责编:王 娟　创意:刘学萍　质检:尚青云

网络消费时代,个人信息泄露、盗用事件时有发生

我的信息,你不该知道那么多!

今天，最懂我们的似乎是互联网。电商了解你的消费需求,专车清楚你每天的行踪,移动支付掌握你财产变动……个体的身体、位置、通信、征信、交易等各类信息被源源不断地收集、存储在网络空间,每个人似乎都成了“透明人”。

中央经济工作会议提出，着力解决网上虚假信息诈骗、倒卖个人信息等突出问题。个人信息泄露、盗窃事件发生的原因是什么？谁来为个人信息安全保驾护航？

隐私在“裸奔”
最怕“有心人”

“骗子不仅选择了恰当时机打电话，而且能准确说出所购商品的型号、颜色等,人们很容易上当。”家住山西太原的网购达人张艳说,虽说互联网带给生活诸多便利,但每天都能收到骚扰短信、垃圾邮件、诈骗电话,不胜其烦。“注册账户、下载软件时不停地提交私人信息,也不知道我的信息是从哪个环节泄露出去的。”张艳很懊恼。

网络消费时代,个人信息在“裸奔”,安全风险日益凸显。360 发布的《2017 年手机安全风险报告》印证了这一点:仅第一季度,360 安全卫士就拦截了 24 亿条垃圾短信,其中 1.82 亿条是诈骗短信,绝大多数伪装成电商和银行通知,容易让消费者上当受骗。

北京师范大学经济与工商管理学院副教授李江予说,从网购、网约车到在线教育、智能家居,互联网正与各行各业深度融合,人们日常生活的各个角落都被网络覆盖，被各类移动终端包围，传统的生产生活方式正在被互联网深刻改变。对于这些新产业、新业态来说，谁占有充足信息，谁就能占领市场制高点,商家必然绞尽脑汁收集客户信息。但技术是一把“双刃剑”,个人信息也面临前所未有的泄露风险。

腾讯守护者计划安全专家马瑞凯指出,人们在网络上的一举一动都能被数据化。“个人信息可用于精准诈骗,提高犯罪成功率,不法分子采取五花八门的手段非法获取个人信息,只要‘有心’,就可能成功。”

网络安全工程师、上海岂安信息科技有限公司资深技术顾问游浩源认为，个人信息被泄露的途径主要有两个：黑客主动攻击知名度较高的企业网站,获取用户数据,或要挟企业支付赎金,或到黑市上交易;企业内部员工和不法分子里应外合，比如快递单是不法分子的“香饽饽”,快递公司员工成为黑色产业链中的重点突破对象。

“后一种不法分子主要是利用了公众的防范意识不足。”游浩源介绍,小区、地铁里经常会有扫码领奖品的活动，手机一扫就会跳转至钓鱼网站。有些车站、便利商店等公共场所安装了共享充电宝，后台人员通过数据线自由“出入”个人手机。各种钓鱼网站、木马病毒伪装成正规网站,诱骗公众点击。有些人热衷于在社交网站晒生活,信息也会被不法分子抓取。

黑色交易猖獗
紧盯百姓钱包

为何不法分子使出浑身解数盗取公民个人信息？马凯瑞说,信息是互联网经济最宝贵的资源之一，正规商业机构为之激烈竞争,不法分子也想分一杯羹。据推测目前我国网络非法从业人员已超 150 万人，相关产业市场规模已达到千亿元级别。高额的经济回报、较小的难度要求、较低的犯罪成本,引诱越来越多的人加入。

去年 5 月,最高检察院公布的侵犯公民个人信息罪的典型案例说明了这一点。广东省河源市的章某从互联网非法购买学生信息,冒充教育局、学校教务处的工作人员，以获取国家教育补贴款为由,诱骗学生家长通过 ATM 机转账到指定账户。截至查获时，章某共拨打诈骗电话 4000 多次,骗取 11 多万元。在另一起案件中,张某在购物时偶然发现某电商平台有技术漏洞,就委托他人,编写恶意程序,进入后台盗取客户订单信息 1 万多条,在网上分批倒卖给姚某，姚某再加价倒卖,牟取不正当利益。

中国政法大学传播法研究中心副主任朱巍介绍,这些典型案例有共性,即盗取手段精细化,犯罪主体组织化,信息需求、盗取、交易形成了一条完整的黑色链条,不法分子分工专业、配合高效,流窜在各个论坛、微信群等,隐蔽性很强。

“围绕黑色链条，还有一些外围产业,比如专门提供各类技术设备的,专门负责海外洗钱的。”游浩源说,这些黑色交易如涌动在地下的暗流,盘根错节,贻害无穷。

“说到底,黑色交易盯上的还是老百姓的口袋。”马凯瑞介绍,不法分子编排巧妙的“剧本”,仿冒公检法部门,实施色情、赌博恶意营销等,抓住公众的心理弱点实施诈骗。

打技术补丁　堵制度漏洞

北京市盈科(深圳)律师事务所经济犯罪法律部副主任翟振轶介绍,经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或向他人非法提供。一旦发生泄露、丢失,应立即采取补救措施。

翟振轶说,我国有近 40 部法律、30 余部法规涉及个人信息保护。《消费者权益保护法》《民法总则》《网络安全法》《刑法修正案(九)》等法律法规进一步明确了责任主体、犯罪要件等,织密了法律保障网络。比如,当相关主体以出售、提供、窃取或其他非法手段获取公民个人信息超过一定数量时,就构成刑事犯罪，可以说很具有威慑力。

“但对个人信息安全的管理权分散在不同部门,工信、工商、公安等都能管,但都管得不彻底。”翟振轶说,相关部门要加强联动,紧密配合,不能让公众求助无门。

企业也责无旁贷。翟振轶说，现在不少企业已经开始重视保护消费者的信息安全。加大投入,购买技术服务,打上技术“补丁”,完善管理制度,防止“内鬼”的出现。比如几家快递公司推出电子扫码面单，尽量隐去快递单上的个人信息,受到消费者欢迎。

但整体上，当前企业的技术、管理手段仍跟不上现实需求。游浩源介绍,首先,个人信息会在企业各部门之间流动,许多员工都能接触，风险点很多。以电商网站为例,从技术、市场到客服都有一定的数据访问权限。不法分子可通过各种手段利诱工作人员,为其提供服务。其次,不同企业之间合作时共享数据,导致信息安全存在系统性风险。“大量的数据都存储在‘云’里,企业不仅要保障自家数据库的安全,不同的企业更要一起保障‘云’的安全。”

“更重要的是,企业保护公民个人信息的意识还不够。”李江予说,升级信息保护系统,对企业而言,意味着投入增加。互联网企业不少是创新型公司,实力较弱，对长远利益考虑不足。应鼓励、引导社会力量,对企业信息安全工作开展监督、评价和评级等，督促企业重视这一问题。

个人因信息泄露造成财产等损失,如何维权?翟振轶说,此类案件因金额小、数量多,公众想要挽回损失，确实比较困难。但不能选择忍气吞声,应尽快到公安机关报案。如果一定时期内,报案和投诉集中在某个企业或某个领域，达到立案的标准,相关部门会根据法律的规定,采取措施,维护公众的权益。

个人也应绷紧信息安全这根弦。冯铭提醒消费者，快递单、收据等重要信息不要乱扔;下载软件要认真阅读隐私条款；在社会网站上尽量不暴露个人信息;分级设置密码;平时多和父母朋友沟通，减少他们被骗的几率。

“保护公民个人信息,需要政府、行业、企业和个人通力合作,打好‘马赛克’,捂紧钱袋子。”李江予说。

（据《人民日报》）