小心！骗子盯上“金三银四”招聘季

开启共享屏幕进行岗前培训、刷单完成公司任务、面试涉密须上交手机……随着“金三银四”招聘旺季的到来，各种网络诈骗开始围猎求职者。骗子甚至潜入招聘平台，发布岗位信息引流，以核查资质、征信等名义诱导求职者“入坑”，导致一些求职者工作还没找到，就被骗走了钱财。

1 招聘平台推送“好工作” 信用测试骗走十余万

北京市民余先生在某招聘平台挂出简历，前些天收到平台推送的一则职位信息——“番茄小说”招聘打字员，不仅可以居家办公，而且薪资十分优厚，他觉得这是个不错的选择。

“湖北省××网络科技公司？怎么不是‘番茄小说’的公司？”当看到招聘主体是一家远在湖北的网络科技公司时，余先生心中闪过一丝疑虑，但还是主动与对方取得联系。

沟通过程中，“人事经理”先是简单介绍了岗位内容和任职要求，随后诱导余先生脱离招聘平台，添加私人联系方式继续沟通。紧接着，对方提出一个奇怪的要求：需查看余先生的支付宝征信记录，进行岗前资质核查。余先生按照对方要求，将支付宝总资产截图发给了对方。

随后，“人事经理”又要求余先生开通花呗，在线给其提供的一个手机号码充值500元，并承诺“这只是一个信用测试，钱是不会实际扣除的”。然而，余先生开通花呗并完成充值后，发现500元已经成功扣款。对此，对方故作吃惊，表示只要完成资质审核，会将钱款全部转回余先生的账户。

接着，对方又以信用测试为由，通过电话指导余先生向一个陌生账户转账多笔钱款。在对方的持续诱导下，余先生陆续转账十余万元。随着转账数额不断增加，余先生的不安也愈发强烈，频频催促对方尽快退款。可对方一边满口承诺立即退款，一边又以余先生的银行卡有问题为由，推脱钱款无法到账。

此时，余先生终于察觉出上当受骗，赶紧向警方报案。可报案时他发现，那个曾经吸引他的岗位，早已从招聘平台上“消失”得无影无踪。

2 明明是正规渠道发布 怎么就成了一场骗局

“明明是招聘平台推送的工作，怎么会是骗局？”这是余先生被骗后最想不通的事。

北京市公安局刑侦总队十支队反诈民警高山告诉记者，招聘平台会对入驻企业的营业执照等资质进行审核，一旦企业账号信息泄露，或被不法人员用特殊手段盗用，就可能被骗子操控，发布虚假招聘信息。

拥有十余年人力资源行业经验的王先生也向记者证实：企业在招聘平台注册，需先提交营业执照等资质证明，审核通过后，每次登录平台还需经过账号绑定的手机号验证。“但在极端情况下，如果不法人员掌握了账号密码和验证信息，账号就有可能被非法利用。”

高山介绍，招聘诈骗的引流手段极具隐蔽性和迷惑性。除了盗用招聘平台企业账号，很多骗子还会在抖音、快手、小红书等社交平台发布招聘信息——他们将昵称改为“××公司HR”，冒用企业LOGO作为头像，伪装成正规公司的人事专员以提升可信度，再通过私信、群聊、评论留言等隐蔽方式，主动接触求职者。

“电信网络诈骗的核心特点是‘不见面’，因此涉诈招聘信息多以配音、打字等兼职工作，或‘居家办公’类岗位为幌子。”高山表示，骗子正是利用兼职、居家办公无需线下见面的特点，将“核查信用”“资质认证”“线上面试培训”等诈骗圈套，伪装成岗位招聘的“必经流程”，一步步诱导求职者转账、充值。

据了解，求职招聘诈骗的受害人年龄主要集中在22岁至46岁之间，其中，刚走出校园的大学生、离职换工作的中年人是最易“中招”的群体。“骗子之所以能够得逞，正是摸准了求职者急于上岗的心理。”高山分析，求职者都希望尽快找到工作，等待时间越长越心慌，一旦遇到看似合适的岗位，生怕被别人抢走，便会下意识配合招聘方的要求，不仔细甄别就照做，接受所谓的“测试任务”，甚至缴纳“保证金”“培训费”，最终落入诈骗陷阱。

3 岗前培训下载“内部App” 招聘各环节都可能有“坑”

记者采访部分被骗求职者发现，骗子的招数五花八门，暗藏在“招聘”的每一个环节，让人防不胜防。

最常见的陷阱便是刷单返利。受害者王先生告诉记者，他看到一条招聘司机的信息后与对方联系，被要求下载该公司“内部App”进行工作能力测试，测试内容是查询航班、制作表格等简单任务。干了两天后，对方通知他被录用，还发了个红包作为“报酬”，同时推荐他做高佣金的返利任务。

“当时光顾着高兴，不仅顺利找到工作，还这么快挣到钱，就欣然接受了，也没多想想这样的好事怎么会落到自己头上。”王先生坦言，原来骗子给的“甜头”，只是为了增加迷惑性，一旦他大额充值，骗子就会以“操作失败”“账户冻结”为由，让他一次次缴纳解冻金、保证金等费用，最终血本无归。

培训环节也藏着“暗坑”。求职者李女士向记者介绍，她在网上应聘一份绘图工作，骗子以“想获得工作机会，需先接受职业培训”为由，要求支付8000余元培训费，还承诺培训期间会给她安排绘图工作，帮她挣回培训费。可事实上，骗子收了培训费后，便彻底失联，再无任何回应。

还有的骗子会让求职者下载会议类软件，在线上开启屏幕共享“完成岗前培训”。反诈民警一语道破其中玄机：在此过程中，骗子会以“岗前培训任务”“系统测试”为由，让求职者往指定账户充值，承诺入职后立即返还，实则借机窃取求职者的银行卡号、密码、验证码等关键信息，远程完成转账盗刷。

更有甚者，利用招聘收集求职者的银行卡、手机卡，用于实施诈骗犯罪，而无辜的求职者却被蒙在鼓里，沦为骗子的“工具人”。反诈民警介绍，有的骗子以“登记工资卡”为由，让求职者提供银行卡，实则用这些银行卡转移电诈赃款；有的则以“面试、培训内容涉密，防止拍摄外传”为由，要求替求职者暂时保管手机。求职者根本想不到，在两三个小时的“面试”“培训”期间，骗子会拔出事主手机中的手机卡，用于拨打诈骗电话。

4 “共享屏幕”“入职先垫资”都是诈骗

“其实，分辨招聘信息是不是电信网络诈骗，关键要抓住电诈的核心特点。”高山结合案例，给出了五项具体防范要点：

首先，骗子通常通过网上隔空诈骗，而正规招聘大多会对应聘者进行线下或线上视频面试。因此，对于打着“居家办公”旗号、连面试都无需进行的招聘信息，一定要提高警惕。求职者可通过国家企业信用信息公示系统等渠道，核查招聘公司的资质和经营状况，确认其合法性。

第二，正规公司招聘，不会要求求职者下载小众通联软件或非应用商店的App。使用小众通联软件、下载不明来源的App，是骗子诱骗事主脱离原平台监管、私下联络，进而洗脑实施诈骗的关键步骤，一旦遇到，务必警惕。

第三，正规公司的培训大多在线下进行，不会要求求职者下载会议类软件并开启屏幕共享。共享屏幕是骗子窃取事主银行卡号、密码、验证码的重要手段，只要对方提出“共享屏幕”的要求，就可以直接判定为诈骗。

第四，求职者找工作的核心目的是赚钱，无论是“核验资质”“入职测试”，还是“刷单任务”，只要要求求职者先垫资、先付钱，千万不要相信，直接拒绝并远离。

第五，只要对方要求提供银行卡号、验证码、密码，或是强行要求上交手机，一律是诈骗，需立即终止沟通，并及时向警方举报。

（据《北京晚报》）