保定晚报编辑部主办 E-mail:bdwbzbs@126.com 责编:盖继文

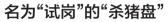
"试岗"杀猪盘,群里同事全是托儿

-揭秘求职"私人定制"骗局

今年以来,社会上出现一种以"试岗"为名的求职"杀猪盘"骗局。不法分子精准锁定求职人群,诱导求职者一步步落入转账陷阱,涉案金额从数百元到几十万元不等。

记者调查发现,这场骗局的特别之处在于, 不法分子精准锁定求职人群、冒用上市公司名义抛出 "试岗补贴"诱饵、伪造"官方文件"三重手段,层层突破求 职者心理防线。

对此,律师提醒,求职者务必警惕交费入职、 预存考核等偏离正常招聘流程的环节,一旦遇 到要求转账、下载陌生App等情况,应果断 拒绝并留存聊天记录、转账凭证等证 据;若确认被骗,需第一时间报警, 借助法律手段挽回损失。



近日,海外留学归来的应届毕业生王萍萍向记者还原受骗过程。某日,她收到一条陌生号码发来的短信,称其简历通过初步审核,希望进行后续沟通。"最近我的确在前程无忧平台上更新了自己的求职信息,虽然不记得是否给这家公司投过简历,但觉得不能错过就业机会,就回复了信息。"

很快,王萍萍收到邮件,附件是一份制作精美的 PPT,首页显示对方为半导体上市公司屹唐股份,内 页罗列着公司背景、拟聘岗位、薪资待遇、组织架构, 甚至绩效评估和入职流程都十分详细。

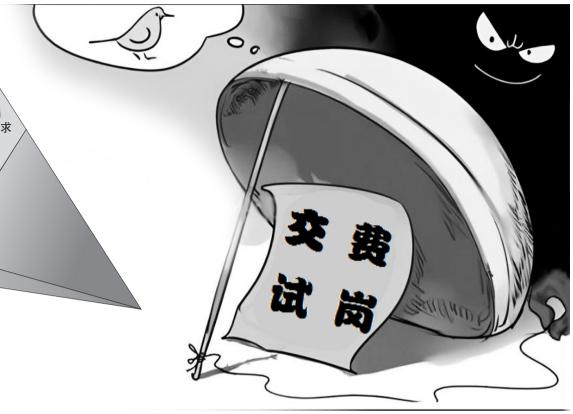
其中试岗安排部分提到:公司将按"政策要求" 提供线上培训,并同步发放薪资奖励,两日试岗综合 收入超过500元,全程只需手机操作,首日工作满3 小时即可,需通过一款名为"AI办公"的App开展。

起初,王萍萍抱着尝试的心态同意试岗,对方随即引导她下载指定App并加入所谓的内部工作群。王萍萍回忆说:"第一天任务很简单,在'考核专员'的指引下,完成资料录入、数据分析测试等工作。完成后绑定软件的银行卡顺利提现156元。"

随后,骗局逐渐升级,"考核专员"要求她完成一项数据分析测试工作,并提出需要个人出资进行数据分析测试,收益为30%。当王萍萍还在疑惑的时候,群里的"同事们"已经测试成功,并纷纷发出到账截图。为了顺利获得工作,她在支付宝转账100元,再返回对方提供的软件内提现,"确实在软件内提现130元,这让我的疑虑逐渐打消"。

第二轮任务里的转账金额开始逐渐变多,转账





200元之后,对方提出要用银行卡再次转账 5000元才能提现。再次转账后,对方立刻变脸,先是指责王萍萍"操作失误,需补款重测",紧接着又以"数据修复失败,无法提现"为由继续施压,甚至提出"需携带3万多元现金到指定地点,才能全额提现"。直到此时,王萍萍才幡然醒悟被骗了,"群里的'同事们'全是托儿"。

此类骗局并非个例,一位曾被骗数万元的网友 云舞,也在社交媒体上分享了受骗经历。该网友在 Boss 直聘平台更新简历求职。第一天试岗过程和王 萍萍类似。试岗次日,对方以"数据测试"为由安排工作,强调"测试内容保密,不可泄露",还发送了中国人民银行支付结算司的协议截图,声称"为了证明操作合规"。该网友特意到中国人民银行官网查询,发现截图与官网高度相似,这进一步加深了她的信任。后来该网友提出报警,便被对方直接"踢出"工作群,彻底切断了联系。

截至目前,已有多位受骗者公开分享了高度相似的经历。从披露的信息来看,被骗金额跨度较大,少则数百元,多则达几十万元;涉及的求职平台范围也较广,既包括前程无忧、智联招聘、Boss直聘等主流商业招聘平台,也涵盖了国聘这类国有引才就业服务平台。

三重手段精准突破信任防线

记者梳理发现,该骗局能够成功突破信任防线,核心在于不法分子精准运用"针对性推荐""冒充知名公司""伪造官方文件"三重手段,层层递进降低求职者警惕,最终实现诈骗目的。

第一重,实施"精准推荐",通过筛选目标人群并适配地域信息增强可信度。此类诈骗短信的目标受众呈现高度集中的特征:几乎均为求职者,其中又以应届毕业生及工作年限较短、初入社会的群体为主。

第二重,优先冒用上市公司、独角兽企业名义,降低求职者防备意识。据不完全统计,天地科技、弘元绿能、新华锦、碧水源、国联股份、亨通光电、易点天下、软通动力等多家上市公司均被不法分子冒名用于招聘诈骗。

骗局的猖獗已引发上市公司警惕,今年6月,上市公司利尔达便发布官方声明称,近期有不法分子冒用公司名义发布招聘信息,公司已第一时间向公安机关报案,并郑重提醒求职者,正规招聘绝不会以"预存资金"为条件,切勿轻信陌生链接、不明App及转账要求。

第三重,通过伪造官方文件与机构信息增加可信度。在诈骗过程中,不法分子不仅会在录用通知等文件上伪造招聘公司的公章,还会仿冒金融监管部门、银行等机构的信息,这些虚假的"官方信息",进一步消解了求职者的疑虑,使其更容易落人诈骗陷阱。

厘清平台责任边界

上述诈骗案有个共同的特点,受骗者都在不同的招聘平台提交了简历或求职信息。

"此类纠纷的核心在于厘清招聘平台的责任范畴与行为边界。"中国法学会消费者权益保护法研究会副秘书长陈音江说,若平台在未经求职者同意,将求职者个人信息出售,或者允许空壳公司通过付费方式,批量购买数百上千条符合特定条件的求职者个人信息,则该行为明确涉嫌违法以及侵犯求职者的个人信息权。

记者注意到,主流招聘平台已设置基础安全防线。在多个招聘App页面底部普遍标注安全提示,明确列出扣押证件、收取财物、诱导异地人职、违法使用简历等违规行为,提醒求职者可向平台举报。进一步点击后,还能看到"安全求职指南",不仅列举常见受骗场景,还通过互动测试帮助大学生识别风险。

尽管平台设有防线,但审核环节仍存在漏洞,部 分不法分子会通过非法途径获取企业盖章文件或营 业执照复印件,借此绕过审核注册账号,给虚假招聘 留下可乘之机。

知恒(上海)律师事务所刑事律师刘正要说,冒用上市公司公章的行为,可能构成刑法第280条规定的伪造公司印章罪。而诈骗过程中伪造国家监管机构官网、银行交易截图等手段,同样属于诈骗罪范畴。

谈及如何防范此类诈骗,陈音江认为,关键是要 压实平台的主体责任。一方面要强化平台对相关招 聘企业或个人的信息审核,确保相关信息的真实性, 切实采取措施确保求职者的个人信息安全,尤其是 未经求职者同意,不能擅自采集、使用或贩卖求职者 个人信息。

另一方面要积极运用大数据、人工智能等技术手段提升风险鉴别能力。比如,核验招聘企业是否具备相关经营资质,排查"无实体公司大规模招聘""招聘岗位与企业主营业务严重不匹配"等高风险情形。唯有将"技术筛查+人工复核"紧密结合,才能有效降低潜在风险,切实保障求职者的合法权益。

新华社北京9月18日电