

空调室外机安全隐患令人忧

爱心商家推出免费安装维修活动

□记者 王凯

本报讯 小小的空调室外机支架很少有人“关心”它,殊不知其一旦超龄服役就会变身悬在人们头上的“利器”。近些年,因支架锈蚀断裂,致使空调室外机坠落伤人的事情时有发生。为此,龙都电器商厦近日推出了免费安装维修空调室外机支架活动。

某小区王阿姨家的空调已经安装 7 年了,她说:“我家住在 5 楼,楼下是店铺,平日里人来人往。由于空调室外机挂得比较高,我从没

有检查过,前不久由于空调出问题需要修理空调室外机,这才发现空调室外机的支架已经生锈,而且还有点松动,如果再发现迟一点儿,空调支架脱落的话,那就非常危险了。”

记者采访发现,很多居民家中的空调室外机都是直接安装在户外。在不少小区,记者看到住宅楼外墙上很少有安装空调室外机的平台,重达三四十公斤的空调室外机,全靠墙外两个三角支架支撑着,由于这些室外空调支架长期日晒雨淋,现已变得锈迹斑斑。

据了解,近些年,空调室外机支架“超期服

役”造成的安全事故时有发生。市民加固空调支架意识淡薄,也间接造成安全隐患的长期存在。而一旦发生空调室外机坠落伤人的事件,受害者虽然可通过法律手段向相关责任人讨要说法,但这些都会显得苍白无力,因为生命是无价的。所以,无论是空调销售企业、购买空调的住户,还是小区物业,都应该把注意力集中到空调室外机支架的安全预防措施上。

对此,龙都电器商厦工作人员表示,市民在享受空调的同时,最好能够定期检修一下空调室外机支架,确保螺丝没有松动情况,避

免空调室外机坠楼伤人事件的发生。对于安装时间超过 5 年以上的空调室外机支架,市民应该主动检修或更换。

针对有些商家在出售空调的时候不负责为室外机安装支架的情况,龙都电器商厦相关负责人表示,为帮助广大市民解决这类问题,他们特意推出买空调送支架活动。活动期间,凡是到龙都电器商厦购买空调的消费者,即可免费安装空调支架,并负责相关维修。此外,有需要维修支架的市民,只要花 40 元购买支架,商场将给予免费安装。

病毒木马占空入侵 智能电视难逃黑手

随着信息技术的不断更新发展,互联网覆盖率逐渐扩大,人们进入一个全新的信息时代。网络和信息技术的普及,人们可以享受更多的便利与服务。但同时,这些便利的享受也产生了许多信息安全问题。

电脑、手机、电视甚至是汽车、马桶都已丢弃传统,融入现代信息化。信息技术的飞速发展,智能终端成为未来电子设备发展的趋势。电视智能化趋势越来越明显,逐渐成为彩电厂商的利器,互联网电视、云电视等概念接连出现,智能化电视市场的占有率越来越高。

目前大多数的电视都采用 Android 系统,或是以 Android 系统为核心开发的自有操作系统,引用 Android 系统应用功能,智能手机和智能电视在智能化应用方面应是一家亲。智能电视搭载 Android 操作系统,可由用户

自行进行软件安装与卸载,实现上网、聊天、视频、电影、游戏、购物等娱乐功能的应用,是一个全开放式平台。虽然目前智能电视使用用户的比例不高,但同电脑、智能手机一样,随着智能电视的普及,也一样面临木马、病毒、恶意程序等安全问题的侵扰。

消费者在选购电视时,很少有关关注智能电视的安全问题,大都是关注智能电视本身的功能与应用。对智能电视的安全问题缺少关注,主观地认为智能电视像普通的传统电视机一样,不需担心病毒、木马入侵的问题。我们知道的关于病毒都是主要针对微软 Windows 系统,Android 系统病毒相对较少,智能电视安全问题并不突出,或者说是并没有存在智能电视会遭遇病毒入侵的意识。

网上曝出李小姐在家使用智能电视进行淘宝购物时遭遇木马,被骗了 200 多元;某品

牌智能电视去年被曝存在安全漏洞,黑客通过漏洞入侵用户账户,安装一个 rootkit,即可控制整体设备,监视用户生活。智能电视的安全隐患问题引起越来越多人的关注。

用户使用智能电视提供的智能操作系统来浏览网页、进行在线视频与游戏、下载应用软件等,为病毒的传播与入侵提供了便利,窃取用户隐私,甚至是让电视瘫痪,用户信息、数据外泄,给消费者带来了财产损失与伤害。

支招

让智能电视远离病毒侵扰

信息安全遭遇破坏,消费者该如何培养安全意识,让智能电视远离病毒侵害,是现在人们关注的问题。以下是防范的一些招数:

1.消费者选购时,应询问软件售后服务是否提供病毒库升级、专业木马查杀、漏洞

补丁下载等服务。

2.进行备份资料。一些重要的资料进行备份另存,给信息加一层遗失保险。

3.注意不要随意下载一些应用软件,有很多就有可能被捆绑了病毒或恶意软件。下载应用一定要去正规应用商店或官方网站,信息安全性相对有保障。

4.安装杀毒软件,设置定时更新升级。及时更新操作系统,时刻留意软件制造商发布的各种补丁,并及时安装应用。

5.不用电脑的时候,千万别忘了断开网线和电源。

6.安装一个或几个反间谍程序,并且要经常运行检查。

7.使用个人防火墙并正确设置它,阻止其他计算机、网络和网址与你的计算机建立连接,指定哪些程序可以自动连接到网络。

8.关闭所有你不使用的系统服务,特别是那些可以让别人远程控制你的计算机的服务。

(深晚)

广告