2014年1月28日,手机游戏“愤怒的小鸟”应用截屏

“六招”教你防手机泄密

美国媒体27日报道,据美国“棱镜”监视项目曝光者爱德华·斯诺登提供的文件显示,美国和英国的情报机构早在2007年开始,便利用“愤怒的小鸟”、谷歌地图等热门手机应用软件搜集用户个人信息。这些情报搜集工作理论上可涉及全球约10亿智能手机用户,他们在智能手机上使用的地图、游戏和社交软件有可能被美国国家安全局和英国政府通信总部利用。

当网络成为社会普遍的生活方式后,个人信息的流动性和暴露风险大大增加,而大数据更是令这种隐患的危险性以几何级数增加。只要用户使用智能手机,他就必须在已知或者未知的情况下,将个人信息暴露在外泄的风险之下。要应对这一前所未有的新风险,无论法律层面还是技术层面,都亟待在“亡羊”之前,及时“补牢”。

A 六招预防手机泄露个人资料

1.玩游戏时把手机调成飞行模式

大部分手机游戏软件不需要连上互联网就能运行,而其配套的广告则需要。因此,打游戏时通过把手机调成飞行模式断网,就能阻止广告自动显现,也能阻止你的个人资料外泄。

2. 用虚拟专用网络(VPN)上网

虚拟专用网络(VPN)能够对所有来往手机的数据加密。使用VPN不能阻止手机软件商和广告商搜集和传送你的个人信息,但是却能增加黑客或间谍监视这一数据传送过程的难度。从苹果的App Store或者Google Play Store就能轻易下载例如Hotspot Shield或者VPN Express之类的VPN软件。

3. 最好不要用手机发微博

首先,尽量不要用蜂窝数据网络发微博。相反,应该在手机处于安全、有密码保护的网络环境下,例如在家里的WIFI时才发微博或在其他社交网站上发布个人信息。事实上,最好不要用手机发微博,而是用个人电脑或笔记本电脑发微博。

4. 关掉WIFI检索、GPS定位功能

手机上的WIFI检索、GPS定位等功能能够很快地定位你身处的位置。你可能需要进入每一个软件的设置功能里面去关闭其定位功能,不过记得先关掉那些有拍摄功能的软件的定位功能。除非很必要,否则不要轻易使用这些功能。这样,间谍和黑客就不能通过软件数据获悉你身处的位置,或者你去过的地方。

5.关掉蜂窝数据网络

如果你不需要在路上随时收发电子邮件,那么最好关掉蜂窝数据网络,等到在安全的WIFI情况下再上网。关掉蜂窝数据网络后,手机还能如常收发短信和打电话,电池还更耐用一些。

6.干脆别用智能手机

如果你想走极端的话,不妨返璞归真,把你的手机“降级”为2007年或以前出产的“傻瓜”手机。所有的手机都可能被追踪,但是很显然,那些无法登录微博或者玩“愤怒的小鸟”的手机,会更难泄露个人资料。

B 大数据时代 隐私泄露成隐患

互联网技术的高速发展令人类社会步入“大数据”时代,个人信息的网络化和透明化成为不可阻挡的大趋势。过去,能够大量掌控公民个人数据的机构只能是持有公权力的政府机构,但在人类社会进入大数据时代的今天,许多商业机构甚至部分个人也可能拥有海量数据,传统的个人信息保护方式不再奏效。

相较于传统的个人电脑,手机由于具有即时性和随身性等特点,更能暴露个人隐私。不知不觉中,用户的个人信息悄悄地被政府机构、企业甚至个人搜集和利用。因此,泄露个人隐私成为智能手机最大的安全隐患。

只要用户使用智能手机,他就必须在已知或者未知的情况下,将个人信息提供给服务商,差别只在于提供个人信息的多少。更复杂的是,由于多重交易以及多个第三方渠道的介入,个人信息以辐射方式外泄,用户别说掌控了,甚至可能连个人信息如何外泄都不知情。

通常,智能手机包含的个人信息包括位置信息、联系人、通话记录,甚至银行账户信息和购买记录等,这些信息涵盖用户生活各个方面,且高度敏感,盗取价值更大,一旦泄露,可能会严重损害用户利益。

无论是通过微博、微信等社交平台“晒”心情,或者关注、评论他人,或者通过手机支付网购,这些操作都存在泄露个人信息的可能性。因此,用户常会莫名其妙地受到推销信息和垃圾短信的骚扰,甚至被伪装成好友的犯罪分子诈骗,却不知道问题出在哪个环节。

当网络成为社会普遍的生活方式后,个人信息的流动性和暴露风险大大增加,而大数据更是令这种隐患的危险性以几何级数增加。要应对这一前所未有的新风险,无论法律层面还是技术层面,都亟待在“亡羊”之前,及时“补牢”。

相关链接

“愤怒的小鸟”如何泄密?

很多人并没有意识到,当他们在使用智能手机听音乐或者玩“愤怒的小鸟”的时候,这些软件可能正在把用户的个人信息传送给软件制造商,而且,软件里还可能暗藏广告商安插的追踪技术。这令活泼可爱的“愤怒的小鸟”,瞬间变身为监视甚至窃取个人信息的“老大哥”。

美国《华尔街日报》在2010年对101个iPhone和Android手机软件进行调查,结果发现,这些软件大部分都会把手机的“独特身份证号”——即手机序列号以及用户所在地传给广告商。更有甚者,在此之后,广告商进一步搜集更多手机软件用户的资料。

掌握手机序列号后,广告商则可以通过多个软件的使用,摸索出特定用户在使用手机软件及用手机上网时的喜好、特征和习惯,甚至连用户的常住地、收入、爱好、性取向和政治立场都能摸得一清二楚。

美国国安局如何利用?

通过全球私人手机网络,美国国家安全局或者英国政府通信总部等机构可以截取用户的大部分个人信息。而且,由于手机序列号的缘故,这些信息被打上个人标签,因此,需要的话,美国国家安全局完全可以掌握你目前所处的位置。

当然,美国国家安全局虽然有能力掌握手机用户的个人信息,但除非与调查有关,否则不一定会仔细查看这些信息。美国国家安全局在27日的一份声明中说,他们对“非有效外国情报目标”不感兴趣,强调“任何暗示国家安全局对外情报搜集针对美国人日常使用智能手机或社交媒体通讯的说法都不属实”。

美国国家安全局还称,他们会“精简”甚至“丢弃”所拦截到的美国常住居民的个人信息。但是,该局的“精简规则”允许其保留怀疑目标或者协助调查人士的个人信息。

据《广州日报》

日本将制定武器出口新原则

日本首相安倍晋三30日在国会答辩时声称将制定新的武器出口原则。

安倍在回答公明党党首山口那津男质询时说,要在充分考虑“武器出口三原则”作用基础上制定新的武器出口原则。新原则应顾及以下几点,即对于禁止向他国出口的武器作出明确规定;对于可以出口的武器实施严格审查;确保对转移至第三国的武器进行妥善管理等。

1967年,日本颁布实施了“武器出口三原则”,即禁止向社会主义阵营国家、联合国决议规定对其实施武器禁运的国家,以及国际冲突的当事国或有冲突危险的国家出口武器。1976年,三木武夫内阁对上述原则进行增补,实际上全面禁止了武器出口。但此后,日本政府多次以发表“内阁官房长官谈话”形式打破“武器出口三原则”,允许日本与他国共同研发、生产武器。

据新华社

日自卫队表演机空中刮蹭

日本自卫队一名发言人29日证实,航空自卫队飞行表演队的两架飞机当天在飞行训练过程中发生刮蹭,随后均安全着陆,没有人员受伤。

这两架飞机隶属日本东部宫城县东松岛市松岛基地的“蓝色冲击波”飞行表演队。当地时间29日11时25分左右,两架T-4型教练机在位于基地东南方向约45公里的太平洋上空训练时发生刮蹭,随即返回基地降落。

事发时,飞行表演队共有4架飞机进行编队训练。两架发生刮蹭的飞机内共有3名飞行员,均未受伤。

共同社发布的照片显示,其中一架飞机机头凹陷。自卫队发言人确认,另一架飞机的稳定器部分零件脱落。 据新华社

美联储再削减月度购债规模

美国联邦储备委员会29日宣布,由于美国经济继续改善,将从2月开始再削减月度资产购买规模100亿美元。

美联储当天在结束货币政策例会后发表声明说,考虑到就业市场已取得的进展和经济前景的改善,决定从2月起继续削减月度资产购买规模,将长期国债购买规模从400亿美元降至350亿美元,将抵押贷款支持证券购买规模从350亿美元降至300亿美元。这样一来,美联储月度资产购买规模将从此前的750亿美元缩减至650亿美元。

据新华社

菲律宾一监狱182名囚犯越狱

菲律宾警方30日说,该国中部莱特省一监狱的182名囚犯当天凌晨集体越狱逃跑。

菲律宾东米沙鄢地区警方负责人亨利·洛萨内斯说,关押在曾受台风“海燕”袭击的莱特省帕洛镇监狱的182名囚犯30日凌晨趁看押人员出去喝咖啡时逃离监狱。该监狱共囚禁431名囚犯。其余人因被监狱看押人员发现而未能逃脱。

洛萨内斯说,他们已抓回150名逃犯。目前,正全力搜捕其余逃犯。 据新华社