可以维修。但客服也告知,要看到实物后才能最终确认。”倪先生告诉记者,“我前往客服指定的位于中山公园附近某写字楼内的实体门店。”门店一位工程师将手

机拿进操作间进行“拆机检修”。数分钟后,工程师告知倪先生,开屏检修后发现,手机不仅外屏碎裂,内屏也已经损坏,无法正常使用,只能更换屏幕。倪先生只能同意更换“原装屏”,价格为 3200 元。

不到 2 个月时间,倪先生手机再度出现故障。倪先生有感于上次维修费“贵到离谱”,没有再上网找客服,而是直接前往该品牌手机的官方维修点。在维修过程中,工作人员告诉倪先生手机的内屏并没有修理或者更换的痕迹,也没有明显故障。“我听了当时脑袋就‘嗡’地一下,意识到之前肯定是被骗了,于是马上向长宁公安分局新泾派出所报案。”倪先生说。

## 低价引流以次充好 “线上线下”联手骗钱

上海长宁警方接到报案后,根据倪先生提供的线索,经过数据分析和综合研判,锁定了一家位于福建、名为“量子穿梭传媒有限公司”的企业。经过警方排查,发现这家“传媒公司”竟然在全国 6 个城市开有 20 家手机维修实体店或加盟店,同时在各大电商平台上设立了 15 家网店。

“经过我们的调查发现,虽然这些店铺在网络搜索中都声称是‘品牌官方维修点’,但却经常发生消费纠纷。”新泾派出所执法办案队副队长高飞告诉记者,



者,“一方面是‘挂羊头卖狗肉’假冒官方维修点,另一方面还消费纠纷不断,种种迹象表明,这是一家‘线上李鬼、线下狠贵’涉嫌欺诈的店铺。”

经过深入调查,警方发现这是一个通过网络发布广告招揽客户,以低价诱骗客户上门或者寄件维修,进而骗取高额维修费用的新型诈骗团伙。9 月中旬,上海长宁警方在当地公安机关的协助下,在广东、湖南、山东、安徽等地同步集中收网,成功抓获团伙主要犯罪嫌疑人吴某等人。

到案后,犯罪嫌疑人如实交代了犯罪手法和作案过程。“线下维修”由该团伙在各地招募开设的实体手机维修店铺进行。客户到店后,工程师采取虚构、编

造、夸大手机故障并制造黑屏、无法开机等假象,最终迫使客户同意支付高额维修费用。实际上,所谓的“原厂配件”都是假冒或者二手配件,有的甚至根本没有更换。而如果客户拒绝维修,工程师也会暗中将手机原装配件拆下替换,将原装配件倒卖获利。

## 小维修做成“大买卖” 维修服务还需多重视

长宁公安分局刑侦支队副支队长钱俊在接受记者采访时认为,本案中犯罪嫌疑人实施诈骗有两个关键步骤,一是线上招揽客户,二是线下实施诈骗。“从我们的调查中发现,线

上客服除了低价招揽客户、提示维修风险外,还会在沟通过程中尽量收集客户个人信息,分析脾气性格,研判是否了解手机专业知识,这样既能选择高端手机,提升获利空间,又能帮助线下工程师实施诈骗提高成功率。”钱俊说,“尤其在维修阶段,团伙成员还专门精心编制了一整套话术来培训员工。”

另一方面,犯罪团伙将线下门店都开设在直辖市或省会城市的中心城区商务楼里,给消费者“高大上”的感觉,误以为是正规的品牌维修点。此外,不法分子开设的店铺均没有明显的店招和广告牌,客户必须凭借预约码在指定时间上门。

钱俊介绍说:“这样做的目的,就是避免接待自行上门、未经事先沟通掌握信息的客户;同时也确保在某个时间段内只接待一位客户。消费者以为自己是享受了‘VIP 服务’,殊不知这是犯罪团伙为了避免客户间相互沟通,造成‘穿帮’的风险。”

“现在很多手机、电脑等价格昂贵,换配件、维修的费用相当高,这让不法分子看到了非法牟利的空间,警方也将不断加大维修类服务诈骗行为的打击。此外,警方还提示大家,无论选择何种维修方式,一是要选择正规渠道,二是在维修服务完成后,务必保留相关维修和交易凭证,便于事后追查。”高飞说。

据新华每日电讯

## “行业助考”形成灰色产业链——

# 付费“助考”悄然滋生 笔试“枪手”肆意横行

“xx 银行笔试发车!包进面试!100%一手题源答案……”眼下,正值秋季校园招聘旺季,不少企业出于疫情防控的需要,将笔试从线下改到线上进行。尽管招聘方事先强调,杜绝任何作弊行为,并要求打开电脑摄像头进行实时监控,但仍有付费“助考”在暗地里悄然滋生。

## 微博发布广告 笔试一场 300 元

先后收到三家银行的在线笔试通知,应届生小雅心中欢喜,但更多的是忐忑。“这些银行的校招笔试向来都很难,竞争特别激烈,想进面试实在不是件容易的事。”为做好准备,小雅开始四处搜索笔试攻略,却意外在网上发现了“秘密”,“本以为只是梳理总结往年题型,没想到还有人号称知道在线考试怎么‘钻空子’,可以提供付费‘助考’”。

小雅所说的“助考”,在校招圈子里并不少见。记者在微博上搜索“银行笔试”,结果看到多个账号公然发布“包进面(试)”的广告,并主动留下微信号或 QQ 号码“引人上钩”。

“四大、交行、三桶油等国企,三年助攻经验,包进面试,以往秋招春招 100 多场笔试题源记录验证,信誉第一……线上笔试抓住机会,一场 300 元进面试!”以其中一个账号为例,博主



特意将封面图片做成“广告牌”,打出业务范围及联系方式。而近期的微博内容,也几乎都与当天的“笔试发车”有关。

“笔试都没有考前答案,所有说考前答案的全是骗子。我们团队是研究生,3 人到 5 人同时做题,行测、金融、经济、计算机、英语、常识、时政,有什么做什么,每个人负责不同的模块,开考以后边做边发答案,速度肯定没问题。”对方信誓旦旦地表示,笔试正确率约 80%,包进面试。

## 介绍作弊方式 可以远程控制

记者在调查中了解到,为避免求职者作弊,大多数企业已经在考前明确告知纪律要求,如“考试全程不要使用 QQ、微信等

网络社交软件及手机交流信息,不要佩戴耳机”“按系统要求开启摄像头,对准面部,禁止替考”“限制切屏次数,切屏次数超过 3 次,将视为无效,取消本次考试成绩”“如发现摄像头遮挡、麦克风静音或其他违反承诺的行为,将取消相应求职者录用资格”等。

不过,“助考”组织者显然有备而来。“笔试一般分为单机位和双机位,其中双机位的银行很少,90% 的银行都是单机位。单机位时,摄像头只能拍到你的脸,拍不到你的手,手机放边上自己看。”说罢,对方还“贴心”地附上实物参考图片,以便直观了解手机和电脑屏幕的位置关系。

在对方看来,即使是双机位,也不难应对。“手机只要放在盲区就行,可以把电脑垫高一

点,这样一机位摄像头对准的就是你的头部,你的手可以自由活动。官方给你的示范和你真正摆好的机位是有差别的,多练习几次。如果允许闭麦,就找朋友边上报答案。”

此外,“助考”组织者还给出不同的助考方式。“通过远程控制软件,可以直接帮你作答,也可以拍题目一对一服务。如果不会操作,那就在群里等答案,我们用题目加答案的方式给出。笔试题目一样,顺序不一样,答案需要自己找。”

## 钱款有去无回 重则触犯法律

“包进面,不进全额退款。”尽管不少“助考”组织者都会给出承诺,但实际操作中,还是经常有求职者遭遇钱款“有去无回”的情况。“对方收了钱以后,很可能只是随便发来点答案,然后利用拉黑等方式‘人间蒸发’,自己就算发现被骗,也只能忍气吞声,毕竟这种事见不得光。”尽管“助考”广告诱人,但小雅深知其中套路颇深,“像那些利用远程控制软件作答的,想想更觉得可怕”。

日前,北京银保监局发布风险提示,提醒消费者远离屏幕共享骗局。北京银保监局表示,屏幕共享功能会把屏幕上显示的内容全都记录下来,并同步让对

方看到,不法分子可以实时监控用户手机的所有操作,不仅包括输入密码、解锁的过程,还有弹框显示短信、微信、其他 APP 推送的内容。

事实上,“助考”带来的潜在风险远不止于金钱上的损失或考试机会的浪费。记者了解到,尽管企业招聘考试通常并不属于“法律规定的国家考试”,但最高人民法院、最高人民检察院《关于办理组织考试作弊等刑事案件适用法律若干问题的解释》第十条也指出,在法律规定的国家考试以外的其他考试中,组织作弊,为他人组织作弊提供作弊器材或者其他帮助,或者非法出售、提供试题、答案,符合非法获取国家秘密罪,非法生产、销售窃听、窃照专用器材罪,非法使用窃听、窃照专用器材罪,非法利用信息网络罪,扰乱无线电通讯管理秩序罪等犯罪构成要件的,依法追究刑事责任。

同时,第十一条规定,设立用于实施考试作弊的网站、通讯群组或者发布有关考试作弊的信息,情节严重的,应当依照刑法第二百八十七条之一的规定,以非法利用信息网络罪定罪处罚;同时构成组织考试作弊罪,非法出售、提供试题、答案罪,非法获取国家秘密罪等其他犯罪的,依照处罚较重的规定定罪处罚。

据《北京晚报》