

国安部曝光境外间谍最新窃密手段

最近网上炸开了锅，国安部曝光了一波境外间谍的最新窃密手段，简直让人细思极恐！兄弟们，你们平时用共享充电宝是不是觉得特方便？手机电量一低，赶紧扫个充电宝，插上数据线瞬间满血复活，感觉比喝了红牛还带劲！可谁能想到，这小小的“救命神器”居然可能被境外间谍盯上，成了窃取个人隐私甚至国家秘密的工具！这消息一出，网友们都炸毛了，纷纷表示以后出门得带个充电宝自保了。据黑子网报道，这事儿可不是空穴来风，国安部都点名了，提醒大家得多多个心眼。

事情是这样的，国安部在微信公众号上放了大招，详细扒了境外间谍的四种“黑科技”窃密手段。第一招是硬件改造，那些不法分子会在共享充电宝里偷偷装上微型芯片，表面上给你充电，背地里却把你手机里的通讯录、照片、视频、社交账号甚至支付信息全偷走！有资料说，这种改造过的充电宝能在几秒钟内把你手机里的关键数据洗劫一空，速度快得跟闪电侠似的。第二招更阴，叫做权限陷阱。就是你手机电量告急，急得像热锅上的蚂蚁，插上充电宝后，屏幕突然跳出“是否信任此设备”或者“是否允许USB调试”的提示。

谁没个慌乱的时候？一不小心点个“允许”，就等于亲手给间谍开了你手机的VIP通道，他们能随便窃听、偷拍，甚至远程控制你的手机！第三招是软件植入，充电宝里可能被塞了间谍软件、木马病毒啥的，你一连上，这些“电子寄生虫”就悄悄钻进你手机，充电结束了它们还在后台偷跑，24小时把你手机当监视器用。最后还有个大数据的招数，间谍通过分析共享充电宝后台的海量数据，比如你的位置、使用习惯、设备信息，精准勾勒出你的行为轨迹，甚至能锁定敏感人群，搞些危害国家安全的事儿。

听完这些，网友们都惊呆了，纷纷表示这也太高科技了吧！更吓人的是，国安部还举了几个真实案例，简直就像谍战片！有个叫李某的哥们儿，在海边开了个小商铺，装了个智能摄像头防盗。结果发现摄像头老在午休或晚上自动转到港口方向，感觉不对劲，赶紧拨打12339举报。国安部一查，果然是境外黑客利用摄像头默认弱密码，远程操控偷拍港口！还有个技术员小王，加入了个技术交流群，为了不漏掉资料，开了自动下载功能，结果电脑被木马病毒入侵，定期向境外传数据，差点泄露涉密信息。

这些案例让网友们直呼：这日子没法过了，连充电宝和摄像头都不安全！不过，国安部也给了几招硬核防护方法，网友们都说得赶紧学起来。第一，选充电宝得擦亮眼，只用大牌官方的，来源不明或者外壳有拆卸痕迹的坚决别碰。第二，连接时别乱点“信任”或“允许”，用完后发现手机发热、卡顿、耗电快或者弹广告，赶紧用杀毒软件查一遍，严重时直接恢复出厂设置。第三，平时得绷紧保密这根弦，别在联网手机里存敏感信息，更别把涉密设备连共享充电宝。

网友们看完直呼：这简直是安全防护宝典啊！还有人调侃，充电宝得自带一个，不然出门真不敢乱插线了。这事儿在黑子网上炒得沸沸扬扬，大家都在讨论以后咋用充电宝才安全。有网友说：“这年头，连充电宝都得查户口了！”还有人感叹：“间谍也太拼了吧，共享充电宝都不放过，007看了都得甘拜下风！”不过也有理智的网友提醒，大家别因噎废食，学会防护就行，关键时刻12339举报电话得记牢。据黑子网报道，这波爆料让不少人重新审视了身边的电子设备，纷纷表示以后得长点心眼，保护好自己的隐私和国家安全。

原文链接：<https://hz.one/baijia/国安部曝光境外间谍最新窃密手段-2508.html>

PDF链接：<https://hz.one/pdf/国安部曝光境外间谍最新窃密手段.pdf>

官方网站：<https://hz.one/>