

医学高职高专院校学生个人信息安全保护意识现状调查及对策探讨

王欢 李潇潇 (通讯作者)

(四川中医药高等专科学校 四川 绵阳 621000)

[摘要]互联网的迅速发展在为人们提供便利的同时,也伴随着因个人信息泄露而带来的后续风险。本文主要通过对该医学高职高专院校学生个人信息安全保护意识及可能泄露信息的日常习惯现状的调查,分析造成目前形势的原因,并探讨解决问题的对策,以期对高校学生信息安全的教育开展提供理论依据。

[关键词]学生;个人信息安全;原因;对策

[DOI] 10.12525/j.issn.2096-6288.2020.07.791

随着大数据时代的来临,我国互联网+发展迅速,我们一边享受着网络带给生活的巨大便利,一边也承受着诸多潜在的风险,其中个人信息的泄露是目前面临的严峻问题之一。自全国信息安全标准化技术委员会于2017年12月29日正式发布《信息安全技术个人信息安全规范》以来,民众对个人信息安全的保护意识有所提高,但是作为网民主力军的大学生^[1],由于其涉世未深,对外界信息真实性的判断力较弱,个人信息安全保护的意识不强,加之遇事后的怕事心理等,致使由个人信息泄露后导致的不安全事件时有发生。本文以某医学高职高专院校为例,调查学生的个人信息安全保护意识现状以及遇到过的问题,探讨提升个人信息安全保护的对策。

一、学生个人信息安全保护意识现状调查

(一) 调查目的

通过问卷调查掌握医学高职高专院校学生个人信息安全保护意识的现状,了解可能泄露个人信息的日常习惯及为保护信息所做的措施,以便为下一步加强个人信息安全保护工作的开展,提供理论依据。

(二) 调查对象

随机抽取某医学专科学校400名高职高专学生为调查对象。

(三) 问卷设计

研究者查阅相关文献后自行设计学生个人信息安全现状调查问卷,主要分学生基本情况、日常信息泄露的现象及个人习惯、个人信息安全保护的态度及意识自评、对保护信息安全的主动行为和措施建议四部分内容,共18道客观题,问卷最后一题添加主观选项,为征求学生对问卷上未提及的保护信息安全的措施做补充。

(四) 问卷实施

本次调查发放问卷共400份,回收问卷354份,剔除无效问卷21份,回收有效问卷334份,有效回收率为83.5%。

调查内容		人数	占比(%)
学生性别	男	88	26.35
	女	246	73.65
学生年龄	18岁以下	14	4.19
	18-20岁	242	72.46
	21岁以上	77	23.35

表1 学生基本情况表

(五) 调查结果

1. 学生基本情况

由表1可以看出,学生性别组成中,女性同学比例多,占73.65%,男性同学占比26.35%,这主要与医学院校性质和社会现状有关。在填报志愿时,教师和医护人员是最受

女性学生家长喜爱的专业。此外,由于为高职高专类医学院校,学生年龄多为18-20岁,占比为72.46%,这与学校生源对象性质相符。

2. 学生个人信息泄露的现象及日常行为

2.1 学生所遭遇日常信息泄露的现象

问卷数据显示,有93.11%的学生接/收过诈骗/推销电话或垃圾短信,其中更有17.96%的学生接/收频率为经常。此外,有近70%的学生有过被个性化推送的经历,说明信息泄露现象在学生中十分普遍。

2.2 学生与个人信息泄露有关的日常行为

问卷调查显示,学生与个人信息泄露有关的日常行为中,各类账号使用相同或相似的名称占比最高为80.54%;参与一些需要个人信息的活动和下载应用程序时不查看服务协议分别位居第二、三位。而直接需要信息的行为,如网络要求直接填写个人信息、下载APP时需要全部开启权限,在学生中占比不高,分别为12.57%和19.46%。这主要与学生对个人信息泄露危险的认识不全面有关系,学生只对直接索取个人信息的行为有提防,但对隐藏起来的索取个人信息行为难以识别,提示我们在不易被学生察觉的个人信息泄露行为上需要加大宣传力度。此外不主动对可能诈骗信息/电话进行举报/分类标记、点击各类软件发来的链接的行为也在学生中占半数,这会无形间增加他人识别风险的精力和成本,不利于个人安全信息的全面防护。

3. 学生对个人信息安全意识自评和对可能泄露个人信息安全的态度

3.1 学生对个人信息安全意识自评

调查数据显示,大部分学生自觉对信息安全保护的知识掌握尚可,仅3.29%的学生觉得基本不懂,但依据上文分析,学生只对直接泄露信息的方式有所警觉,对隐藏型意识不到位。在对个人信息透明度的认识上,小部分学生(20.36%)持乐观态度,认为完全安全;而有10.48%的学生认为个人信息持悲观态度,认为已完全透明;另大部分学生(69.16%)认为信息部分泄露。此外,有半数学生(52.69%)曾向长辈普及过个人信息安全防护知识,说明学生对个人信息安全的关注度尚可。

3.2 学生对可能泄露个人信息安全的态度

在调查数据中,绝大多数学生非常介意隐私被泄露(92.51%),但仍然有不介意者,说明对个人信息安全意识的普及仍有死角。另外,在面对网络上流传的“对手机说出关键字,即可得到相关推送”的现象,有56.59%的学生认为可能会涉及隐私暴露,持反对态度;有31.14%的学生认为无影响,不以为意;另有12.28%的学生认为对生活有帮助而赞同。这提示在新事物应用前,需要保证用户信息安全,以

利于产品的推广。

4. 学生对保护信息安全的主动行为和措施建议

调查数据显示,如图6,在学生中对保护信息安全的主动行为中,销毁快递包装上个人信息占比85.33%,这说明除了说明学生具有保护个人信息的意识外,还从侧面反映了电商时代的繁荣发展现状。另外,有半数学生会关闭手机位置信息、编写复杂密码/定期修改密码和撕毁火车票后车票二维码。还有一部分学生会提供假的个人信息(35.63%)。这都说明学生有一定的保护个人信息泄露的行为和能力。

二、现状分析

(一) 学生个人原因

“00后”出生和生长在网络技术已经十分发达的时期,学生或多或少都与网络有接触,现在的互联网+时代更是迅猛发展,各种新技术与新鲜事物层出不穷,app、二维码、网购等在学生中十分普遍,随之而来的网络诈骗/犯罪也成倍增长。但是随着国家对违法犯罪行为的打击和宣传,学生均有一定的个人防护意识。但由于是医学类高职高专学校,绝大多数学生对计算机网络可获取的个人信息途径并不了解,这就出现了学生一方面十分介意信息泄露,但另一方面却只能对直接索取个人信息的手段会有防备,而对隐藏型能获取到信息的手段不防备或防备意识较差。此外,有一些学生不介意个人信息被泄露,可能因为没有产生过大型的财物损失,或存在侥幸心理^[2],这都说明学生意识较差。

(二) 学校原因

据笔者了解,就该调查学校而言,在每年新生开学季,特别是学生尚未到校时,都会有学生因各种形式被骗,这说明学生的个人信息有不同程度的泄露。而信息泄露会增加学生受骗的风险,犯罪分子通过被泄露的个人信息,联系学生,撒网式实施诈骗,轻则导致学生财物损失,严重者导致学生生命受到威胁。虽然该校为防止出现类似事件,从多方面进行了宣传教育工作,包括但不限于尽早联系学生加入班级群,集中管理学生,宣传防骗攻略等,但仍然不能完全避免学生受骗的发生,这提示我们从学校角度需要寻找更易被学生接收、覆盖面更全面的宣传突破口。

(三) 社会原因

近些年,随着网络技术的迅速发展,个人信息泄露引起的违法犯罪事件迅速增长。虽然国家对网络犯罪的打击力度加大,陆续出台了一些法律法规来防治利用个人信息的网络犯罪,但是仍然有犯罪分子顶风作案,这主要由于网络犯罪门槛和成本低、犯罪行为不受时间和空间的限制、犯罪分子的组织化、以及犯罪造成的损失难以追回等原因引起^[3]。此外,有许多个人或线下平台利用“邀请亲友返现”“注册抽奖”“扫码免费送礼物”“完善信息送会员”等方式窃取个人信息,这部分由于缺乏预见性和散在存在而难以得到管控。另外,虽然国家或当地政府做了一些保护个人信息的宣传,但多利用公益广告或宣传海报等方式进行普及,对实物信息来源相对闭塞的学生来说,效果不佳。

三、研究对策

(一) 学生要加强个人信息保护意识,提升个人安全素养

作为学生个体,首先需要认识到个人信息可能从哪些途径被泄露,只有清楚哪些途径会泄露信息,才能从源头杜绝这些泄露信息的行为,学生可以从学校宣传和网络查阅中明确该途径。其次,要充分认识到信息泄露后可能会导致哪些严重损失,只有对信息泄露后可能带来的危害足够重视,才能从内心萌生加强个人信息保护的意识,这可以从社会事件的反思中得到培养。再次,学生需要杜绝侥幸心理,不要认为某某简单的贪图便宜(如:拼单、扫码免费送)不会让自己成为信息泄露新闻和报道里的主角,甚至有些认识到了风险的存在,也觉得后果微不足道,自己完全有能力应付可能发生的危险,而不重视信息的保护,这都需要从根本意识上培养安全素养。最后,若是真正遇到了人身财产损失,需要第一时间报警,并联系学校、家长,以期将损失降低到最低,万不可自己强撑。

(二) 学校要加大宣传力度,做好个人信息安全教育工作

作为学校,有育人的本职工作,特别作为学生与进入社会的最后一道围墙,安全教育工作需要与授业一样得到重视。首先,学校可以增设与个人信息安全相关学科,将学生个人信息安全教育课程纳入培养方案中,从学科建设上直接加强学生安全素养。其次,强化与学生接触较多的教师、辅导员意识培养,通过提升“管理者”信息安全意识,达到事半功倍的效果。再次,学校可丰富教育形式,创新宣传方式,目前个人信息安全教育多局限于班团组织活动上,出现了仅参与/分享者意识较高,但未直接参与者无显著提升的现象,可以以全校有奖竞赛/趣味活动的形式提升学生的安全素养。最后,学校需紧跟时代步伐,多关注新型窃取个人信息的案例,定期将其传达给学生,对易上当受骗的学生保持关注度,鼓励学生在面对危险时选择用法律的武器保护自己。

(三) 社会共同参与监管维护,创建个人信息安全新环境

作为个人信息安全维护的武器——法律的制定与颁布者——政府,除了需要加强网络安全外,还可以联合社会力量,举办各类主题活动,例如:宣传深入社区,从家庭方向让学生提升安全素养。而作为社会现象的报导宣传者——媒体,可以增加与个人信息安全有关的案例报导,加大公益广告的投入力度。作为银行、支付媒介等社会机构,在涉及资金流动时,做到多次提醒,警示风险等行动。同时,作为对学生思想影响重大的家庭成员,也需要多了解和参与到个人信息安全保护的中来,多与学校和辅导员沟通配合,起到监督作用,以便纠正孩子的危险行为。

参考文献

- [1]彭永峰.国内大学生网络安全认知现状与提升[D].郑州大学,2019.
- [2]马旭.大学生网络犯罪现状及原因分析[J].法制博览,2019(01):35-36.