◎制图 / 厉建红(豆包 AI)

一笔转账 牵出 两头风险

事主坚称未被骗,财务手机却已“失守”

商报济南消息 年关将至，各类企业、单位都在全力冲刺年度目标,而诈骗分子也趁机加紧“冲业绩”。他们瞄准年底资金周转、收支结算等关键环节,专门针对财务人员设计骗局。近日,济南市公安局市中分局四里村派出所办理的一起案件中,诈骗分子就利用技术手段短暂操控了公司财务人员的手机,企图“无声无息”转移资金。

近日，市中公安分局四里村派出所接到反诈中心资金预警：外地来济旅客成先生有向涉诈账户转账的记录，极有可能遭到诈骗。接到预警后,四里村派出所所长朱琳立即尝试与成先生取得联系，取得初步联系后,“成先生自称‘绝无可能’遭到诈骗,也拒绝了到所说明情况。”

“但为了成先生的财产安全,我们还是通过各种途径了解到他正在某酒店办理服务,遂立即前往该酒店与其见面。”据朱琳介绍,经过长时间沟通,成先生终于同意跟随民警到所配合梳理、核实情况,经核实,他的手机中确实没有来自陌生链接、涉诈软件等。

“但成先生有笔 6000 元的转账记录,他自称是向公司财务账户转的账。”为落实收款方身份信息，朱琳与成先生公司财务进行了视频通话,经核实,这笔转账财务确已收到,“但涉事财务反馈说刚刚手机有点‘不听使唤’，莫名弹出了需要输入支付密码的窗口,但还没来得及进行相关操作,就接到了警方的电话。”

“我们怀疑成先生公司财务的手机是被诈骗分子短暂控制了。”朱琳告诉山东商报·速豹新闻网记者,为了避免成先生及其公司、财务账户出现经济损失,他和四里村派出所辅警张凯分别结合真实案例，向本案涉事人员进行了反诈宣传，提醒他们及时修改银行账户密码并核实账户资金是否有变化,确保诈骗分子无可乘之机。

“年关将至,此类针对财务人员的诈骗近期案发率有增长的趋势。”朱琳提醒财务人员,若需进行转账,要在操作前进行线上线下结合的双核查;若收到陌生信息,切记“不点击、不填写、不转账”;发现有问题及时联系公安机关或拨打 96110 反诈专线说明情况。

（本文中所有当事人姓名为化名,为保护当事人隐私,部分信息已做模糊处理。）

◎山东商报·速豹新闻网
记者 李瑞琪 通讯员 丛琳 张大亿

四里村派出所所长朱琳

【 聚焦 】

@财务人员 这些诈骗近期高发,请注意防范

除了成先生遇到的这种诈骗,近期还有哪些类型的诈骗高发?财务人员在日常工作中应该如何预防?记者就此事联系到济南市公安局市中分局刑警大队反诈骗中心一级警长卢吉敏。

据她介绍,警方在近期工作中发现,济南已出现涉诈嫌疑人在税务所组建的财务人员工作群中植入木马程序,通过静默安装软件方式远控企业财务人员电脑的电信网络诈骗案件,“他们还会冒充企业领导或客户诈骗财务人员。”

记者了解到，诈骗分子常用的各类手段极具隐蔽性、潜伏性。在将木马静默安装至财务人员各类系统的过程中,诈骗分子通常会将木马病毒伪装成报税工具、办公软件、电子发票、涉税文件等,再通过发送短信、电子邮件或推送下载链接等方式,诱骗企业财务人员点击下载,实施木马攻击。

“电脑一旦被木马病毒入侵，诈骗分子就可以对电脑进行远程监控,进而长期潜伏,并通过办公文件、聊天记录等信息精准分析出企业基本情况和财务、管理、销售等人员信息,以及相关人员聊天习惯和企业财务审批流程。”卢吉敏告诉记者，诈骗分子能够在财务人员未发觉的情况下,远程控制其社交软件,将用于诈骗的账号添加至其好友列表。等到时机成熟后,再将诈骗账号伪装成该企业老板或客户的 QQ 、微信,编造多种理由要求财务等人员转账汇款。

“诈骗分子会利用此前掌握的人员信息和财务人员在职场中对权威的服从心理，伪装老板的说话方式或通过 AI 等技术手段合成虚拟语音、形象,制造‘时间紧迫’‘特事特办’的紧张氛围,并以‘手续后补’等话术阻断正常核实流程。”卢吉敏建议税务所及辖区企业,及时查杀工作群或电脑中有无被植入木马病毒、钓鱼软件。同时,积极主动完善财务制度,提升系统安全防护能力,切实消除风险隐患。

卢吉敏提醒财务人员，要严格遵守执行财务制度,切实提高防范意识,一旦发现伪装成好友的诈骗账号立即删除并更改聊天软件登录密码。如遇到企业领导、公司客户在聊天软件中要求转账汇款的，一定要当面或者电话核实,以免遭受财产损失。

“若确实不幸被骗,请完整保存相关资料,尽快报警并联系汇款银行,及时取消汇款或冻结有关款项,争取止损黄金时间,及时挽回损失或将损失减少到最低。”卢吉敏说道。