

“领导”让你帮忙转账?“李鬼”转向“精准施骗”

《半月谈》 鲁畅

从操着浓重口音的“猜猜我是谁”,到发送短信称“换号”顺带嘘寒问暖,再到“复刻”领导朋友圈添加好友……诈骗分子一边操着新话术、耍着新花招,一边通过非法渠道获取公民个人信息,实现从“广撒网”向“精准施骗”转向,有的案件有了AI深度伪装技术的加持,令人防不胜防。

面对此类“李鬼”冒充熟人骗局,一方面要持续加强打击和提醒防范,另一方面要努力铲除此类诈骗行为所依赖的土壤。



冒充熟人诈骗，涉案金额普遍较高

“我是XX(某领导),这是我的新号码,之前的已停用,请惠存!方便日后联系,收到回复!”不久前,北京市民李先生收到“领导”发来的短信,他不假思索地更新了通讯录信息,随后通过了“领导”发来的微信好友验证。

不久,“领导”以家里亲戚公司需要经费周转且自己身份不便为由,要求李先生先汇去一笔钱,自己同时将同等金额打到李先生账户上,并附上了一张银行转账截图。一想到“领导”有私事相求,而且只是“过一道手”的功夫,李先生不仅快速卸下防备,内心甚至还有点窃喜,马上操作完成了转账。

结果可想而知,李先生的钱转走了,“领导”的钱却迟迟没有到账,他这才意识到上当受骗:转账截图是合成的,再想联系却已经被微信拉黑,电话忙音……

这是一起典型的冒充熟人诈骗。“李鬼”领导胆大妄为,无孔不入。近期,从地

方政府、公安部门到中国航空工业集团、中国兵器工业集团等央企,都频发反诈提醒。

据记者了解,某些政府部门领导蒙受被“冒充”困扰,只得群发信息进行辟谣;从多地警方披露的案例来看,有当事人给“领导”转账近百万元;还有公司财务人员被“领导”要求给“客户”打款,诈骗金额高达数百万元。

北京市公安局朝阳分局反诈民警刘罡介绍,今年以来,朝阳分局反诈中心接到冒充熟人类警情300余起。与“刷单类”等诈骗相比,“冒充熟人”类诈骗涉案金额普遍较高,过程中骗子还会模仿领导口吻,使用“尽快”“马上”“你办事我放心”等命令、催促性词语,营造紧张气氛,并利用时间差降低当事人核实真伪的可能性。

“沉淀账号”实为骗子“马甲”

一些遭遇过冒充领导诈骗经历的当事人,心中不免充满疑问:骗子是怎么知道自己和“领导”有交集?

多位受访反诈民警结合办案经验表示,一种情况是当事人的身份信息、手机号和通讯录遭到泄露,通过黑灰产交易到了不法分子手中。在一些境外社交网站中,交换和买卖个人信息早已成为公开的秘密,不法人员对海量信息不断丰富、比对,从姓名手机号到购物记录、家庭住址,为“精准施骗”提供了更大可能性。

另一种情况是,受骗当事人社交软件中的某个好友被盗号,或是平时不注意而添加的陌生好友,实际上是骗子用来施骗伪装的“马甲”。例如,有的不法分子长期潜伏在微信好友列表中,伺机更改头像姓名,包装好自己的朋友圈,突然发来的信息让人第一时间难以识破。

在更为开放的社交软件中,骗子可钻的空子更多:在一起真实事件中,骗子关注到一位微博博主与好友互动频繁,便如同蚂蚁搬家一般将其好友发的微博内容接连复刻到自己的微博中,“更新”约一个月后,将头像改为对方好友头像,用户名加了个“”,然后通过私信方式向对方借钱。

冒充熟人诈骗成案时间有长有短,骗

子往往“见人下菜碟”,针对不同施骗对象,前期投入多少时间成本、计划骗多少钱,都可能经过筛选。

对此,部分社交平台加强了关注和打击。微信安全中心信息显示,今年初共针对3.5万多个确认存在欺诈行为的账号进行了阶梯式处理;对1万余个确认存在欺诈行为的微信群进行了限制群功能(封群)处理。

受骗者心态给了骗子可乘之机

北京中凯律师事务所律师厉彦杰认为,核实一个领导干部的身份并不难,可受骗人往往不去做这样的事情。在很多受骗者看来,质疑领导身份是件极其不尊重对方的行为,如果弄错了,还会有得罪领导的风险。正是这种想法,让那些行骗者畅通无阻,屡屡得手。

多地警方在“以案释骗”中都提到,在收到自称是单位领导或熟人发来的好友邀请时要提高警惕,不贸然添加对方微信,如对方提出金钱方面的往来要求,一定要通过见面、电话等多种方式进行核实,避免造成个人信息泄露及财产损失。同时,部分企业也应制定详细的财务审批规章制度,严密拨款流程,禁止利用社交软件下达拨款指令,并加强印章管理。

从更深一层看,不少人潜意识中有通过金钱往来等形式“和领导拉近关系”的心态,而这种心态恰恰给予骗子精准收割的可乘之机。厉彦杰认为,提升防范意识,前提是不能把与“领导”间非正常的金钱往来当作是工作中的一种考验,想象着帮了“领导”的忙,知道了“领导”的短,就成了“领导的自己人”。这种对于上下级、政商关系不正确的投机观念,最终变成真金白银的损失。

转发抽奖、“挂人”、盗图……警惕新技术为新型网暴推波助澜

《工人日报》 卢越

将辱骂他人的博文设置“转发抽奖”;“大V”私信被骂后“挂人”泄愤;朋友圈盗图冒充他人发送不良信息……

随着社交网络不断发展以及新技术的应用,新型网络暴力手段层出不穷。在冲破道德底线、破坏网络生态的同时,也给司法实践带来了新挑战。

网络暴力为何屡禁不绝?揪出幕后网暴者到底有多难?如何杜绝网暴让悲剧不再发生?8月3日,北京互联网法院通报涉网络暴力案件审理情况,并发布典型案例,呼吁社会各方共同参与网络暴力治理。

网暴形式不断花样翻新

人肉搜索、合成虚假照片、制作表情包、传播“AI换脸”视频……新型网络暴力形式不断花样翻新。北京互联网法院在审理中发现,为了扩大侵权范围,出现“抽奖转发”“0.01元链接挂人”等新侵权形式,助推侵权信息迅速广泛传播。

在一起典型案例中,李某通过社交平台发文辱骂赵某,并且对该博文内容设置“转发抽奖”。该条博文转发量超过4000次,评论数超过400条。博文发出后,赵某陆续收到网友私信,大多数内容带有攻击、谩骂的性质。法院判决李某通过涉案社交平台账号公开发布道歉信向赵某赔礼道

歉,赔偿精神损害抚慰金。

在另一案例中,“网络大V”被私信辱骂后选择“挂人”泄愤,受害者反变侵权者。刘某是一名微博粉丝数近50万的“大V”博主,另一微博用户孙某因某一时事问题与刘某观点不同,通过微博私信向刘某发送侮辱性言辞。刘某在微博上将孙某的私信、微博账号、照片等信息“挂”出来,并配有侮辱性言论,引发网友对孙某的网络暴力。法院判决刘某行为构成侵权。

值得关注的是,青少年易受误导加入网络暴力活动。在一些涉及社会热点的网暴案件中,部分青少年判断力相对不足,容易被舆论裹挟,参与到网暴活动中,甚至呈现出组织化参与网暴的新特征。在多起涉及明星的案件中,青少年通过微信、豆瓣等“饭圈”群,有组织地向他人发布攻击性言辞,引发网暴。

揪出幕后黑手有多难

网暴受害者往往维权漫长而艰难。维权困境之一,就在于取证难。

“有的权利人直接对网络账号个人信息页面备注的主体进行起诉,不能充分举证证明侵权主体身份。”北京互联网法院副院长赵瑞罡介绍,有的对网络侵权行为的取证不完整或未能及时存证,有的未能第一时间根据平台规则发送有效通知,而是

使用私信平台助手联系官方账号、@平台官方账号等无效通知方式,未能及时阻止侵权损害范围进一步扩大。

“如果侵权者是以匿名的方式发表侵权言论的,可以和平台方协商要求提供侵权者的身份信息。”北京互联网法院综合审判三庭庭长孙铭溪建议,为避免恶意言论继续发酵,受害者可以尽快向网络平台提供初步侵权证据并要求该平台立即采取删除、屏蔽、断开链接等必要措施。

在司法审判中同样面临难题。“侵权主体难以直接锁定、侵权行为复杂多样和侵害后果难以量化是此类案件审理的主要难点。”赵瑞罡说。

由于网络平台往往不会直接提供涉嫌侵权网络用户的实名信息,受害者只能通过诉讼方式申请法院调取信息。然而,北京互联网法院在案件审理中发现,部分平台无法及时、准确、完整披露用户信息,甚至拒绝提供用户信息。

此外,侵权行为复杂多样,加大了司法认定难度。比如,有的是直接复制、转发他人侵权言论,有的是以评论、回复、留言、点赞、发布弹幕等方式发布侵权言论,有的是直接采用截图等手段跨平台传播,有的是收集多人发布的侵权信息后再次整合发布原创……哪些构成侵权?承担何种责任?这些都成为司法实践中面临的问题。

对网暴始终坚持“零容忍”

对于网络暴力,我国始终坚持“零容忍”。中央网信办于2022年11月印发通知,要求加大网暴治理力度,进一步压实网络平台主体责任。今年6月,最高人民法院、最高人民检察院、公安部发布《关于依法惩治网络暴力违法犯罪的指导意见(征求意见稿)》,提出依法严惩网络暴力违法犯罪。

“平台作为网络服务提供者,在网暴问题治理方面负有相应主体责任,包括对网络账号的管理责任、对网络用户发布信息的管理责任、对网络安全的保障义务等。”赵瑞罡说,“部分平台仍存在审核不严、治理不力的情况。”

北京互联网法院在审理中发现,部分平台对受害者侵权删除通知未及时采取合理措施进行处理,直至诉讼权利人起诉至法院才处理,使得侵权后果进一步扩大。

在涉网暴案件审理过程中,既要维护被侵权人合法权益,也要依法保障公民网络言论自由,二者应如何平衡?

“对于网络用户通过信息网络检举、揭发他人犯罪或者违法违纪行为,只要不是故意捏造事实或者明知是捏造的事实而故意散布的,不应当认定为诽谤侵权。”赵瑞罡介绍,“针对他人言行发表评论、提出批评,即使观点有所偏颇、言论有所激烈,只要不是肆意谩骂、恶意诋毁,不宜认定为侮辱侵权。”