



装个摄像头 可能引来一群人偷窥你家

央视调查显示大量家庭摄像头遭入侵,质检总局称智能摄像头抽检八成存隐患

现如今,很多人家里都装有智能摄像头。下载一个相关联的应用程序,可以随时用手机看看家里的情况。比如老人独自在家是否安全,保姆带娃是否尽责,有没有进小偷之类的。

不过,央视及国家质检总局要给装了摄像头的消费者提个醒:除了你,可能此刻还有成百上千双陌生的眼睛,也在看着你家。

综合 央视



很多人家中装有智能摄像头 资料图片

失联北大女硕士 案情取得重大进展

中国女学者章莹颖在美国伊利诺伊州失联将近十天,她的亲属已抵达美国。中国驻芝加哥总领事馆工作人员引述警方的话说,案件调查取得重大进展,但是没有透露详情。

章莹颖的父亲、小姨和男朋友在美国中部时间17日上午,也就是北京时间17日晚间到达芝加哥。中国驻芝加哥总领事馆的工作人员开车三个多小时带三位亲属到章莹颖做访问学者的伊利诺伊州大学香槟分校(UIUC)。他们之后和警方见面两个小时,了解案件的进展。

中国驻芝加哥总领事馆的工作人员告诉记者,警方称案件调查取得重大进展,但是因为工作的需要,目前不能够透露具体细节。

相关的调查取证工作也还在继续,伊利诺伊州大学香槟分校警方的社交账号发布消息说,FBI悬赏一万美元征集案件相关的信息。截至18日下午,网络筹款平台上为章莹颖家人募集到的捐款已经超过三万美元。

章莹颖的小姨说,相信警方和FBI的工作。这是章莹颖的父亲第一次出国,他对媒体说,能尽快找到女儿,就是最好的父亲节礼物。

据央广之声

东航一国际航班 遇强气流26人伤

18日凌晨,从法国巴黎飞往中国昆明的东航MU774航班在飞行途中突遇气流颠簸,经初步核实机上旅客有26人受伤。目前航班已安全落地昆明,伤员已被送到云南省第一人民医院、昆明市延安医院救治,均无生命危险。

据多名旅客讲述,该航班17日从巴黎戴高乐机场起飞,18日近9时抵达昆明机场。引发事故的气流颠簸发生在18日凌晨3时左右,包括两次剧烈颠簸和多次小的颠簸,前后持续10多分钟。气流颠簸导致不少乘客头部、肩部碰撞到行李架等处,有行李架被撞破裂损坏,还有行李滚落砸到一些乘客。

航班落地昆明机场后,部分受伤旅客被救护车紧急送到云南省第一人民医院救治,部分伤势较轻的旅客由东航中巴车送到昆明市延安医院。云南省第一人民医院相关负责人介绍,截至18日12时,共有28名旅客入院检查,其中4人重伤,8人轻伤,16名旅客经检查无碍后自行离院。另据了解,昆明市延安医院收治了14名受伤旅客。

云南省委、省政府主要负责人对此事作出批示,要求全力做好伤员救治和善后工作。据了解,目前所有伤员生命体征平稳,伤势较重的分别为颅底骨折、颈椎损伤、肩胛骨骨折、头皮裂伤等,其他伤员多为软组织挫伤。

据新华社

网上买软件,记者成功侵入家庭摄像头 QQ群每天更新破解文件

不寒而栗

在QQ搜索栏输入“摄像头破解”,就跳出很多相关聊天群,记者随机加了几个,发现聊天的内容绝大多数有关家庭摄像头隐私,时不时会放出一些号称他人家庭摄像头拍下的画面。很快,不少人主动添加记者为好友,询问是否需要扫描软件,并声称这些扫描软件能够攻破摄像头的IP地址。

只要将被破解的IP地址输入播放软件,就可以实现偷窥,不被觉察。似乎只有电影中的特工或黑客才能做到的事情,竟然可以这么简单地实现吗?记者决定尝试一下,向其中一个卖家支付188元后,记者收到了两款软件和详细的使用教程。

记者在播放软件中,输入卖家提供的IP地址、登录名和密码,竟然成功进入了一个摄像头。这是一户人家,画面显示的是客厅,一只小狗正在窝里睡觉。卖家称,这家住着一对小夫妻,安装摄像头的目的,应该是观看这条宠物狗。

卖家还向记者提供了大量IP账号。为了辨别画面中的影像是不是实时影像,记者再次

登录一个账号,进入了另一个摄像头,放大,缩小,居然真的可以实现远程操作。

而在一些QQ群内,IP地址会被群主作为聚拢人气的礼物,免费向群员发放。在这个近2000人的QQ群中,每天都会新增一份最新破解文件,包含200到400个IP地址,每份都被下载几百次。一位叫“大胆吻下去”的卖家告诉记者,靠卖号当天已赚500多元。

记者找到一个可被攻破的IP地址,并联系上这家主人。

记者:请问您家是否有个小书柜,上面有个五星红旗图案的贴纸?

户主:对。这个信息是随便在网上找到的对吗?

记者:对,在网上找到的。

户主:如果这样,是谁都能看到是吗?

记者:如果有心搜的话,真的可以看到。

户主:天啊,那不是谁都能看到我家,看到我家什么样子了吗?这也太不安全了吧!

目前,记者已将获取的材料向警方进行了举报。

质检总局:智能摄像头抽检八成存隐患

权威发布

6月18日,国家质检总局官网发布关于智能摄像头的质量安全的风险警示称,已检测的40批次中,32批次样品存在质量安全隐患,可能导致用户监控视频被泄露,或智能摄像头被恶意控制等危害。

智能摄像头,是指不需要电脑连接,直接使用Wi-Fi联网,配有移动应用,可以远程随时随地查看家里的一切,与家人语音通话,还支持视频分享、远程操作监控视角、报警等功能的一类产品的总称。

据央视新闻6月18日报道,破解智能摄像头的密码,侵入相关系统,偷看或直播智能摄像头监控内容,已经成为一条非法产业链。

质检总局的风险提示称,智能摄像头可能存在终端安全、后端信息系统安全、数据传输安全、移动应用安全等质量安全隐患,若消费者使用不当或超预期使用,容易导致个人隐私信息泄露、财产损失等危害。

质检总局产品质量监督司组织开展了智能摄像头质

量安全风险监测:共从市场上采集样品40批次,主要依据GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》等标准要求,对操作系统的更新、恶意代码防护、身份鉴别、弱口令校验、访问控制、信息泄露、数据传输使用安全有效加密、本地存储数据保护等项目进行了检测。

抽检结果表明,32批次样品存在质量安全隐患。其中,28批次样品数据传输未加密;20批次样品初始密码为弱口令,或者用户注册和修改密码时未限制用户密码复杂度;18批次样品在身份鉴别方面,未提供登录失败处理功能;16批次样品对用户密码、敏感信息等数据,在本地存储时未采取加密保护措施;10批次样品后端信息系统存在越权漏洞,同一平台内可以查看任意用户摄像头的视频;8批次样品未对恶意代码和特殊字符进行有效过滤;5批次样品后端信息系统存储的监控视频可被任意下载使用等。这些都可能对用户监控视频被泄露或被恶意控制。

“弱口令”带来强风险 IP地址和密码是这样泄露的

智能摄像头的IP地址是怎么落到别人手中?而登录的密码怎么也会一同泄露呢?记者来到国家互联网应急中心寻求答案。

国家互联网应急中心高级工程师高胜称,这种泄露主要是依靠扫描器,用一些弱口令密码,做大规模的扫描。弱口令就是一些user或者admin。

专家介绍,不光是个人购买的摄像头是这样,在用于城市管理、交通监测的公共摄像头中,也大量存在使用弱口令便可以打开的问题。因此,这类摄像头很容易被人入侵。不过,监控平台弱口令漏洞频发,这是

一种世界级的普遍现象。

中国人民大学法学院教授肖中华表示,运用非法的技术侵入他人的家庭生活场景,一般性的生活场景,在民法上侵犯他人的隐私权,这也会涉嫌刑事责任的问题。

肖中华称,个人的行踪轨迹属于个人信息的核心内容,一旦非法获取、出售或者提供50条以上,就触犯了《侵犯公民个人信息罪》。而截取家庭摄像头中的性行为进行展示,制作、传播到一定数量,就构成传播淫秽物品罪;如果传播者因此牟利,并达到一定数量,将构成传播淫秽物品牟利罪。

购买使用家用摄像头请注意这五点

消费提醒

- 一是选择正规渠道购买智能摄像头产品,切勿购买“三无”产品,留意权威部门发布的相关产品质量信息。
- 二是增强隐私信息保护意识,审慎考虑厂商收集、保存和使用用户信息的要求,根据自我实际情况和意愿作出购买和选择决定。
- 三是使用时,应及时主动修改智能摄像头默认密码,密码设置应有一定的复杂度并定期修改。
- 四是及时更新智能摄像头操作系统版本和相关的移动应用,发现异常应立即停止使用,并向生产厂家反馈,等待厂家修复,养成定期查杀病毒的好习惯。
- 五是使用时,摄像头不要正对卧室、浴室等隐私区域,并要经常检查摄像头的角度是否发生变化。