

注册校园交友软件后骚扰电话频繁 学生个人信息成为黑灰产交易筹码

近期,四川、山西等地公安机关接连破获非法倒卖学生个人信息大案:校园“内鬼”违规导出数据,运维人员“监守自盗”,中介层层加价转卖,非法倒卖学生个人信息的黑灰产业链条浮出水面。与此同时,记者对多款校园交友软件开展实名注册实测,采用专属姓氏溯源方式排查泄露源头,注册后很快便接到众多信贷、兼职类骚扰来电。

学生个人信息究竟如何从校园、平台、机构流出,又怎样在黑灰产业链条中被层层倒卖?记者对此展开了采访。



(漫画来源:法治日报)

骚扰电话接踵而至

多名受访学生表示,他们日常会高频使用多款校园墙、校园社交、学生专属交友软件。这类平台主打校园交友、同城互助、校园树洞等功能,深受学生群体青睐。为测试平台信息安全程度,记者对多款热门校园交友软件进行实名注册体验;在注册不同软件时,记者特意预留了区分度不同的专属姓氏信息,以此排查信息泄露渠道,排除其他干扰因素。

注册完成后短短几天时间,记者的手机便频繁接到陌生人的来电骚扰,类型高度集中,主要分为两类:

一类是信贷推销电话,来电人员话术统一,反复询问是否有资金需求,主动推销各类贷款业务,声称“征信不好、没

有信用记录,也可以办理贷款”。另一类是兼职招募骚扰电话,对方频繁推送各类陌生兼职岗位,不间断询问是否需要兼职工作。

多名来自不同高校的大学生同样遭遇过个人信息泄露带来的困扰。

北京某高校新闻与传播专业的蒋同学在某平台为领取考研备考资料填写了自己的手机号码。提交表单后,骚扰电话数量明显增多,某平台工作人员反复向她推销考研培训班。她联系客服要求停止致电但并未起效,直到她明确告知将发起投诉,骚扰来电才最终停止。

另一所高校金融学专业的研一新生张同学每隔半个月左

右就会接到一通骚扰电话。他曾浏览过健身相关内容,此后健身房推销电话接踵而至。“有可能是平台采集了我的浏览行为数据,将健身需求标签连同联系方式一并给到商家。”张同学说,“现在不少小程序、App都需要手机号码授权,很难确认到底是哪一次操作造成的信息泄露。”

近期正在求职的某高校大四学生刘同学每隔三四天就会接到一通骚扰电话,部分来电者甚至能够精准报出他的姓名、学校、年龄。信息泄露的线索指向一次线下面试:他在现场如实填写纸质个人信息登记表,面试结束之后,大量打着“包就业”旗号的技能培训推销电话持续了半个月。

合力构建治理闭环

学生个人信息泄露频发,治理路径何在?受访专家从制度建设、部门协同等多个维度提出建议。

张继红认为,亟须构建全流程闭环治理体系。一是落实备案准入机制,全面推行教育类App备案管理制度,未经备案或备案不通过的App严禁在校园场景使用,并进一步细化教育场景类“必要个人信息清单”,将学校、平台、运维服务商、教培机构等主体纳入清单规制范围。二是健全常态化合规审计机制,将外包运维等关联服务环节全面纳入合规审计范围。三是强化专项监管抽查与多方共治,严格落实个人信息保护责任人制度,同时联动检察公益诉讼制度,整合学校管理、家长监督等社会力量,构建多元共治格局。

在制度长远完善层面,受访专家提到,现有个人信息保护框架仍有优化空间,可进一步优化告知授权机制,针对不同年龄段学生建立差异化保护规则,强化未成年人群体权益倾斜保护。

受访专家一致认为,学生个人信息泄露的治理,是一项从源头收集到末端使用的系统工程。只有压实学校、培训机构、互联网平台等主体责任,公安机关全链条打击泄密“内鬼”与倒卖信息的中间商,多部门协同斩断整条黑灰产业链条,才能守护青少年群体的个人信息安全。

(法治日报)

案件揭开信息黑市

学生个人信息泄露并非个案。记者梳理公开报道发现,近年来多起特大侵犯公民个人信息案件被破获,其共同特征是:泄露源头往往是机构内部人员利用职务便利“监守自盗”。

学生个人信息为何成为黑灰产的“香饽饽”?互联网法治研究院(杭州)特邀研究员张继红分析,学生个人信息完整度高且商业价值大,通常涵盖姓名、性别、身份证号码、户籍、学籍、就读学校和班级、监护人联系方式、家庭住址等多维度内容,数据完整性与准确度远优于普通用户信息,能够精准匹配各类营

销需求。

“同时,学校缺乏专业化数据安全保障能力。学校的核心职能为教育教学,并非专业化的数据处理和管理机构,普遍存在信息安全保障体系缺位问题。部分高校未设置专职个人信息安全管理,中小学的信息安全配置更为薄弱;部分学校未常态化投入校园网络运维、数据安全防护等专项经费,缺乏完善的信息存储、权限管理、风险防控机制,导致学生个人信息在存储、传输等环节存在安全风险,极易被非法窃取、泄露和滥用。”张继红说,“此外,学生个人信息泄露具有隐

蔽性、滞后性等特点,侵权行为难以被及时发现;普通学生与监护人普遍缺乏溯源、取证的技术能力,无法精准定位信息泄露环节、固定侵权证据。”

北京嘉润律师事务所律师高攀告诉记者,学生个人信息贩卖的违法犯罪链条可以分为前、中、后三个环节:在前端,学校、培训机构过度收集学生和家信息,内部工作人员监守自盗是泄露的重要诱因;在中端,信息被汇总、加工后,在相关平台中传播、售卖;在后端,培训机构、招生中介乃至诈骗团伙利用这些信息进行精准营销或实施电信网络诈骗。



本报刊载的所有内容(包括但不限于文字、图片、绘图表格、版面设计),未经本报授权和许可,任何单位和个人不得转载、摘编或以其他方式任何形式使用。违反上述声明者,本报将依法追究其相关法律责任。

如需使用本报自有版权作品,须与本报协商合作并事先取得书面授权和许可。法务及版权合作:

联系电话:0510-88300000