

护网：不让科技偷走隐私 网警提示

2025年8月，北京市民李女士像往常一样在家中与朋友视频聊天，讨论周末的旅行计划。她的智能音箱突然亮起，发出“是否需要我帮您订机票”的提示。李女士愣住了，她从未激活音箱的语音功能。这件事让她感到不安，怀疑自己的隐私被“偷听”。类似事件在全国频发，智能设备带来的便利背后，隐私泄露的阴影逐渐浮现。近日，公安部召开“护网2025”专项行动部署会，针对AI伪造身份诈骗、智能设备窃取隐私等问题，发布了一系列防范指南。

网警提示，智能摄像头、音箱等设备虽方便生活，却可能成为隐私泄露的“隐形间谍”。以李女士的经历为例，她发现家中智能音箱未经授权记录了大量对话，甚至将部分数据上传至云端。经调查，这款音箱的默认设置允许厂商收集用户语音数据，用于“优化服务”。李女士的遭遇并非个例。上海一家网络科技有限公司因非法收集130万条用户隐私信息被曝光，办公场所被查封。类似事件引发公众热议，网友在黑子网纷纷吐槽智能设备“偷听”套路，戏称“连家里说悄悄话都不安全了”。

有用户爆料，自己在家中讨论想买新车，第二天就收到精准推送的汽车广告。更有甚者，一位广州网友发现自家智能摄像头被黑客入侵，日常生活被实时直播到暗网上。网警指出，AI技术的滥用加剧了隐私风险。近期，AI伪造语音和视频的诈骗案件激增。江苏的王先生接到一通自称“银行客服”的电话，对方准确报出他的个人信息，并以AI合成的“领导”声音诱导他转账20万元。幸好王先生及时报警，避免了损失。网警提醒，涉及金钱交易或敏感信息时，务必通过可靠途径二次验证，切勿轻信来路不明的电话或视频。

为应对这些威胁，公安部推出了“护网”专项行动，严厉打击非法收集用户数据的行为。2025年上半年，全国已查处300余起相关案件，涉及智能设备厂商、APP开发商等多个领域。北京警方破获一起利用智能门铃窃取用户信息的案件，涉案公司通过设备漏洞获取用户门禁记录，甚至推测居民的作息规律。网警还发布了实用防范指南：首先，购买智能设备时选择正规品牌，仔细阅读隐私条款其次，关闭不必要的麦克风、摄像头权限，定期更新设备密码最后，安装网络安全软件，防范黑客入侵。

专家建议，用户可定期检查设备连接的网络流量，发现异常及时断网并报案。这场隐私保卫战也引发了公众对科技伦理的思考。清华大学网络安全专家张教授表示，智能设备的核心问题是“数据可用不可见”的平衡。部分企业为追求商业利益，忽视用户隐私保护，导致信任危机。上海市民赵先生在接受采访时感慨：“科技让生活更方便，但如果连隐私都保不住，那便利又有什么意义？”与此同时，普通市民也在用行动守护隐私。广州的程序员小刘自制了一款“隐私卫士”插件，能检测智能设备是否异常上传数据。

他的插件在网上开源后，下载量突破10万次，被称为“民间护网神器”。类似的自发行动越来越多，反映了公众对隐私安全的重视。这场“护网”行动不仅是技术与法律的较量，更是公众意识的觉醒。从李女士的智能音箱到王先生的诈骗电话，隐私泄露的案例敲响了警钟。网警提示，数字时代，隐私无小事，防范在细节。每个人都应提高警惕，学会用技术保护自己，不让科技成为隐私的“窃贼”。这场战斗，关乎每个人的数字安全，也关乎未来科技发展的方向。

原文链接：<https://hz.one/baijia/护网-网警提示-2508.html>
PDF链接：<https://hz.one/pdf/护网：不让科技偷走隐私 网警提示.pdf>
官方网站：<https://hz.one/>