15万条简历就这么被卖了?

智联招聘个人简历遭私售,信息安全成隐忧

《检察日报》 史兆琨

“一般官网报价为50元一条的简历,我们出卖的价格为2元至2.5元一条。”6月2日,在北京市朝阳区法院,被告人申某接受记者采访时表示。

作为智联招聘的大客户部销售,申某利用智联招聘网站系统漏洞,于2016年3月至10月间,在智联招聘的客服李某帮助下,将该网站15.5万余条个人简历廉价卖给北京某科技公司的人事经理余某。该案于2日上午在北京市朝阳区法院开庭审理。

利用系统漏洞私售个人简历信息

据智联招聘负责人介绍,按照公司的正常流程,销售人员去找有招聘需求的公司,双方签署服务合同,对方缴纳服务费用后,公司会提供网站简历库下载的用户名和初始密码给对方,对方在已开通的权限内对简历库的个人简历进行下载。

申某告诉记者,在做销售期间,业绩压力很大,如果完不成业绩奖金就泡汤,经常有人私下问他能不能将简历便宜出售。

“2016年3月,我发现公司的程序有漏洞,于是便以乙公司的名义发起转移合同的邮件,李某在后台回复邮件确认,之后运营部门逐层审批,我截取邮件审批结果截图上传公司系统,转移合同便生效,系统会生成一个用户名和密码。”申某告诉记者,他将这个包含数份简历的账户密码私下销售给客户获利。

李某帮申某确认邮件的过程中,简历数量最多的一次就达1万多份。“前期大约一周一次,后期几乎每天都有。”李某坦承,“由于磨不开面子,加上自己也想从中挣点钱,”就同意了。

申某每次获取简历后会通过微信红包付给李某200元。“李某觉得钱少,我答应每1000份简历给他200元。”申某表示,自己一共挣了将近50万元,给李某的好处费差不多接近4万元。

该案由北京市公安局朝阳分局侦查终结,以被告人申某、李某、余某涉嫌侵犯公民个人信息罪,于2017年1月19日向北京市朝阳区检察院移送审查起诉。

北京市朝阳区检察院认为,被告人申某、李某违反国家规定,向他人出售公民个人信息,情节严重;被告人余某非法获取公民个人信息,情节严重,应当以侵犯公民个人信息罪追究三被告人的刑事责任。被告人李某在共同犯罪中起辅助作用,应当从轻处罚。

该案未当庭宣判。

批量信息缺口催生牟利卖方市场

“我真没想到自己会触犯刑法,还请法官从宽处理。”“80后”、具有本科学历的被告人申某在庭审现场作最后陈述时非常后悔。

据悉,侵犯公民个人信息的犯罪案件中,信息提供者通常为“内鬼”或“黑客”,不少高学历者也因错误认识走上了犯罪之路。

北京京师律师事务所刑事诉讼部主任张立文接受采访时表示,侵犯公民个人信息犯罪案件多发、高发,一方面,贷款、保险、房屋销售等从业人员由于业务开拓,具有大量公民个人信息的需求缺口;另一方面,银行、部分商家拥有公民个人信息资源,但内部管理规定缺失或相对不完善,给个别人员可乘之机。

“公民保护意识不强,在生活中大量填录个人基本信息,同时,不少商家采取赠送小礼品、免费服务等手段免费获得公民个人信息。”该案公诉人、北京市朝阳区检察院检察官助理石晓琼认为,这些都是造成个人信息泄露的渠道。

批量公民个人信息的泄露,很容易衍生出有牟利意图和动机的卖方市场。“依赖于现有网络大数据技术条件提供的便利,获得公民个人信息的一方可以通过技术优化手段对信息过滤、归类,然后以获利为目的地实施广告投放,也不排除借助所获得的公民信息实施各类诈骗、网络盗窃等刑事犯罪行为,给公民个人的正常工作、生活造成不当困扰,甚至导致财产损失或者人身伤害。”北京兰台律师事务所合伙人唐烈文分析道。

依法保护个人信息刻不容缓

就在该案开庭审理前一天,即6月1日,《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(下称《解释》)正式施行。《解释》明确,非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息50条以上的将入罪。《解释》对公民个人信息的类型进行了区分,相应设置了50条、500条、5000条的入罪标准,侵犯数量达入罪标准10倍以上的,即属“情节特别严重”,可能判处三年以上七年以下有期徒刑。

“随着新司法解释的颁布施行,公检法机关应加大对侵犯公民个人信息犯罪的打击力度,提高电子取证能力,切实保障公民个人信息的安全。”石晓琼表示。

唐烈文认为,两高出台司法解释保护公民个人信息,强化公民信息形成、保管单位的法律责任,将促使其加强技术措施投入,让犯罪分子无漏洞可钻。

同样于6月1日生效的网络安全法,首次在法律层面规定了个人信息保护的基本原则。该法明确指出,收集适用信息应经用户明示同意,不得收集无关信息,不得向他人提供个人信息,不得非法出售个人信息。

“司法机关应持续保持打击侵犯公民个人信息犯罪的高压态势,政府部门应建立多位一体的综合治理机制,通过多种渠道开展保护公民信息的教育。”张立文接受采访时建议。

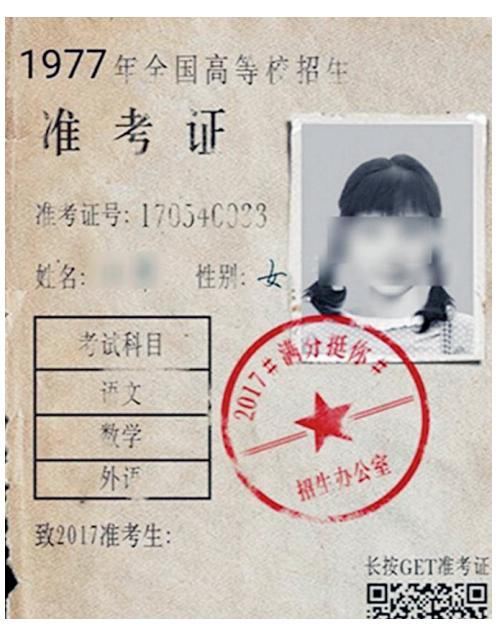
“刷脸”定制“准考证”?这么玩可能后果严重

网络专家:或导致个人信息泄露

《新京报》 王煜

高考临近,近日,一些在线生成个性化“高考准考证”的链接,在朋友圈“刷屏”。识别二维码后,进入生成界面,用户上传姓名及照片,即可完成。

多名网络安全专家称,类似链接来源鱼龙混杂,不排除不法分子通过这样的“创意”,获取公民照片及个人信息的嫌疑。这些信息一旦泄露,会对部分依赖“刷脸”的软件,如银行个人支付系统等构成安全威胁。



高考前“准考证”刷屏

泛黄发旧的纸张上,写着“1977年全国高等学校招生”字样,此外,准考证号、姓名、性别及考试科目,一个都不少。“考生”的黑白照片下,还盖有鲜红的“招生办公室”印章。连日来,个性化的“高考准考证”在朋友圈“刷屏”。

6月3日,记者以用户身份,致电“准考证”生成器的推出方——某国际快餐连锁品牌客服热线。一名工作人员称,这一生成器是高考期间推出的策划,主要目的是“激活用户,同时提高品牌关注度”,并不具体推销某一款产品。

类似创意并非首次出现。此前,朋友圈中常见各类通过识别二维码进入,生成各类证件、场景的生成器。其操作流程大同小异,并需用户填写部分个人信息,上传照片。此外,这些生成器中,大多附有各类商业推广信息。

一名互联网从业人员介绍,类似生成器,实际上是一种H5动画。设计者事先将场景固定,用户通过上传照片等信息,替换模板中一些画面,即可实现“私人定制”。“制作比较简单,主要看创意能否吸引人。”其表示,随着移动端的兴起,这类通过“刷屏”博取品牌关注度的生成器,在朋友圈中走热。

生成器暗藏泄密风险

简单个性的各类生成器,实际上潜藏着信息泄露的风险。多名网络安全业内人士指出,制作过程中,生成器实际上获得了用户的部分个人信息及照片,稍加技术处理,即可“攻破”一些依赖人脸识别进行身份验证的软件。

网络安全专家李铁军称,目前商用人脸识别技术,主要在银行的个人移动支付上,即以人脸代替传统的密码进行操作。此外,在一些车站及码头、机场,也有“刷脸进站”的应用。

一名网络安全工程师表示,如果不法分子渗透“人脸识别”领域,则可以通过设计类似生成器,大量获得人脸数据及相应的个人信息。在人脸识别技术大量应用后,这些数据将面临被贩卖,甚至直接用来窃取个人财产,后果严重。

李铁军建议,用户在使用类似生成器时,不要轻易泄露个人基本信息及照片,以免造成财产损失。

■ 记者体验

“准考证”1分钟生成

6月3日,记者通过识别朋友圈一张“准考证”上的二维码,进行生成体验。

点击二维码后,图片跳转进入H5界面,某国际连锁快餐品牌的商标下,是一台显示正在工作中的老式打印机画面,其出口不断滚动着各种式样的“高考准考证”。再往下,加粗的字体标注有“点击制作自己的准考证”选项。

进入制作流程后,图片再次跳转,界面显示,用户可自行选择“参加高考”的年份,再根据提示,选择性别,并上传正面照。

点击“一键回到高考岁月”,系统将生成具有年代感的“准考证”,如上世纪70年代“考生”会身穿绿军装、海魂衫或中山装,而上世纪90年代后的考生,则身穿衬衫、T恤,发型也更为现代。

“证件照”制作完成后,填写姓名及个人寄语,再点击确认,一张专属“高考准考证”就生成了。

如果事先选好了照片,从识别二维码到“准考证”制作完成,全程不过一分钟左右。

记者体验发现,如果上传的照片不够清晰,或并非正脸照片,则生成器无法进行识别,用户也无法进入下一程序。