zhi liao 知了

主笔:于梅君

隐私“刺客”

仅凭一个手机号竟能泄露那么多信息

最近,话题“注销手机号等于出卖自己”一度冲上热搜榜。仅凭一串实名手机号,就能顺藤摸瓜,查到一个人几乎所有的私密信息。

除了手机号注销带来的隐患,你随手拍的照片,可能暴露你的位置,和人聊天提起的内容,手机APP很快就会进行相关推送……我们的隐私是如何泄露的?大数据时代,该如何避免信息裸奔?

换手机号前一定要做的事

❶解绑银行卡

◎及时与手机号所绑定的银行卡、发卡行联系,变更绑定的手机号,保障账户安全。

❷修改各类网站APP绑定的手机号

◎及时更换微博、微信、支付宝、QQ等账户绑定的手机号。

❸修改购物网站资料

◎更换手机号后,记得修改收货信息里的电话号码。

❹妥善处理原手机卡

◎变更手机号后,原手机卡仍会保留联系人、短信等个人信息,一定不要随意丢弃,以免泄露个人信息。

❺通知亲友手机号已变更

◎及时通知亲友手机号已变更,方便联系的同时,降低亲友被骗的风险。

❻及时销户

◎带身份证件到营业厅办理销户,不要随意丢弃不用的手机卡,以免被不法分子捡到,冒用身份实施诈骗。

❶ 手机号难断“前缘”麻烦多

在实名认证的当下,手机号往往关联了用户个人信息、消费数据、财产账号及密码等内容,“一号查万物”“一部手机走天下”的说法并不夸张。

近日,安徽省铜陵市公安局民警“徐督督”发布科普视频表示:“注销手机号等于出卖自己,随手注销的手机号很可能造成财产损失。注销的手机号会被运营商重新投入市场。下一个用你手机号的人,可以用手机验证码登录你的支付宝、微信等各类软件,后果不堪设想。注销手机号时不妨多做一步,将绑定此手机号的软件统统解绑,银行卡预留的手机号也一定要修改。”

被注销的手机号,真的会重新回流市场吗?运营商均表示,根据国家规定,所有号码都是循环利用的,但用户的手机号注销后,会有90天的冻结期。期限过后,才能被重新投放“号码池”。用户的手机号注销超过90天就无法再找回,手机号被新用户激活后,新用户无法查询原主人的缴费详情等记录。

不过,手机号注销后,与其绑定的银行卡或软件并不会自动解绑。所以,新用户有可能登上原手机号没解绑的软件、银行卡或支付宝等,危及原主人的利益和安全。

目前市面上的社交软件,几乎都要绑定实名手机号注册,并且会默认开通“通讯录添加好友”功能。

拿微信举例,如果你设置了可通过手机号添加微信,那不管你是拒绝还是通过好友申请,对方都可查询到机主的微信昵称,并且很多人的习惯是,所有社交帐号都是同一套ID名称和密码,所以,只要解锁一个,就可能获得“个人信息套餐”。

一些启用了旧号码的新机主,有时也会遇到麻烦,甚至会“被继承”前机主的网络资产、负债甚至犯罪记录,成了“背锅侠”,给生活带来极大困扰。

❷ “一键解绑”真的那么难?

如今手机更新换代频繁,很多人不只拥有一两个电话号码,有些号码及绑定的业务,自己都已记不清。那么,该如何查询本人名下有多少个号码?

业内人士提醒,既可在运营商App里搜索“一证通查”进行查询,也可由本人携带身份证到营业厅查询。如果新办的号码在使用过程中,收到未注册过的APP、网站等发来的短信,要提高警惕,拨打相应APP、网站等客服电话进行咨询。

如何查询手机号过往绑定的业务?目前,工业和信息化部已推出“一证通查”功能。

用户可通过工业和信息化部微信公众号“工信微报”“工信部反诈专班”,“中国信通院”微信公众号及支付宝“一证通查”小程序等,查询名下手机号关联的互联网账号。

如果发现本人手机号关联的互联网账号,与查询结果不一致,可在“一证通查”页面点击“解绑与明细查询”,如果对查询结果存在异议,可以拨打企业客服电话咨询。

专家表示,把手机号的回收利用当成严肃的事对待,十分必要,目前,虽然有关方面推出“一证通查”功能,并提供解绑服务,但“一证通查”只是覆盖主流APP,并未覆盖所有APP。

也就是说,“手机号码绑定了多少APP”这个痛点,并没得到有效解决。因此,相关部门应尽快实现更加完善的“一键查询”和“一键解绑”功能。

话说回来,如果真的忘了注销手机号,真的会出现财产损失吗?答案是,有可能,但也不必过于担心。

目前,很多常用App,像微信和支付宝,当账号在一台从未登录的手机上登录时,都需要“双重验证”。微信需要用原手机扫描二维码或找微信好友来验证。支付宝需要输入身份证号后四位。

大部分银行客户端,采用的登录方式则是“用户名+密码”,而不是简单粗暴的“手机号+验证码”,这些措施,对个人财产安全也有一定保障。

❸ APP会“偷听”我们聊天吗?

你是否有过这样的经历,刚刚说完某个东西,不一会儿,手机就会推送给你相关内容。无论聊什么,手机好像都能“听到”,如此细思极恐的现象,让不少人担心:手机APP真的会“偷听”吗?

这种担心不无道理。一项来自浙江大学、加拿大麦吉尔大学的最新研究显示:部分智能手机APP,可在用户不知情且无需系统授权的情况下,利用手机内置的加速度传感器,采集手机扬声器所发出声音的震动信号,实现对用户语音的窃听。

对此,清华大学人工智能国际治理研究院副院长梁正表示,目前“聊什么推什么”,主要还是基于大数据的用户画像,能让商家摸清你爱吃辣还是吃酸,并通过算法,把更符合你口味的餐厅排序靠前。

梁正表示,在技术上,APP虽然确实可以实现“偷听”,但目前通过分析实时语音信息来推送商品的技术,并不容易实现。因为以现阶段AI发展水平来看,想要在“偷听”的同时,理解、概括人类语言,并进行精准推送还比较困难。

APP治理工作组技术专家何延哲也表示,目前还没发现哪款APP,有把用户语音信息上传后的“偷听”行为。不过,虽然网络内容精准推荐,或许并非“偷听”所致,仍需引起各方高度重视。这种类似于“监听”的技术一旦被滥用,将严重威胁所有消费者的隐私安全。

为防患于未然,用户可在手机操作系统的权限设置里,找到麦克风权限,检查目前有哪些APP被授权使用麦克风。根据需要,可随时关闭对APP使用麦克风的授权。

何延哲还介绍,在对市面上的APP进行检测时,发现很多APP存在隐私政策篇幅长、用户难读懂、账户无法注销等问题。比如一款壁纸APP,隐私政策竟然有一万多字。

工信部多次通报,不少APP存在违规收集个人信息,强制、频繁、过度索取权限。在下载量较大的千余款移动APP中,每款应用平均会申请25项权限,其中申请与自身业务无关权限的APP超过30%。因此,在安装APP时,不要贸然给APP全部权限,如读取通讯录、短信、相册、位置信息等。

❹ 输入法、剪贴板也能泄密

一般来说,我们手机里的APP有很多个,但常用的输入法就一个。如果你通过输入法输入的内容,经常会有不同的APP给你推荐,这或许就是输入法将信息共享的原因。

一些输入法在安装时,会在用户协议里,要求用收集到的信息,向用户提供定制内容,展示个性化的内容或广告,从而造成个人信息泄露。

2021年,国家网信办曾发布33款APP违法违规收集使用个人信息情况,被广泛使用的讯飞、搜狗等五大输入法就赫然在列。

如何保护隐私?建议使用手机原装的输入法。如果使用第三方的输入法,可以关闭其智能推荐和个性化推荐功能。

在玩手机时,我们有时会使用复制或剪切功能。手机剪贴板就像一个中转站,在使用这一功能时,接触一些隐私信息是不可避免的,比如你的账号密码、个人收货地址、聊天记录等,这就让一些APP和第三方软件开发包有机可乘,导致信息泄露。

如何保护隐私?建议定期删除剪贴板中剪切的句子;或者在剪贴板设置中,关闭其记录功能。

另外,现在许多支付软件都有免密支付功能,虽然可节省时间,但也增加了账户被盗刷风险,建议关闭免密支付功能,确保账户安全。

很多人在网上发图片时,喜欢以高清原图方式发送。但是,手机拍摄的原图会携带更多信息,包括手机型号、拍摄时间、地理位置等,都可能被他人获取。

所以,拍摄照片时,我们可以关闭手机定位,这样原图就没有地址信息;在网上发图片时,不要勾选发原图的选项,发送压缩图片即可。

知多一点

可怕的偷拍黑产——一个人竟控制18万个摄像头

你站在桥上看风景,无数双眼睛可能正在盯着你……

日前,北京市朝阳区人民法院发布《网络犯罪案件审判白皮书(2019-2023年度)》,其中一起“窥私”案例让人后背发凉。

被告人巫某某通过技术手段,获取了某品牌摄像头的用户名和密码数据库,将其置于自建的APP中,通过指令调取数据库信息,实现入侵并控制目标摄像头。

巫某某控制的摄像头超过18万个,场所涵盖医院、家庭、养老院、实验室等,宣传“足不出户看世界”,向“客户”收取68元至688元不等的会员费,并提供实时监控画面。最终,法院以非法控制计算机信息系统罪,判处巫某某有期徒刑5年,罚金10万元,并没收其违法所得80余万元。

摄像头存在大量系统漏洞,不严格的访问控制,更容易被黑客入侵,加上很多视频数据缺乏加密处理,让许多家庭、酒店隐私信息处于“裸奔”状态。在部分社交平台和论坛中,只要支付两三百元,就可看到陌生人家里的实时监控画面……

保护个人隐私,切断摄像头窥私黑色产业链,已成为摄像头行业,甚至是网络空间迫切需要解决的问题。