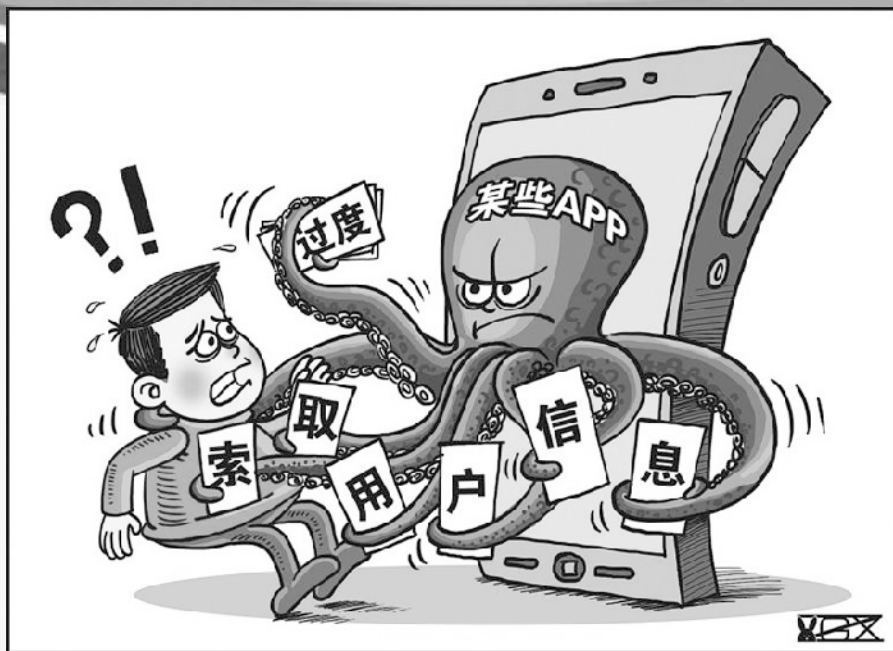


打开手机的应用程序(以下称APP),输入18位社会保障号、姓名、8位查询密码、登录密码、手机号,你所有的个人信息有可能出现在别人的电脑后台上。

这是曾发生在央视“3·15”晚会上的一幕,主持人通过一款名为“社保掌上通”的APP注册并进行社保查询,现场模拟了个人信息被远程截取的全过程。专家称,该社保查询APP暗含多项不合理条款,强制、过度索取用户隐私,如“您同意并授权我们使用您的社保账户密码”及“模拟您登录网站获取您的个人信息”等。但用户注册后,其个人信息却被发往某大数据公司的网站,并且这一切是发生在用户毫不知情的状况下。

需要注意的是,类似“强制索权”、违法违规收集个人信息的APP并不少见。



“疯狂”索取

新华社发 翟桂溪 作

对APP“强制索权”说不

没有电话业务,为何要电话权限

国家互联网应急中心发布的《2019年上半年我国互联网网络安全态势》显示,今年上半年,国家互联网应急中心通过自主捕获和厂商交换获得移动互联网恶意程序103万余个,通过对恶意程序的恶意行为统计发现,排名前三的分别为资费消耗类、流氓行为类和恶意扣费类。

国家互联网应急中心监测分析发现,在目前下载量较大的千余款移动APP中,每款应用平均申请

25项权限,其中不少APP与电话业务无关,却申请拨打电话权限,数量占比超过30%。在个人隐私方面,每款应用平均收集20项个人信息和设备信息,涉及社交、出行、招聘、办公、影音等各方面。此外,大量APP有探测其他APP信息、读写用户设备文件等异常行为。

隐私的“钥匙”不要说给就给

当APP越界收集用户的隐私信息时,这对用户个人信息安全造成的威胁不容小觑。因此,消费者

应增强安全意识,加强对APP索权的重视程度,审慎对待APP索要的每一项授权。但不同类型授权的背后,究竟隐藏着怎样的风险?对此,记者进行了简单的归纳整理。

如若授权APP读取位置信息,一旦位置信息被不法分子利用,或导致财产盗损甚至引发人身伤害;如若授权APP读取存储设备权限,重要文件、隐私照片有可能泄露;如若授权APP读取电话权限,就有可能被查看和修改通话记录、查看本机号码及设备ID,APP还可能获取通话状态和正在拨打的电话号码,甚至直接挂断电话;如若授权APP通讯录功能权限,APP可能会读取、修改通讯录,这样联系人的信息可能泄露;如若授权APP短信功能权限,那么APP可能会收发、读取和删除短信,用户进行银行转账、网站登录的验证码也可能被读取,容易造成财产损失;如若授予获取摄像头、麦克风权限,那么用户打开设备的摄像、拍照、录音功能时,APP可能会窥探用户生活隐私。

总之,对手机用户而言,一定要“长点心”,尽可能地保证个人隐私信息的安全,然后再享用APP带来的便捷。互联网企业要认识到,无底线的“强制索权”不仅有违商业道德,而且违法违规,应确保相关应用索取的权限与功能相匹配,并妥善使用这些权限,避免伤害用户权益。

举报信息近8000条,百余家企业须整改

一些网站和APP“强制索权”“过度索权”、超范围收集个人信息,有的APP甚至向用户索要70余项权限,而一旦被拒绝,整个应

用都将无法使用。某些软件开发者的“蛮横”行为激起用户的不满,也引起了有关部门的重视。

近日,由中央网信办等指导举办的“2019年网络安全博览会”展示了今年1至9月中央网信办等4个部门开展APP个人信息保护专项治理工作的成果,其中就包括近600款APP的违法违规使用个人信息评估和处理情况。

中央网信办网安局一级巡视员兼副局长杨春艳提到,针对当前APP“强制索权”“过度索权”、超范围收集个人信息、违法违规使用个人信息等问题,中央网信办起草了《APP违法违规收集使用个人信息行为认定办法》、国家标准《移动互联网应用(APP)收集个人信息基本规范(草案)》等系列制度文件。

此外,就目前APP专项治理行动取得的阶段性成果,杨春艳表示,今年1月以来,中央网信办、工信部、公安部、市场监管总局联合开展了一系列综合治理活动:指导成立了APP专项治理工作组;设立了举报平台,建立了专门针对APP违法违规收集使用个人信息的举报渠道,至今已收到近8000条举报信息,其中实名举报占到近1/3;将400余款下载量大、用户常用的APP纳入了评估,向100多家APP运营企业发送了整改建议函,评估发现的问题得到整改落实;通过微信、网站等渠道加大宣传普及力度,配合央视“3·15”晚会等对典型APP违法违规收集个人信息行为进行曝光,其目的是为了促进APP运营企业加紧整改。

“目前这项工作还在加紧推进,我们将继续完善相关文件标准,加大治理力度,不断提升APP个人信息保护水平。”杨春艳表示。

(据《人民日报海外版》)



“贪心”

新华社发 程硕 作