株洲日报
社会周刊
28823925
2020年6月3日 星期三
责任编辑:邓金星
美术编辑:左 骏
校 对:马晴春

大数据时代 如何给个人信息上把“安全锁”

株洲日报记者 温琳

【核心阅读】

你是否有过这样的经历:刚给孩子报了个兴趣班,便会接到多个早教机构的招生电话;刚生完娃,就会接二连三地接到婴幼儿产品推销商的电话;去医院体检,保健品推销的电话便会尾随而至;下载一个汽车相关的手机应用,各种品牌汽车的推销电话立马就来了……

在当前信息越发透明化、公开化的大数据时代的大背景下,面对复杂的隐私安全问题,我们该如何保障公民个人信息安全?

立法是关键。不久前,本届人大公布的立法计划中,针对个人信息安全的《个人信息保护法》已经被明确列入立法规划,不久的未来,个人信息将有“专门法”保护。

1. 个人信息频频泄露 用户成了“透明人”

“因为网络服务升级,您所办理的宽带业务需要更新,收到信息请点击如下链接……”家住芦淞区的许女士,家里办理的宽带业务马上到期,这条信息差点让她信以为真。多亏留了个心眼,她向宽带公司电话咨询后才知道,这是一条包含木马程序的诈骗短信。

许女士的遭遇并非个例。即将毕业的大学生小刘在某招聘网站上注册了求职信息,随后,手机不断接到各种公司的招聘电话和骚扰短信,而他并没有向这些公司投简历,甚至专业也不对口。“我重新登录网站才发现,当初提交个人简历的页面下方有一个很难发现的选项,默认平台上的所有公司都可以查看我的简历,目前已无法修改了。”

“在商业利益驱动下,一些网络运营商、平台服务商或手机应用会读取、上传用户的通讯录、短信、通话记录等信息,有时候,用户并不知情。”国家互联网应急中心运行部高级工程师李佳说。

网上注册个账号学习英语,一些课程广告就会充斥邮箱;开个股票账户,还没交易就有各色理财顾问前来“问候”……除了个人姓名、性别等信息,这些素未谋面的“关心者”甚至连你的年龄、职业、婚姻状况等信息都了如指掌,这让公众对网络的信任和安全感日益消解。

近日,中国社科院发布的《社会心态蓝皮书:中国社会心态研究报告(2019)》指出,民众对个人隐私和信息的安全观念逐渐增强,参与调查的民众中超九成对个人信息安全表示担忧。在株洲,记者通过问卷和采访形式,在市中心广场和黄河路口,随机询问40名市民,36名表示因信息泄露带来困扰,其中有1人因此被骗过。

如同硬币的两面,互联网在提供生活便利的同时,也让用户成为不折不扣的“透明人”。

相关专家表示,在移动互联网时代,公众难免要牺牲个人信息以获取一定的服务,大众办卡、居家、出行甚至消费购物,在享受服务便利的同时,也需要提供各项信息。其中任何一个环节因为利益出现了松动,就可能导致信息泄露。

2. 五成以上诈骗案件 与个人信息泄露有关

“信息泄露可能会带来更严重的后果。”市委网信办相关负责人介绍,从商品退款诈骗、到机票退改签诈骗,至少50%以上的诈骗案件跟个人信息泄露有关。

2016年,山东发生一起震惊全国的诈骗案:因接到了一个诈骗电话,即将踏入大学的18岁女孩徐玉玉,被骗走全家人省吃俭用大半年才凑齐的9900元学费,导致突然晕厥,最终心脏骤停离世。

类似信息泄露引发的诈骗案,在株洲也屡见不鲜:2010年,株洲2000万元电信诈骗案告破,抓获犯罪嫌疑人6名,因为影响巨大,此案还曾惊动了公安部;2015年7月,芦淞公安分局破获一起大型电信诈骗案,捣毁6个电信诈骗团伙,抓获嫌疑对象40名,涉案金额达500余万元,嫌疑人遍布全国各地;2018年2月,我市就查处一家房产公司与装修公司进行地下交易的“潜规则”,现场查获数万条被非法倒卖的居民身份信息,涵盖居民的电话号码、住址,甚至还有户型图,而犯罪嫌疑人刘某和朱某因涉嫌侵犯公民身份信息罪被警方刑拘。

互联时代,个人信息随时有可能被泄露。记者梳理了这几年媒体报道的信息泄露事件,个人信息泄露主要有多个源头:网站漏洞,这是在黑市上流通的个人信息主要来源;针对个人用户的木马病毒、钓鱼网站和伪基站,以点对点的方式盗取个人信息;无良商家的“内鬼”和技术黑客;甚至现在最时兴的无人机、儿童智能玩具、扫地机器人等,都可能成为监视你的“间谍”。

“当前黑客技术门槛变低,窃取信息变得更加容易。与此同时,网络犯罪出现职业化倾向,已然形成网络黑色产业链条,工具开发者、工具应用者和利用工具实施犯罪者都有明确的分工,形成了一套体系。”网络专家说。

市委网信办相关负责人介绍,除了在网络安全宣传周开展相关宣传,我市公安刑侦部门每年都会应邀到高校举办预防电信(网络)诈骗知识讲座,以此应对日益上升的信息泄露带来的危害。

3. 保护个人信息安全 除了立法,还要建立监管体系

不用怀疑,隐私泄露将成为我国社会越来越严峻的问题,法律法规制度应尽快完善,有关部门应当尽快有所作为。

目前,全世界有100多个国家和地区制订了个人信息保护法,2018年5月,欧盟正式生效的《一般数据保护条例》更是成为对个人信息保护的里程碑之作。在世界上很多国家和地区重视个人信息保护的大背景下,我国各地对个人信息保护也越来越重视。

近年来,我国多条法律涉及公民个人信息保护。我国《刑法修正案(九)》中加入了侵犯公民个人信息罪这个新罪名。随后,两高司法解释明确规定:非法获取、出售或提供50条以上征信、财产等公民个人信息,即构成刑事犯罪。

网络安全法明确规定:网络运营者应当采取技术措施和其他必要措施,确保其收集的个人信息安全,防止信息泄露、毁损和丢失;关键信息基础设施的运营者应当履行安全保护责任。

有法律工作者指出,然而,关于公民个人信息保护的规定,散见于《网络安全法》《电子商务法》《刑法》等多部法律中,过于繁杂和笼统,且只限于规范侵犯个人信息造成后果的行为,执行力度不理想,信息泄露行为的违法成本偏低,震慑、打击力度不大,造成个人信息被泄露和非法利用现象泛滥成灾。就在本届人大刚刚公布的立法计划中,针对个人信息安全的《个人信息保护法》已经被明确列入立法规划,居民个人信息未来将有“专门法”保护。

2016年11月11日,市公安局成立市打击治理电信网络新型违法犯罪中心(下简称反电信诈骗中心),迄今已经破获电信诈骗案件数百起,涉案金额过亿元,有效避免了公民因信息泄露造成损失。

2018年1月,市公安局专案组以株洲市火车站周边办证刻章人员为重点,经过近1个月的缜密侦查,抓获犯罪嫌疑人18人,收缴身份证3091张,制作假证工具1套,摧毁一个长期盘踞在株洲火车站附近的制作假证和贩卖身份证犯罪团伙,有效地打击了电信诈骗的源头黑色产业链条。

中国社会科学院法学研究所研究员周汉华认为,除了立法,还得建立一个有效的监管体系,有力的执法结构,科学的执法方法,有威慑力的执法手段,以及执法的监督制约机制,形成一个社会共治的结构。

4. 互联网平台三条原则 保障公民信息安全

个人信息“裸奔”,不仅让公众陷入不安,也让互联网平台陷入信任危机。

近年来,移动互联网应用程序(APP)得到广泛应用,在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时,APP强制授权、过度索权、超范围收集个人信息的现象大量存在,违法违规使用个人信息的问题十分突出。

中国消费者协会2018年发布的《APP个人信息泄露情况调查报告》显示,超八成受访者曾遭遇个人信息泄露问题,经营者未经授权收集个人信息和故意泄露信息成个人信息泄露的主要途径。与此同时,当消费者个人信息泄露后,约86.5%的受访者曾收到推销电话或短信的骚扰,约75.0%的受访者接到诈骗电话,约63.4%的受访者收到垃圾邮件,排名位居前三位。

去年,市公安局网技支队曾对株洲属地的38个APP进行了全面检查,并针对抽检的APP做出了详细的检测报告。结果显示:抽检的株洲属地38个APP均存在漏洞问题,平均每个APP漏洞达6.23个,且大部分未进行安全加固防护。

据互联网专家介绍,数据收集越多,采集机构越杂,安全隐患越大。保护个人隐私,保障数据安全,首先需要反思的是数据收集是否过头,数据安全能否得到保障。数据采集有了规矩,公众才可能消除在透明“玻璃房”中的恐惧感。

未来智慧生活中,高度智能化与高度隐私安全如何兼得,安全专家认为应当遵守三条原则:收集要授权,使用有界限,存储应保护。

首先,任何机构或个人在收集、利用个人信息时,需先得到用户授权。用户有知情权和选择权,即知道哪些信息被收集、可以选择是否让渡。所有信息应归属于用户本人,收集方只是“借用”,所拥有的是数据分析的结果,而不是其所有权和处置权。其次,信息收集应有度,使用也应有边界。对于敏感的密码、指纹、签名字迹、人脸特征等身份认证信息,更应该有明晰的界限,除特定的情况并征得用户授权外,用户本人应绝对掌控,信息采集方也无权违规使用。最后,保护隐私,信息收集方要承担起保障数据安全的义务。

国家互联网应急中心副主任刘欣然建议,政府方面应建立监测、研判、预警、处置和追踪的联合处理网络安全问题的机制。与此同时,个人用户也要提高自身安全意识。如非必要,尽量不要在一些网站上提交个人信息;要访问正规的网站,避免被钓鱼网站骗取个人信息等。

相关链接

四种电信诈骗比较常见 女性、中老年人易上当

近些年,越来越多的电信诈骗案件暴露在公众视野中。近日发布的一份《中国电信网络诈骗分析报告》显示,电信网络诈骗整体呈现犯罪手段多样、骗术翻新快的特点,诈骗类型从中奖诈骗到冒充公检法、冒充熟人;诈骗技术也在逐步升级,从伪基站到改号软件;诈骗对象也越来越精准,从“满天撒网”到如今的“精准识别”。

其中,四种电信诈骗比较常见:即假冒公检法诈骗,冒充购物网站、银行、电信等工作人员诈骗,贷款理财诈骗,冒充领导、熟人诈骗。

最高人民法院发布的一份报告显示,近五年来,电信网络诈骗案件以电话诈骗为主,占全部案件的5成以上,排名前五的诈骗方式,还有短信、木马病毒、钓鱼网站、QQ。

《中国电信网络诈骗分析报告》指出,目前电信网络诈骗的受骗人群主要包括四大类:大学生和大专生,城市外来务工人员,老年人以及农村地区人群。

记者查阅30起近五年警方已破获的信息泄露诈骗案显示,受害人中女性占了21起,占70%,成了主要受害群体。受害人年纪四十五岁至七十岁的有19起,占到案件数的6成以上,上当受骗者往往是退休在家的老人,或和社会接触少、对网络知识了解少的中老年人群体。

防止个人信息泄露 六个小细节请您注意

填写问卷不要留联系方式。目前填写问卷似乎是一件很时髦的事情。在网上、街头,甚至是学校的自习教室,都可能遇到有人以各种借口请你填写问卷,不能在问卷上填写个人重要的信息,如电话号码、邮箱等重要的联系方式。

不贪占小便宜。爱占便宜是人的天性,但是天下没有免费的午餐。在网上或者是街头,会遇到这样一种情况:留下联系方式等相关信息,就会获得免费赠送的小礼品。此时,你泄露的是个人的信息,但是得到的是并不实用,甚至是根本没用的小物件。

快递单据不随意丢弃。收发快递似乎已经成为了很多人生活的一部分,更有不少人接到快递后,把东西拿走,箱子和快递单据随手就丢在了垃圾桶里。快递单据上一般都会记录着你的姓名、地址和联系方式。

车票机票正确处理。目前火车票和飞机票都是实名制购票,在票面上留有自己的姓名和部分身份证号码等信息。因此在乘车出站之后绝对不能随意将票据丢弃,更不能一出站就被非法分子收走。

不随意留下自己联系方式。在很多时候,我们随意留下了一个电话号码,结果会莫名其妙地接到很多电话,比如看房的时候。打这些电话的人往往知道你的需求,不厌其烦地打电话给你,甚至会影响你正常的工作和休息。因此,为了自己耳根清净,尽量不要随意留下自己的联系方式。

电脑做好安全措施。网络世界丰富多彩,但同时也充满危险。为了能够更好的享受网络生活,在上网前,最好打开防火墙。如此可以给自己的电脑穿上一件防护衣,避免外来的攻击,减少通过网络泄露自己信息的概率。

如果市民的身份信息被他人泄露,可以报警求助。如果泄露者的泄露行为给市民造成了经济损失,市民还可以向法院提起诉讼要求泄露者承担赔偿责任。