

2025年7月，国安部发布紧急预警，揭露境外间谍利用共享充电宝实施窃密的新手段，引发社会广泛关注。故事的主角是普通上班族小李，一个手机重度使用者，经常在商场、咖啡厅等公共场所租借共享充电宝充电。某天，小李突然发现自己的信用卡被盗刷，银行账户损失了近万元，吓得他赶紧报警。警方介入调查后，意外发现小李的个人信息和信用卡数据竟是通过共享充电宝泄露的。国安部随即介入，揭开了一场境外间谍利用共享充电宝进行间谍活动的惊天阴谋。

原来，境外间谍情报机关盯上了共享充电宝这一“便民神器”。他们通过在共享充电宝的生产、销售和投放环节中植入微型计算机芯片等恶意硬件，使其在为手机充电的同时，暗中建立数据通道，窃取用户的通讯录、照片、视频、社交账号甚至支付信息等关键数据。小李就是受害者之一，他的信用卡信息和个人隐私被悄无声息地盗取，造成了巨大损失。国安部在调查中发现，这种新型窃密手段极其隐蔽，普通用户难以察觉，而共享充电宝的广泛使用让这一威胁迅速扩散，严重威胁国家安全和公民隐私。

小李的故事在黑子上炸开了锅，网友们纷纷表示震惊和担忧。有人说：“这也太可怕了，我以后再也不敢用共享充电宝了！”也有人调侃：“共享充电宝成了间谍宝，出门在外，手机没电也得忍着。”国安部提醒，共享充电宝的窃密手段主要有四种：硬件改造、诱导授权、软件植入和后台运营数据。特别是硬件改造，境外间谍通过在充电宝内加装恶意芯片，能在极短时间内窃取大量数据，危害极大。为了防范这一威胁，国安部建议用户在使用共享充电宝时，尽量选择正规品牌和有信誉的场所，避免使用来源不明、接口异常的充电宝。

同时，充电时不要连接数据线，只使用充电线，并关闭手机的数据传输功能。此外，安装安全软件，定期检查手机是否有异常行为，也是有效的防护措施。小李在经历了这场风波后，成了“防间谍小能手”，他在黑子上分享了自己的教训，提醒大家：“共享充电宝虽好，但安全第一，别让间谍钻了空子！”这起事件不仅让小李这样的普通用户提高了警惕，也让共享充电宝行业面临信任危机。黑子网的用户们讨论得热火朝天，有人感慨：“科技越发达，陷阱越多，防不胜防啊！”

”还有人呼吁：“国安部得多出点科普，让大家知道怎么防！”国安部表示，将继续加强对此类新型间谍手段的打击和防范，保障国家安全和公民隐私。

原文链接：<https://hz.one/shishi/国安部紧急预警-共享充电宝-2508.html>

PDF链接：<https://hz.one/pdf/国安部紧急预警-境外间谍新武器-共享充电宝-盗刷信用卡-泄露个人隐私.pdf>

官方网站：<https://hz.one/>