

# 大学生涉电信网络诈骗案件预防研究

王静雯 薛昕怡 夏盈

(南京审计大学 江苏 南京 211815)

**【摘要】**近年来,电信网络诈骗犯罪频发,犯罪形势日趋严峻复杂,其中发生在高校里的电信网络诈骗犯罪占80%。电信网络诈骗犯罪中的大学生群体,分别以受害者和犯罪者的角色存在,本文通过研究该群体的基本特征,梳理了大学生成为受害者和犯罪者的共性原因和特性原因,从国家、社会、个人三个方面提出预防措施建议。

**【关键词】**电信网络诈骗犯罪;大学生群体;原因;应对措施

**【基金项目】**本文系江苏省大学生创新创业训练计划资助“大学生涉电信网络诈骗犯罪预防研究——以南京高校大学生提供身份证案为例”(编号:202211287068Y)的研究成果。

**【作者简介】**王静雯(2001.10-)女,汉族,江苏南通人,本科在读,研究方向:刑法。

薛昕怡(2002.6-)女,汉族,河南南阳人,本科在读,研究方向:刑法。

夏盈(2002.2-)女,汉族,江苏泰州人,本科在读,研究方向:刑法。

**【中图分类号】**D92 **【文献标识码】**A **【文章编号】**1671-0633(2023)04-00061-03

随着电信网络发展,电信网络诈骗案件呈现高发趋势,诈骗手段不断翻新。网络的不安全性使犯罪分子轻松获取信息诈骗钱财;网站域名隐藏技术等让钓鱼、诈骗网站更加逼真;再加上电话号码修改器、自动短信等工具,几乎使诈骗者无所不能。此类犯罪已经严重危害人民群众财产安全,造成财产损失数额巨大,引发了社会巨大的舆情愤怒和关注,如何防范大学生被电信诈骗是急需解决的问题。本文通过对大学生涉电信网络诈骗犯罪的原因剖析,提出相应的犯罪预防对策,有助于减少电信网络诈骗犯罪,对大学生起到双向保护作用。

## 一、大学生涉电信网络诈骗现状

国家反诈中心公布数据显示,2021年电信网络诈骗的受害者中,18岁以下占比2%;18至35岁占比65.5%;36至59岁占比31.3%;60岁及以上占比1.4%。同时,电信网络诈骗犯罪占高校刑事犯罪的80%<sup>[1]</sup>,这些数据足以表明大学生已经成为电信诈骗最主要的受害者。

当下较典型的电信网络诈骗方式包括:刷单类,贷款、代办信用卡类,杀猪盘,冒充网购客服类,冒充“公检法”、领导、熟人,虚拟购物服务、投资理财类,虚拟博彩类,游戏装备虚拟交易类以及其他类型<sup>[2]</sup>。在诸多的诈骗类型中,刷单占比最高,其次是贷款和代办信用卡类。很多的学生因为校园贷遭受了严重心理伤害,也有人误入歧途,参与犯罪活动,甚至锒铛入狱,针对大学生电信网络诈骗犯罪主体的特殊性提出实践性的应对策略已成为亟待解决的问题。

本文结合大学生作为电信诈骗受害者与犯罪者的相关调查数据及案例,对大学生涉电信网络诈骗进行了原因分析,并提出了相应的预防措施。

## 二、大学生涉电信网络诈骗的原因分析

作为电信网络诈骗对象重灾区,大学生群体在电信网络诈骗犯罪中无论是作为受害者还是参与者,两者身份涉电信诈骗的原因都存在共性和各自的特性。

(一)大学生作为电信网络诈骗被害者或参与者的共性原因分析

### 1. 社会经验不足,缺乏成熟的判断能力

结合线上问卷与线下调查发现,80.81%的同学认为大学生易受电信诈骗的原因在于防范意识差。随着网络发展,诈骗套路也越来越多元化,常见套路如扫码献爱心、街头才艺扫码等利用大学生的善良与同情心进行诈骗。

### 2. 活动范围广,接触领域丰富

大学生正处于精力旺盛的阶段,特别是单身的大学生在课余时间安排上,倾向于网络聊天消遣,助长了诸如“杀猪盘”“裸聊”等骗局的嚣张气焰。一些为了满足人们日常交友需求的软件在繁忙而缺乏情感宣泄方式的生活中应运而生,出发点是消遣、娱乐,却被不法分子钻了空子,利用大学生情感空虚的特点,通过这些软件与之建立虚拟的亲密关系,套取个人信息进行诈骗。

(二)大学生作为电信网络诈骗受害者的特殊性原因分析

### 1. 大学生上网目的多样化

经线下调查,在校大学生使用手机上网主要用于交友、学习、娱乐、休闲和购物,享受网络功能的同时却也承受了潜在危机。网络门槛低促成了危险信息泛滥,大量网页存在安全隐患,而很多学生都或多或少存在不规范使用网络的情况,例如浏览不法网站,为电信诈骗提供了机会。

## 2. 大学生个人信息泄露严重

信息泄露是犯罪分子进行电信诈骗的上游犯罪，针对个人信息的犯罪已形成一条灰色产业链，预防电信诈骗，必然从源头管理信息泄露问题，前提是了解信息泄露的原因。依照《个人信息保护法》等法律规定，“规范个人信息处理，加强个人信息保护，建立个人信息被用于电信诈骗的防范机制”，而部分个人信息处理者未尽到信息保护义务。据调查，大学生信息泄露的常见途径有高校因集体活动收集“学生个人信息”文档，教学服务平台中个人信息采集等，信息采集人员将收集的学生信息出卖给不法分子，不法分子通过这些信息对大学生实施精准诈骗，大大提高了诈骗成功率。

## 3. 相关部门在电信诈骗防治中监管和宣传不到位

虽然《中华人民共和国反电信网络诈骗法》规定各部门、单位在反电信网络诈骗工作中应当密切协作、协同配合，但在实践中却存在各部门配合不协调、执法进度缓慢等问题。同时，维权流程的繁琐与拖沓以及可能存在推诿责任的情况让受害者即使及时报案也不能得到尽快处理，使其难以维权，更让社会寒心，更多受害者选择干脆不报案。

其次，目前的宣传只停留在表面，分享电信诈骗的真实案例，对于新型电信诈骗类型、遇到电信诈骗后如何维权等宣传还不到位。另外，《反电信网络诈骗法》中提到对举报电信诈骗的人提供奖励和保护，但相关制度并不完善，实践中也很少有因举报而获得奖励的案例。

## (三) 大学生作为电信网络诈骗犯罪参与者的特殊原因分析

帮助信息网络犯罪活动罪，是2015年《刑法修正案(九)》增设的三个新型网络犯罪之一：“明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持……”2022年1月至6月全国检察机关起诉帮助信息网络犯罪活动罪的人员中，30岁以下的占64.8%，18至22岁的占23.7%，<sup>[9]</sup>其中许多是在校大学生。非法买卖“银行卡、手机卡”是最常见的帮信罪类型，因为来钱快、回报高，大学生往往会作出出租、出售银行卡，帮助犯罪团伙实施买卖电话卡等违法行为，成为帮助信息网络犯罪活动罪或者有关犯罪的共犯。

作为电信网络诈骗犯罪参与人的大学生群体与作为受害者相比，消费欲望强，攀比心重，却苦于无经济来源，易被所谓的“低成本、高收入”的非法交易“两卡”行为所诱惑。由于缺乏法律意识，他们可能对自己的行为存在误解，认为仅出租、出售自己的银行卡、手机卡不构成犯罪。不少大学生在犯罪过程尝到甜头，被犯罪团伙利用，诱骗其他同学出

租出售两卡。

## 三、大学生涉电信网络诈骗的预防措施

基于以上对大学生涉电信网络诈骗原因的共性与特性分析，可以将其归为三个层面的缺陷：国家、社会和个人，对此本文提出相应预防措施：

### (一) 国家层面

近年来，电信网络诈骗随着数字化时代的发展而兴盛，而国家对电信诈骗的管控措施尚未及时更新，对此，本文从立法、司法两方面提出建议。

#### 1. 完善相关立法

个人信息泄露往往是电信网络诈骗的源头，然而现有的法律规范不足以对侵犯个人信息的行为进行充分评价。本文认为，可以通过加强刑法与个人信息保护法的衔接来有效打击侵犯个人信息的行为，如《个人信息保护法》已经明确了对已公开信息的不当处理可能构成侵犯个人信息的行政违法行为，因此刑法可对此侵权行为积极介入，做出规制。

其次，从现有诈骗罪所保护的法益来说，<sup>[4]</sup>诈骗罪注重保护单一的财产法益，无法评价电信诈骗对其他价值的侵害。在数字化的时代，电信诈骗的危害不仅体现在财产损失上，还对人们的生活造成了大量负面影响，如社会信任度下降，数字化交往成本提高等，这些都是诈骗罪未能评价到的价值。同时，在单一财产法益的影响下，电信网络诈骗的不同行为方式所导致的除财产损失之外的不同附带危害结果，可能会因为数额相同而得出相似的量刑结论，从而导致电信网络诈骗中侵犯的其他需要刑法额外评价的行为方式被数额掩盖。在数字化浪潮的推进下，诈骗罪以财产法益为核心的单一评价思路难以与时代发展相匹配，不能有效充分地评价电信网络诈骗，既无法为其从重处罚提供合理依据，<sup>[5]</sup>又难以分别评价及处罚不同种类的电信网络诈骗。

从诈骗罪情节标准的适用门槛来说，诈骗罪既有的情节标准或许存在适用门槛过高的问题，使得电信网络诈骗的处理与犯罪事实存在不相称的情况。随着个人信息泄露的情况越来越严重，电信网络诈骗日趋精准化。然而除《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(二)》外，《诈骗罪解释》对于情节标准的设置都针对于广撒网式的电信网络诈骗。然而，实际上，精准针对少数人的诈骗信息可能与地毯式发给大多数人的钓鱼诈骗信息具有同样大的危害结果。如果仍采用较高的标准，会导致精准诈骗造成的危害与其对应的情节标准不相称，成为打击电信网络诈骗的一大漏洞。因此，国家可增设有关电信网络诈骗专门法律，整合、重建被电信网络诈骗破坏的数字化生活秩序与交往准则，

彰显刑法基于数字正义的价值导向和人文关怀。

## 2. 改进司法活动

与一般犯罪相比,电信网络诈骗有分工明确、作案手段高端多样、涉及区域广泛等特点,因此在司法实践中对整个犯罪行为进行准确认定存在一定困难,且常出现管辖机关之间争权或互相推诿的问题。

打击电信诈骗犯罪,公检法三机关不可各自为营,而应以捍卫公民的生命财产为目标,相互配合与监督。大数据时代下的电信诈骗让侦查机关在证据收集、案情调查、锁定嫌疑人等方面面临技术上的挑战,是以,侦查机关需引进更多技术型人才,学习新技术。检察机关也应顺势而为,调查手段及时更新换代,适时介入,监督和引导侦查机关调查取证。同时,法院工作人员要注意关注数字化时代下的法律变迁,更新旧理念,吸收新知识,严厉打击电信网络诈骗活动。

管辖冲突分为境内跨区域管辖权冲突和境外管辖权冲突。关于境内跨区域管辖权冲突,我国刑诉规定,确定管辖法院应以犯罪地为主。然而,在电信诈骗案件中,司法机关可以积极突破该限制,按有利于查清事实原则来确定司法机关。同时,要想打击跨区域电信网络诈骗,各区域之间司法机关的协助尤为重要,要建立高效便捷的跨区域整体治理机制,加大各地司法机关合作的深度,简化程序,提高合作效率。而对于跨境管辖权冲突,要加快建立国家之间共同打击电信网络诈骗的合作关系,健全司法机关合作交流机制,以更务实的态度持续有效地共同打击跨境电信网络诈骗。

## (二)社会层面

社会层面又分为社会组织和高校,二者在预防电信网络诈骗问题上既要分工明确也要通力协作。

关于社会组织,本文主要强调金融机构和电信网络经营者的主体责任。在诈骗活动中,转账是一个关键行为,如果加强对犯罪者银行账户的控制,就能有效识别异常账户,即使被害人转账之后也可以及时冻结账户,最大程度减少被害人损失。根据银监会发布的文件,各金融机构须严格落实银行卡开户实名制的要求,加大对银行账户的监督力度,必要时及时冻结实施电信网络诈骗者的账户。电信业务经营者、互联网服务提供者等社会组织要积极承担风险防控责任,研究预防电信网络诈骗的技术手段,如建立信息泄露防范机制,检测识别涉诈信息并及时预警等。

高校应与当地公安、网信部门联合起来,共同预防和打击针对于大学生的电信网络诈骗。一方面对高校出现的有诈骗嫌疑的不良信号进行监测,早发现,早阻断,将危险扼杀在源头;另一方面定期净化高校网络环境,整改不良网站。

此外,校内面向学生的反诈教育必不可少。一是定期进行宣传,通过转发近期电信网络诈骗案件等方式,让同学们了解到电信网络诈骗就在身边,提高防范意识。二是注重理论教育,可通过开展讲座让同学们熟悉电信网络诈骗典型套路,识别预警信号,了解参与电信网络诈骗应承担的法律后果。

最后,高校应当完善电信网络诈骗应对机制,鼓励学生遭骗后及时寻求学校帮助,学校也能迅速反应,最大程度地减少损失。

## (三)个人层面

首先,大学生要增强法律意识。在校大学生要学习基本的法律常识,特别是针对大学生群体高发的犯罪,积极参加学校组织的安全教育活动,了解这些犯罪的典型套路,避免上当。同时,增强法律意识能够帮助同学们有效辨别非法行为,避免沦为不法分子的“作案工具”。

其次,大学生要注重保护个人隐私,个人信息的泄露往往是遭遇电信网络诈骗的开端,在涉及个人信息的问题上敲响警钟。在浏览网页和下载程序时应注意从正规渠道获取,不可随意相信来历不明的电话。一旦上当受骗,立即向公安机关报案,并详细描述被诈骗的过程,以及有关嫌疑人身份、住址等线索,积极配合公安机关开展侦查活动。

最后,大学生必须明确道德底线,在诱惑面前坚持底线。作为新时代的接班人,大学生更要端正脚踏实地做事的生活态度,当务实成为一种生活习惯时,就不会在无端出现的蝇头小利上或是诱惑巨大的“馅饼”面前犹豫不决。

## 参考文献

- [1] 颜志宏,陈远爱,刘诗艺.大学生被电信网络诈骗类型、原因以及对策研究[J].法制博览,2021,No.847(23):129-130.
- [2] 杨润泽,赵泓彰,王琮等.电信诈骗对大学生的危害与防范措施[J].法制博览,2022,No.889(29):14-17.
- [3] 数据来源:最高人民检察院网上发布厅,2022-07-21,[https://www.spp.gov.cn/xwfbh/wsfbt/202207/t20220722\\_566409.shtml#1](https://www.spp.gov.cn/xwfbh/wsfbt/202207/t20220722_566409.shtml#1)
- [4] 张明楷:《刑法学》(第6版),法律出版社2021年版,第1303页。
- [5] 叶良芳.犯罪场理论视角下电信网络诈骗犯罪的治理对策[J].犯罪研究,2021,No.249(06):2-10.