



网 址: www.sxjib.cn
投稿邮箱: sxjrb@sxjrb.com
新闻热线: 4660816

山西经济日报

周刊

SHANXI ECONOMIC DAILY

2020年12月9日 星期三

责编: 组版: 王俊菲 校对: 小雷

数据安全, 我们该知道些什么?

本周聚焦

现在人人一部手机, 手机可以随时移动支付购物、打车、吃饭, 上公交车刷手机, 进公共场所亮手机上的二维码, 可以说到了一部手机行天下的程度——钱包可以不带, 零钱可以没有, 只要有手机就行。而且, 对很多人来说, 目前手机也是可移动的电脑, 不少工作可以通过手机进行。

另一方面, 手机里有很多个人重要信息、身份信息、金融信息、购物留的家庭住址信息乃至家人的信息, 需要保护好。

对于这些信息的数据安全, 大家都非常重视。但是对我们个人来说, 数据或个人隐私的信息, 在安全上该如何保护呢?

大数据下的精准营销

太原姑娘肖雯在北方长大, 大学去了更北的地方。她一直想去南方旅游一下, 不是报团走马观花游, 就想到一个地方住几天, 深入大街小巷转转。前一阵子, 看看疫情防控常态化了, 国内景区景点也基本都开放了, 各个城市间的流动也正常了, 肖雯冒出一个想法“去武汉看看”。

她和几个同学一商量, 大家都赞成去武汉看看。于是开始了做攻略。肖雯告诉记者: “以前我也没有注意, 这几天工作之余我在手机上刷武汉旅游攻略景区景点等信息, 也在去哪儿网上搜了去武汉的特价机票。然后手机上的UC浏览器就给我展示去武汉的特价机票广告, 小红书有武汉的旅游攻略。这几个应用是不是交换我的信息呢?”

不仅仅是肖雯有这个疑问, 记者也一样有。因为嫌麻烦, 记者手机上并没有安装淘宝、天猫等购物平台, 需要网购一般是在电脑上操作。常年熬夜写稿子, 头发越来越少。记者就在手机上搜索了一下生发洗发水, 这一下可了不得了, 只要打开手机, 所有的浏览器都向我推送各种生发洗发水; 打开几个新闻APP, 醒目的位置也是生发洗发水。他们怎么知道我想



山西尚东易斯科有限公司总经理杨锡瑞为我省部分网信部门工作人员进行数据安全培训。 本报记者 王昕 摄

要洗发水? 为什么还是好几个平台都知道? 这, 算不算信息泄露呢?

记者咨询了做IT行业的几位人士。田斌曾经从事多年通讯信息行业, 他告诉记者: “这个还算不上信息泄露, 应该是大数据下的精准营销推送。大数据下, 你的搜索内容被抓取到, 系统自动就会推送你所要的东西。”最麻烦的是, 东西已经买回来, 还一个劲儿推送。针对这种问题, 田斌说, 点击一下, 就会出现不感兴趣等选项, 点击不感兴趣, 以后就不会推送了。

田斌进一步分析, 之前搜索过的东西后来一打开手机就有, 主要是两个因素: 第一个是大数据的算法分析, 发现你感兴趣, 就自动给你推送; 第二个就是手机内存的自动读取。很多人以为打开手机不打开购物APP, 大数据就不会读取购物信息, 其实不是, 内存的读取和你打不打开购物APP没关系。要想不被系统读取看过的页面, 就要立即关机重启, 但意义不大, 有的浏览器有记忆功能, 开机就有。

学软件专业的薛剑说, 其实大家在手机上下载一个软件或者应用程序的时候, 都会有一个好几页的说明, 大意是你提供的微信或者支付宝或者其他账号仅供消费承诺, 不会提

供给第三方等, 需要你同意。这个条款一般人不会仔细看——下载这个程序就是为了用, 肯定越过内容直接同意。这个程序就会把你的需求传回系统分析推送。田斌和薛剑都表示, 不管大数据把你的消费习惯摸得多么清楚, 只要没有具体到个人头上, 就不算是泄露。

大数据怎么获取信息

在手机上的各个应用中, 拼多多是记者个人最反感的一款应用。它在很多程序中都做了链接, 不小心碰着了, 速度条走得飞快, 火速就下载到桌面上, 还得再卸载。给老人养老金认证上老来网、看天气预报等, 都会时不时下载个拼多多, 烦不胜烦。

第二个就是同事朋友们有的特别喜欢去各种APP砍一刀要特价商品。这么久真没砍过用什么价格砍成过一次。这种被链接砍价的程序, 基本上就把个人的信息抓取走了。

山西尚东易斯科有限公司是山西网络信息安全服务及运维提供商, 总经理杨锡瑞说, 互联网技术的发展确实是日新月异, 发展迅速。举个例子来说, 数据可以通过分析消费者打车的起始点、每个月的日常消费位置情况, 定义你所居住的小区; 还

可以精确提供小区内居民的消费习惯、购物重点。这些数据可以为广告商在小区内精准发布广告提供帮助。杨锡瑞表示, 大家对大数据获取信息以前是不理解不关心, 现在则是贪方便且反感。其实, 不管你理解不理解, 支持不支持, 技术已经发展到相当的程度。别的不说, 就拿现在去那里需要的健康二维码来说, 规定时间里你去过哪里, 手机轨迹不会撒谎, 二维码不会作假, 一目了然。关键是否合法合理获取大数据信息?

记者在日常采访中也了解到, 疫情防控常态化的大前提下, 如果某地有疑似病例, 密切接触者、一般接触者, 去过那里的人员信息可以迅速找出来, 直接通知到所居住的小区, 这要归功于越来越优化的大数据技术。大变当前, 生命肯定比信息安全更重要。

大数据获取信息的渠道有很多, 数据很多也是碎片化的。事实上, 在大数据从业人员看来, 信息的合理利用是数学建模方式在起作用, 是算法的应用成果, 无所谓对错。但是如果信息细致到每个个人身上, 包括身份信息、家庭住址、联系方式等等, 那就属于个人信息范畴了; 获取的信息要是未被授权而运用到商业化行为上, 或者提供给第三方, 确凿无疑是信

息泄露, 涉及到对个人隐私的侵犯。

怎样保护自己的隐私信息

说起隐私信息保护, 记者觉得自己还是比较小心的。但是前几天收到的一条探探应用发的短信让我很疑惑: 让给一个人回应, 给了一个网址。我手机用的是先生名下的, 但是短信却写着记者的名字, 这是从哪里来的?

田斌说, 这种情况很常见。目前超市会员卡、小区里的菜店、饭店、各种专卖店都要登记手机号码和名字, 不知不觉就泄露了。薛剑也说, 以前那种从快递包裹单上获取信息的情况已经不多见了, 获取信息的渠道已经不那么粗放了, 移动支付的使用, APP的应用, 获取信息都是瞬间的事情。

另一方面, 我国在信息保护立法方面的进程也有很大进展。杨锡瑞告诉记者, 2017年6月1日实施《网络安全法》后, 越来越多的比较细化的网络安全法规条款陆续出台, 今年实施的就不少了。他梳理了一下, 1月1日实施的《国家政务信息化项目建设管理办法》, 3月1日实施的《网络信息内容生态治理规定》, 6月1日实施的《网络安全审查办法》, 特别是10月1日实施的《信息安全技术 个人信息安全规范》, 旨在遏制个人信息非法收集、滥用、泄露等乱象, 最大程度保障个人的合法权益和社会公共利益。此外还有《工业数据分类分级指南》、《APP违法违规收集使用个人信息行为认定办法》等等, 逐步搭建起了一个信息安全保护的法规框架。

具体到个人信息保护方法, 目前我国寄邮件发件人要实名, 收件人不用实名, 建议网购时只留电话和花名、小区楼号就行; 小件自行到快递驿站拿取, 大件送到单元门口。使用移动支付、网银等涉及绑卡业务的, 最好使用一个专用手机。不要在街上参加扫码有礼的活动, 不要浏览非法网站。

非必要, 不要留下个人隐私信息。也不要相信任何想要你卡号、密码、转账信息的电话、短信、通知、APP。一定不要相信天上会掉馅饼。一贪小便宜, 肯定会有损失。犹豫的时候, 最好多问几个人, 小心总没错。

个人金融信息, 怎样才能保护?

热点关注

前一个时期, 信息安全老骆驼写的《一部手机失窃引发的惊心动魄的战争》, 在全国火爆。记者认真读了这篇文章, 真的是触目惊心。

作者是从事信息安全的人, 他的遭遇警察都没听过, 表示不可能。作为大数据小白的小编等, 面对这种情况, 真的是无从下手。

金融信息泄露渠道挺多

楚乔大二暑假回到太原, 联系了一家外资银行实习。银行在太原当地没有对私业务网点, 领实习补助需要开立一个国内银行的账户。楚乔就到某国有大行办了一张卡。

很快, 第三天开始, 她的手机就收到各种信息, 接到各种推销商铺、办理贷款等业务电话。楚乔明白: 自己的信息被泄露了。因为在上大学之前, 她在太原只有一个小时候拿户口本办的存压岁钱的存折, 只能自己到网点柜台存取。上大学时, 学校统一办理的银行卡和录取通知书一起寄到家, 她和妈妈拿着卡和身份证到银行网点办理了网银业务, 方便汇学费和生活费。这张卡在南方用, 回家就不用了。因为是学生, 而且是学校批量办的卡, 楚乔的校园卡并没有给她带来各种信息骚扰, 挺清静。在太原办了卡后, 接到的电话和信息都是推销太原本地的楼盘。烦不胜烦的楚乔, 又一次接到推销电话后, 对着电话直接说: “我知道谁泄露了我的个人信息, 再打我就举报。”她打了银行客服电话, 反映了情况。然

后电话就安静了。

其实, 个人金融信息的泄露, 不只是银行一个渠道。记者采访了解到, 去年以来, 移动支付使用的范围迅速扩大, 走到哪里都是扫一扫, 现金的使用频率都降低了。除了移动支付扫码以外, 超市门口、小区广场还有很多摆摊展销的商品, 各种兴趣学习培训班, 乃至帮助亲朋好友同事同学到某购物APP上“砍一刀”, 都会有信息泄露的可能。另外, 微信注册可以不捆绑银行卡, 但支付宝注册必须捆绑银行卡, 一不小心, 也有漏洞。而且大数据下几乎没有秘密, 手机失窃后, 捆绑银行卡的网银、移动支付捆绑的银行卡、云支付捆绑的银行卡, 还有各种购物平台捆绑的银行卡, 都会被专业窃贼攻破。

银行加强个人信息管理

平心而论, 从银行的角度来说, 一般以中老年人居多。疫情常态化后, 他们好不容易被逼学会的手机操作能力日趋下降。在渤海银行迎泽支行的客户群里, 12月2日一个客户问杨威: “自己操作, 不知道到期利息是多少, 从哪里能看到?”杨威表示买的什么产品、多久、利率都不清楚, 不好计算。这位客户立即就把截屏发到了群里, 杨威赶紧说, “这是个人隐私, 不建议发到群里。你到行里办业务, 专业理财人员可以提供服务, 还有纸质单据留存。”大家在群里发出了不同大笑的表情。

记者了解到, 各种事件之下, 商业银行对客户的信息管理越来越严。浦发银行太原分行信息科技部付旭表示, 分行年初就分别与43家部门和分支行负责人签署了信息安全目标责任书, 建立健全分行信息安全组织体系, 信息安全人员队伍渗透到最基层, 确保每个网点都有信息安全人员可以及时处本网点的信息安全事件。截至目前, 今年进行了17次信息安全检查。在数据防泄漏方面, 该行部署了数据防泄漏系统, 对邮件外发、打印等相关功能严格管控, 确保行内信息不泄露到行外。对蓝牙、USB严格管控, 有效防止信息不通过蓝牙及USB插口泄露到行外。付旭说: “针对软硬件漏洞和监管机构、总行下发的安全漏洞预警, 我们及时修复; 对重要的生产系统, 先在测试环境测试无误之后再到生产环境中实施, 确保不因补丁的兼容性出现生产性问题。同时, 银行的办公网及业务网严格隔离, 在重要节点部署防火墙及IDS, 从网络上杜绝不安全事件发生。”

我省最大的省属地方性法人银行——晋商银行, 以科技化的引领、系统化的防控手段, 在维护消费者金融信息安全方面做了大量细致有效的工作。该行在网络安全防护体系建设过程中, 同步规划、同步运行网络安全保护、保密和密码保护措施, 定期监测并堵塞系统存在的技术漏洞等安全隐患。筑牢信息保护的各级防线, 从数据管理、征信信息安全、个人客户金融信息安全等方面, 对接触消费者金融信息的岗位人员合理设置权限, 并采取内部审批等有效措施进行权限控制。同时加强员工教育, 有效防范金融信息的操作风险。



我省金融机构防止金融诈骗宣传活动现场。 本报记者 王昕 摄

晋中银行也同样有自己的一整套制度, 保护客户信息安全。

……

必须强化自我防范意识

个人金融信息虽说是消费者个人的信息, 但也是国家金融信息的组成部分。金融机构在做好自己的工作, 努力确保信息安全的同时, 作为金融消费者的我们个人, 其实也有事要做。

记者采访到的银行人员首先强调的就是每个人都要有自我防范意识。比如银行办理业务, 柜台有一米安全线, 别人办业务不凑近看, 自己办业务也要避免被别人看到细节。尤其是在行外自助机器上操作, 更要注意保护信息安全。其次, 就是保护好好自己的移动支付各种密码, 手机里最好不要有身份证照片、社保卡照片。手机的开机密码和手机银行密码以及移动支付密码不要设置成生日, 防止手机丢失后容易被不法分子破解盗刷。再次, 就是更保险的做法了。付旭说, 很多非金融机构的政府职能部门APP, 一年也就用很少的几次, 他们不是金融机构, 对个人信息的保护要求不高, 不用了在本上记录了登录号、登录密码后就卸载, 用时再下载, 既节约内存也比较安全。各种日常应用的小

程序和APP, 比如预定酒店和买机票的网站和APP, 也可以轻易获得身份证号码信息; 移动支付时最好不要设置免密支付, 还是自己输密码支付安全, 否则被盗刷后连个提醒都没有。目前有的银行账户变动也是自动设置多少元以上才给短信提示或者微信提示, 麻烦一点, 直接设置为只要变动就提示, 哪怕一分钱。另外, 很多非银行的支付机构基本上允许用不同手机号码注册相同实名认证的支付账户, 允许两个账户绑定一张银行卡, 也增加了个人金融信息泄露乃至资金被盗窃的概率。

还有一个最关键的地方就是, 现在手机里承载的内容太多, 不仅仅是手机要设置屏幕锁, 手机卡也要上密码, 这样手机丢了, 别人拿上手机卡也不能插到其他手机上用。付旭最后强调, 万一丢失了手机或者银行卡, 第一时间就是冻结挂失手机卡和所有银行卡, 换掉所有银行卡的预留手机号码。

自我防范, 正确保护自己的金融信息安全在今天无比重要。为此, 很多银行在金融消费教育时会指导大家如何做。作为个人, 有时间还是学习一下比较好, 万一不小心丢了手机的是自己, 又没有信息安全老骆驼的本事, 只能干着急上火, 还不如现在防患于未然。

银行开户还管手机号码?

近日, 因为单位要开一个银行账户, 省城太原的周女士很是抓狂。

因为有一笔业务, 合作方需要周女士所在单位要开一个J银行的账户。周女士向领导汇报后准备去开。

周女士来到了离单位最近的一家J银行, 按照要求该拿的东西都准备好了, 银行员工也上门服务, 当着单位领导的面把单位开户需要做的双录工作都做了。接下来就等着办理开户手续了。没想到开户事宜进展不顺。

银行工作人员在开户过程中发现周女士单位的证件有点小问题, 具体是什么不能确认, 因为银行系统只显示不匹配。周女士和同事开始了“破案”般的工作: 基本户开户许可证、法人的证件以及公司开立章程与决议和各种印章肯定没有问题, 有问题的应该在营业执照方面。具体是什么? 和银行人员沟通了解到, 也许是营业执照信息有问题? 周女士联系了市场监管局的同学, 同学分析有可能是法人在市场监管局留的信息有问题。周女士同时还咨询了在银行工作的同学, 同学说, 这种情况一般是法人登记时留的电话是单位座机。央行有规定要求必须留手机号码。周女士到市场监管局把营业执照留底信息里的单位座机号码变成了法人手机号码。银行系统还是不能通过。之后, 银行问: “单位领导的手机号码是不是他自己身份证实名认证的呢?”周女士简直要抓狂。

无奈之下, 12月4日去省城大南门移动营业厅把领导的手机号码和身份证再做核实——原来, 手机号码是用一代身份证办理的, 那时是15位号码, 现在身份办理的是18位的二代身份证号码。能变更的都变更了, 银行系统还是过不去, 说需要打一张领导的话费单。周女士心急如焚, 12月7日中午跑到移动营业厅, 把身份证一放一扫就行, 我们系统没问题。周女士把电子单据发给了银行工作人员, 探讨也许是移动公司的系统和银行的系统对接有个时滞效应, 又正好赶上5日和6日是周末, 看看再说。

就这样, 单位银行开户事宜前后加起来7个工作日跨了两个周末10天还没办完, 周女士急得满嘴是泡。

针对周女士“银行开户还管领导手机号码是不是自己实名?”的灵魂拷问, 浦发银行信息科技部总经理任永胜告诉记者, 央行216号文件明文规定建立单位开户审核核实机制, 要严格联系电话号码与身份证件号码的对应关系等。而且, 目前银行在对公开户环节都上了一键查询功能, 和移动通讯运营商以及市场监管、公安、税务等部门联网, 确定开户人是不是本人使用的手机号, 确保开户信息安全, 从而有效防范电信诈骗, 避免反洗钱等。

虽然银行开户还没有办成, 但是在办理进程中, 周女士感受到了目前银行等机构对信息管理确实比较严格。通过各种补充、更正信息的忙碌, 也把单位在一些职能部门的基础信息完善了, 以后再办别的业务, 不会有今天的“麻烦”, 从这个角度来看, “破案”值得, 奔波值得。

信息安全人人有责

评 论

大数据下虽说没有秘密, 但是数据信息安全人人有责。在做这一组稿件的过程中, 记者采访发现除了银行工作人员和专业信息安全人员外, 更多的群众对于个人信息安全的泄露渠道还是不太了解, 大家觉得只要不把银行卡密码泄露就高枕无忧。

事实上, 银行卡的密码设置一般银行工作人员都会提醒不要设置为出生年月日, 有的银行甚至明文规定不得设置出生年月日, 这是最基础的信息安全。除了银行卡外, 手机的开机设置也比较简单, 更有人嫌麻烦给银行卡设置了免密支付, 200元以下闪付。还有的人手机银行捆着几乎所有身家, 一旦手机丢失, 损失惨重。

说信息安全人人有责, 有的人觉得不是自己的事儿, 涉及个人信息的部门, 比如银行、通讯公司、网购平台、支付平台就应该为客户保守秘密。没错, 他们有义务有责任保守秘密, 但是架不住坏人, 有知识有文化懂大数据业务, 你自己一不小心有漏洞信息泄露了, 怎么办? 可以这样理解, 财产安全人人有责, 信息保护最为基础。

本版稿件均由本报首席记者崔晓农采写