手机信息被盗一年损失近千亿

2017年12月5日,北京市公安局海淀分局宣布破获一起新型特大非法获取公民个人信息案,查获包括手机号在内的公民信息100余万条。根据中国互联网协会发布的《中国网民权益保护调查报告2016》,2016年上半年,网民平均每周收到垃圾短信20.6条、骚扰电话21.3个。

私人号码成了“公开信息”,手机用户不堪其扰。到底是谁卖了我的手机号?

网页也能“偷走”手机信息

“我用手机搜索了血小板偏低的危害,就是浏览网页,没有输入手机号,谁曾想没过几个小时就有医院打电话介绍治疗血小板偏低的特效药。医院是怎么知道我的手机号的?”

早在2015年,就有网友在网络上询问,有类似遭遇的网友不在少数。

北京市海淀分局破获的这起案件,给出了答案。“某些网站植入一段恶意代码,只要用户使用手机流量打开网页,黑客就会利用运营商漏洞,抓取到用户的手机号、IP地址、访问时间、搜索时输入的关键词等信息,”海淀分局网安大队副大队长董立波介绍,“这是一种新型黑客手段,能在用户不知情的情况下获取个人信息,进而开展精准营销甚至电信诈骗,多出现在医疗、教育、贷款等网站。”

看似简单的代码背后,暗藏着一条黑色产业链。董立波介绍,本案所涉黑色产业链分三个层级。上游是恶意代码的生产者,下游则是植入恶意代码的网站,中间商在两者之间牵线搭桥。下游网站虽已购买恶意代码,但不能直接看到被抓取的个人信息,得按条数或者包月从中间商手中购买。中间商从上游网站获取代码的价格是600元,收购的个人信息8分至1角钱一条;转手卖给下游网站时,代码价格涨到1000元,个人信息则能卖到5角至1元钱一条。

上游网站“薄利多销”,中间商网站赚取差价,下游网站精准出击。黑色产业链各个环节“皆大欢喜”,用户则成为买单者和受害者。

“我们通过技术手段对全网网站进行检测,鉴别哪些网站植入了窃取公民信息的脚本或者黑客工具,通过溯源摸清产业链的规模和上下级关系,并把这些情况提供给警方。”百度安全实验室X-Team负责人黄正说。据百度安全团队统计,有4万多家网站存在此类行为,非法获取超过5000条手机号信息的服务平台有27家。若不采取措施,预计每天将有500万人次点击中招。

外贼内鬼造成信息裸奔

据统计,截至今年8月,三家基础电信企业的移动电话用户总数达13.8亿。而仅在2015年下半年至2016年上半年,因垃圾信息、诈骗信息、个人信息泄露等造成的总体经济损失就高达915亿元。

一些黑客利用运营商或网站平台的漏洞,采用技术手段非法获取公民信息。去年引起广泛关注的“徐玉玉案”中,黑客杜某非法入侵山东省高考信息平台,窃取64万余条考生信息;购买这些信息的徐某以发放助学金为名义拨打诈骗电话,造成了徐玉玉离世的悲剧。

也有内鬼作怪,把正常途径获取的公民信息转手卖给他人。今年6月,浙江宁波警方破获一起案件,“上游卖家”程某出售多年从事通信、房产等行业积累的个人信息,涉及公民信息1.2亿条之多。

今年2月,有媒体曝光称,只要报上手机号,就能从信息贩子手中获取大量公民信息,包括精确到秒的打车记录、来电去电号码记录和通话时长的手机通话记录、误差在50米以内的实时定位信息等。

中国传媒大学法律系副教授刘文杰说:“手机号本身包含的信息有限,但如果和其他公民信息组合起来,比如姓名、身份等,能大大提高精准营销或者电信诈骗的成功概率。”泄露或者非法传播包括手机号在内的个人信息,除了可能侵犯公民的隐私权和个人信息权,还可能导致公民的财产权和其他人身权利受到侵害。

标本兼治打击黑色产业

2017年 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》正式施行,明确了公民个人信息的范围和侵犯公民个人信息罪的定罪量刑标准。

根据这一司法解释,非法获取、出售或提供公民手机号信息达到5000条以上,属于“情节严重”。业内人士认为,这为裁决公民信息泄露案件提供了统一标尺,起到了威慑和预防的作用。

“不得不说,黑色产业自身也在不断‘进步’,不会因为新规出台就‘坐以待毙’,他们想尽办法更新技术、逃避监管、继续牟利,有的黑色产业利用地域差和时间差,专挑监管薄弱的地方和时段下手,这对我们提出了挑战。”百度安全事业部总经理马杰说。

目前,多家互联网企业已开始使用人工智能技术和机器学习技术监测抗击黑色产业,保护网络安全。

既要治标,更要治本。“解决手机号等公民信息泄露问题,不能只处罚下游买家,要从网站平台等源头下手。手机号泄露的源头在运营商或者网站平台,财产信息泄露的源头在金融业,医疗信息泄露的源头在医疗业。所涉单位要严格履行职责,从严管理运营、从严管理队伍,为公民信息提供安全保障,发生信息泄露时要及时预警,并向主管部门报告。对有责任的源头单位,有关主管部门要加大监管,及时处理。”刘文杰说。

完善立法 保卫用户信息安全

在互联网时代,用户数据的价值是不言而喻的。根据被泄露的个人信息,不法分子可以筛选分类,然后进行“有针对性的营销”。

个人信息安全已经严重威胁到人们的生活。人民网的一项调查显示,90%的网友曾遭遇个人信息被泄露;有94%的网友认为,当前个人信息泄露问题非常严重。因为个人信息泄漏,让人们无时不处在烦恼之中。因此,依法治理网络社会,保护个人信息安全是迫在眉睫的现实课题。

我国目前对网络个人信息保护的立法,仅体现在一些零散的法律条文中,此外,还有一些地方性法规作了简要概括的规定。为防止信息泄露引发的信息骚扰甚至违法犯罪,要尽快完善个人信息安全保护的制度体系,在立法、执法、普法上都要进一步推进。

专家建议,要推动《个人信息安全保护法》尽快立法,对政府部门、金融、电信、交通、中介等单位的个人信息保护作出严格规定,同时严打泄露、倒卖个人信息的违法行为,让贩卖个人信息者受到严惩。与此同时,还要加强对行业的规范和监管,对拥有个人信息的政府单位、企业和个人,明确其保护个人信息安全的责任和义务。此外,提升个人信息安全保护的技术能力,通过宣传提高全社会的信息保护意识,也有利于营造一个安全的信息消费环境。

此外,个人也要加强信息安全保护,网络账号应尽量设置复杂密码并定期更换;不随意使用公共电脑处理涉及个人隐私的业务;如发现信息泄露或账户异常,要及时通知服务机构,必要时报警。

互联网带给我们很多的生活便利,要根治信息泄露的顽疾,还需要各方通力合作,共同打造干净的互联网环境。

(摘编自 人民网)

交通肇事碾死醉汉逃逸 一男子被判有期徒刑三年

东胜一男子明知自己撞人后还驾车逃逸,最终自食恶果,被判有期徒刑三年,缓刑四年。

东胜区法院经审理查明,2017年3月16日22时许,被告人高某驾驶帕萨特小轿车,将醉卧在道路上的王某碾压,致王某当场死亡,被告人高某驾车逃逸。后被告人高某在返回事故现场途中被巡警抓获。经公安机关责任认定,高某驾驶机件不符合技术标准的机动车上道路超速行驶违反禁止标线且发生事故后驾车逃逸是造成此次事故的主要原因;被害人王某在车行道内坐卧是造成此次事故的次要原因。由此认定,被告人高某应负此次交通事故的主要责任,被害人王某负事故次要责任。

另查明,案发后,被告人高某与被害人王某的家属达成经济损失赔偿协议,向被害人家属赔偿了折合人民币60万元的款物,并取得了被害人家属的谅解,被害人家属明确表示,希望法庭从轻处罚被告人。

合议庭认为,被告人高某违反交通运输管理法规,因而发生重大事故,致一人死亡,其行为已构成交通肇事罪;被告人高某在被查获时准备去事故现场看事态的发展,并非主动投案,故合议庭认为,高某不构成自首。但被告人高某到案后始终如实交代自己的犯罪事实和真实身份,属坦白,可以从轻处罚。且事后,高某积极赔偿了被害人家属的全部经济损失并取得了被害人家属的谅解,具有悔罪表现,酌情予以从轻处罚。依照《刑法》相关规定,遂作出上述判决。 (吴晓春 于立辉)