民有所呼 / 我有所应

点题·报料邮箱:mssd@xmwb.com.cn 线索一旦采用 即付稿酬

家庭智能摄像头、路由器等可能暗藏泄密风险

打造智能家居勿忘扎牢“篱笆”

民生速递

今天是世界电信日，对很多消费者而言，信息通信技术的高速发展为生活带来便利。随着物联网、大数据及人工智能等应用推广，智能家居开始走进市民生活。足不出户，就能感受到智慧生活的魅力。然而，便利背后有隐忧。

一项调查显示，对国内市场上销售的近百个品牌的家庭智能摄像头进行安全评估测试发现，近八成产品存在用户信息泄露、数据传输未加密、APP未安全加固、可横向控制等安全缺陷。很多号称守卫家庭安全的智能家居产品，是否反而可能泄露家庭隐私呢?

■ 保护隐私安全，乐享智能家居 图 CFP

家庭生活可能被网上直播?

前不久，吴敏在1岁儿子的床头安放了一款智能摄像头。在她看来，这款摄像头售价便宜，功能强大，解决了她很多麻烦。“最大的优点是可以用手机实时监控。我上班后，可以随时用手机APP查看孩子在家中的状况。此外，孩子跟我是分房睡的，夜里如果孩子出现磕碰、翻下床等情况，手机APP还会自动发出警报，我也可以回看哪个时段是孩子睡眠情况最差的，能有针对性地想出解决办法。”

记者在采访中发现，不少智能摄像头主攻母婴市场，很受年轻父母的青睐。在电商网站上，智能摄像头的产品多达几万个，价位以100元至300元居多。很多店家都打出了“看娃神器”的宣传语，部分产品除了监控，还有实时记录室内温湿度、空气检测、双向语音对讲等功能。因为用着顺手，吴敏本想在家里卧室也装一个，达到全方位监控的目的，但是最近一则新闻吓坏了她。

近日，一组摄像头拍摄“真人秀”的照片在网站流行，这些照片拍摄场景包括道路、办公室、家庭客厅甚至还有卧室场景。据一名计算机爱好者透露，这些照片来自名为“Shodan”的网站，由于网络摄像头RTSP(实时流传输协议)存在安全漏洞，这家网站收录了成千上万网络摄像头拍摄的照片。

原本希望安装智能监控获得更多安全感，然而，现在却失去了隐私安全感。吴敏现在很纠结，智能摄像头到底用还是不用?

目前在国内上市销售的智能摄像头品牌就多达107个，市场上销售的无品牌的山寨产品更是不计其数，然而由于参与智能摄像头设计生产和推广的相关企业繁杂，品牌众多，其中的很多产品都缺乏完善的安全相关设计，很容易被黑客控制。

安全专家谈剑峰表示，智能摄像头是目前智能设备发展的一个缩影。随着互联网技术和智能技术的发展和应用普及，以互联网化和智能化为核心的智能生活已经从“概念”成为真实可触及的现实。世界正在以超宽带速度进入“万物互联”时代。美国科技行业咨询公司Linley Group曾预计到2020年每一个家庭将拥有大约十个智能联网设备。

“趋势不可阻挡，网络世界没有绝对的安全，除却厂商的自律和安全设限，更重要的是消费者的自我防范。”他认为，消费者在购买时应该多问问，用户数据是否使用强加密算法，访问数据时是否会采用动态令牌认证机制，是否会发送异常登录提醒等。

路由器为谁大开方便之门?

就在几天前举办的全球首个关注智能生活的安全极客大赛上，一家科技团队通过漏洞攻破了几乎市面上销售的所有主流品牌路由器。他们还进一步发现这些存在漏洞的服务被暴露在互联网上，攻击者不需要连入内网就能攻击。通过选手提供的监测数据显示，全球受到影响的路由器达到40万台。

谈剑峰表示，路由器作为家庭的上网入口，连接了许许多多设备，安全性尤为重要。一旦路由器存在安全漏洞被黑客攻破，家里的其他设备就会更容易地被监听、劫持，通过这些漏洞，黑客可以远程入侵控制路由器，在用户下载正规软件时将其替换为植入了木马的后门恶意程序、收发和查看SMS短信、控制手机的电话功能、调用手机摄像头拍照摄像、浏览删除手机文件等。

“虽然目前漏洞很难避免，但是只要保证家庭内网不对外开放，不给不信任的人接入，路由器不对公网暴露，就可以相对安全一些。面对复杂的安全问题，智能硬件厂商应积极应对每一条安全信息的反馈，主动修复产品安全漏洞、不断升级固件，完善路由器软、硬件，从源头堵死漏洞。”

上海市信息安全行业协会副秘书长张凯认为，消费者自身的安全意识还不强。“我们做了一个小型调研，安全因素并不是主导消费者购买智能产品的决定因素，这也导致许多厂商并没有花精力在安全上加大研发，因为一旦更加关注安全，成本就会提高，会影响产品的市场推广力度。”

张凯介绍，目前在信息安全上还没有明确的法律条文，在实践中，调查取证的难度也非常大。“比如智能摄像头拍摄的私照泄密事件，到底是哪个环节引发的，是摄像头本身?上传到云端的云服务泄密?还是路由器被攻击?每个环节都可能出现问题，大部分信息安全案例最终只能不了了之。”近两年，信息安全逐渐被人们所重视，但真要有所改善，还任重道远。

智能家居只是“看上去很美”?

去年以来，智能家居市场异常火爆，不仅许多互联网企业纷纷推出新品，传统家电企业也不甘落后。

点击手机屏幕，智能门锁自动感应解锁；开电灯、拉窗帘也无须自己动手，手机安装应用软件皆可控制；电视、网络摄像头、遥控插座、门锁、灯具、家用警报器和车库门遥控开关等皆可互联，远程操控……智能家居能通过物联网技术将家中的各种设备互联到一起，并且提供家电控制、照明控制、电话远程控制、室内外遥控、防盗报警、环境监测、暖通控制等多种功能。

听上去很美，然后我们的生活真的“智能”了吗?林永江是一家传统家电企业的部门负责人。在实现传统家电智能化转型升级的过程中，他认为遭遇了很多困难。

“智能家居有很大一部分都是基于Wi-Fi的。通过Wi-Fi，你可以控制家中所有设备。但Wi-Fi本身很开放的。传统电器、遥控都是用的红外，隔着一堵墙信号就断了。但Wi-Fi的范围较大，可能你的楼上楼下都能连上，如果不小心让他们获知了密码，逻辑上讲，都可以被控制。”他认为，智能家居、物联网处于发展初期，技术不成熟；企业急于抢占市场，将精力主要放在产品和市场宣传上，还没有将安全问题放到重要日程上。

“有的公司号称安全下了很大功夫，但是一套智能家居系统可能涉及到多个公司的产品，某些安全策略无法彼此兼容，为了控制不同产品，消费者不得不频繁切换应用。目前，还没有一个集成安全包能控制所有智能设备。”林永江认为，家电厂商应该不断突破智能技术相关的门槛，规避一些看似无害的安全陷阱，否则，智能升级不能让家电厂商成功转型，反而是逐步走向衰败。

本报记者 **叶薇**

《2016中国伪基站短信研究报告》出炉

伪基站短信身份冒充类占九成多

民生提醒

根据360手机卫士近日发布的《2016中国伪基站短信研究报告》，从伪基站短信类型看，广告推销类短信数量最多，占比高达41.3%；其次为违法信息类短信占比为33.8%；诈骗短信占比为24%。而在诈骗类短信中，身份冒充类伪基站短信占绝大部分，占比为93.8%，打款诈骗(1.7%)、电商网站欺诈(0.7%)位列其后。

伪基站是相对于基础电信运营商架设的正常基站而言，由不法分子临时搭建，用于实施电信诈骗或扩散垃圾信息的无线电收发设备。伪基站是网络诈骗和非法营销的重要技术工具。它能够搜取以其为中心、一定半径内范围内的手机信号，之后使用任意号码，如冒充公共服务号码，强行向其影响范围内的手机发送短信息，普通用户往往难辨真伪。

伪基站短信在全国具有很强的地域特征。一方面伪基站短信在个别省区如河南、四川、北京等地区数量巨大，这三个省区的伪基站短信占全国总量的1/3以上。另一方面，不同类型的伪基站短信也存在明显的地域差异，“垃圾推广”类短信主要骚扰河南、山东等地区，尤其是房地产类推广短信在山东、河南、河北最多，而色情类短信主要盘踞北京、上海，赌博类短信主要集中在四川、重庆等地，而金融类伪基站短信则集中爆发于辽宁、吉林等地区。

值得一提的是，伪基站短信最多十大城市为北京、郑州、成都、重庆、大连、长春、深圳、上海、沈阳和青岛。大连和长春的伪基站短信拦截量排名甚至高于深圳和上海等IT发达地区。

本报记者 **金志刚**

神器外挂刷钻软件最易“藏雷”

全球近90万部手机感染勒索类恶意软件

延伸阅读

“支付10元给你解锁密码！联系XXXXXX。”手机突然失灵，点哪都没用，只能按屏幕提示付钱解锁，这种被敲诈的情况你遇到过吗?360移动安全团队发布的《Android勒索软件研究报告》显示，自2013年6月首个伪装成杀毒软件的勒索性质软件出现，截至2016年第一季度，勒索类恶意软件在全球范围内已累计感染近90万部手机。

360移动安全团队介绍，手机勒索软件是一种通过锁住用户移动设备，使用户无法正常使用设备，并以此胁迫用户支付解锁费用的恶意软件。这类软件除了能敲诈勒索用户钱财，加密手机文件，破坏用户数据，甚至还能清除手机应用，破坏手机系统。

这些极其“强势”的勒索类软件存在三种表现形式：一，通过将手机触摸屏幕部分或虚拟按键的触摸反馈设置为无效，使智能手机无法通过触摸点击进入其他界面；二，频繁强制置顶某一指定页面，造成手机无法正常切换应用程序；三，更改手机解锁密码，使手机用户无法解锁手机。

对比国内外勒索类恶意软件最常伪装的软件名称可以看出，国外勒索类恶意软件最常伪装成色情视频、Adobe Flash Player和系统软件更新这类软件。而国内勒索类恶意软件最常伪装成神器、外挂及各种刷钻、刷赞、刷人气的软件，这类软件往往利用了人与人之间互相攀比的虚荣心和侥幸心理。

从感染趋势来看，国内勒索类软件在2016年第一季度增长较为迅猛。国内Android平台勒索类恶意软件历史累计感染手机34万部，整个产业链收益逾千万元。

本报记者 **金志刚**