



▲新丝路模特历代服饰秀

### 制作历史可追溯至宋代 已形成全产业链条

据介绍,新会古典家具制作的历史可以追溯到宋代,通过与华侨文化、西方文化的交汇融合,逐渐形成了有别于京作、苏作的古典家具流派——“广作”古典家具,是东西方美学交融的结晶,深受国内外民众欢迎。新会也因此成为“广作”商业化运作的发源地。

目前,新会古典家具已形成全产业链条,拥有全国最大的古典家具专业市场和国内最大的单体古典家具展销商城,建成十里古典家具长廊,并以此为基础组成方圆20公里的古典家具产业集群。全区古典家具生产、销售及配套企业4000多家,从业人员15万多人,产品远销京、津、沪、穗、港、澳及美国、澳大利亚、东南亚等十多个国家和地区。

### 举办博览会 助推古典家具产业转型升级

中国工艺美术协会副会长兼秘书长王山表示,举办博览会的目的就是借助“一带一路”东风,依靠党的十九大新时代的战略规划,加强红木家具非遗保护和传承,健全传统文化产业体系和市场体系,推动古典家具产业转型升级,把中国古老的传统手工艺延续下去,薪火相传。

在行业高峰论坛上,各位知名大咖就如何看待中国传统家具文化的传承和创新,让新兴消费者爱上它,让全世界认可它纷纷亮出真知灼见,进行了“思想”碰撞、令人耳目一新。

慕名而来的世界著名中国古典家具大收藏家,美国加州“中国古典家具博物馆”前馆长柯惕思在接受采访时称,中国古典家具包涵很多文化理念,博大精深,是中国优秀传统文化的很好体现,为世界认识中国文化打开了一扇窗。他将继续静下心来学习研究,以真正了解中国传统家具文化的精髓。

(林阳)



▲榫卯结构纯手工制作大赛



▲博览会开幕式盛况



### 相关链接

新会,古称冈州,是一座有着近1800年历史的南粤历史文化名城。是全国著名侨乡,有海外侨胞、港澳台乡亲70多万人,分布在全球50多个国家和地区。新会先后诞生了理学泰斗陈白沙、维新先驱梁启超、史学大师陈垣、蔡李佛拳始祖陈享、晚清民族英雄张其光等许多名人。新会旅游资源丰富,拥有南中国绿宝石圭峰国家森林公园、岭南名泉古兜温泉、世界唯一的蒲葵林等自然胜景。上海世博会广东馆最大的亮点——“生命之树”,其原型就是位于新会的著名生态旅游景点、著名作家巴金笔下独木成林的小岛天堂。

# 第二届中国(新会)古典家具文化博览会举行

## 声名通四海 木香传古韵

11月10日至17日,备受关注的第二届中国(新会)古典家具文化博览会在广东省江门市新会区举行。

博览会由中国工艺美术协会和新会区传统古典家具行业协会主办,在为期7天时间里,围绕“传承·创新·发展”主题,举办了行业高峰论坛、榫卯结构纯手工制作大赛、高端VIP客户专场讲座等一系列活动。除了吸引众多行业泰斗、知名专家和实力经销商前来赴会,还赢得了来自全国各地的25家媒体的关注。

# 我们家中潜伏了多少“小间谍”?

## ——“黑入”智能家居设备盗卖个人隐私黑灰产业起底

家里的智能扫地机器人在你眼皮底下工作,“看不见的客人”通过内置的感应摄像头却在看着你……近日,韩国某品牌的智能扫地机器人被曝存在安全漏洞,黑客可以远程操控其在用户家中自由行动,窥探个人隐私。

智能家居设备在给我们带来更舒适生活体验的同时,其安全性一直令人担忧。记者调查后,为你挖出潜伏在我们身边、有可能被人利用的“小间谍”。



### “破解”家用摄像头和智能门锁很容易

专家演示

在实验室中,工程师们正在演示“破解”家用摄像头和智能门锁。经过在电脑上的一系列操作,摄像头被成功“黑入”,其所拍摄的画面实时传回工程师的电脑中。系统显示,视频存储量逐渐增大。

在另一个实验中,工程师利用手机的NFC功能(无需接触即可实现互联互通的通讯技术),拿预设好的手机轻刷一下门卡,匹配信息便存储到手机中,再用手机对着门锁一刷,锁就打开了。

### 家里的这些设备可能成为“间谍”

细思极恐

360信息安全部云安全团队负责人王阳东介绍说:

●如果存在安全隐患,家用摄像头、智能网关、带摄像头的扫地机器人、智能电视、游戏主机等设备容易变成“耳目类”间谍,在被远程入侵后容易泄露用户家中的隐私画面,还可能造成包括银行卡密码、社交软件账户等信息泄露。

●具有一定功能的智能电饭煲、微波炉等则有可能成为“攻击类”间谍,在被远程控制后可能造成火灾等破坏性事故。

●而当逐步普及的智能门锁等安防设备,则有可能沦为“策应类”间谍,为上门实施犯罪行为的不法分子“打开方便之门”。

### “请把控制权还给消费者”

用户吐槽

在某品牌的智能网关论坛上,有一些用户发帖称“自己的网关经常‘自己’把家里的灯打开”,也有不少用户跟帖吐槽“下班回家,总看到灯亮着,而且是‘长亮状态’”“一觉醒来,不知道灯什么时候亮了,请把控制权还给消费者”。

记者在采访中了解到,一些用户在使用智能家居设备时也遇到了诸如家用摄像头“自主”转动起来、智能电视“自动”开机等诡谲现象,最终不得不放弃使用。

### 智能设备如何沦为犯罪助手

记者调查

在智能家居设备频遭入侵的背后,是一个逐渐形成的盗卖个人隐私黑灰产业。

记者在调查中发现,尽管一些智能家居设备的产品漏洞反复见诸媒体,但是部分用户仍不知情或不在意,其生活状态有可能长期处在他人监视之下。

记者曾于今年9月浏览百度贴吧、腾讯QQ群等网络社交空间,发现多个贴吧、群组存在倒卖被破解的智能家居设备账号密码的行为,随后将有关信息移交警方。记者11月再次核查时发现,不少贴吧、群组仍存在活跃行为,甚至有一些贴吧公然兜售破解有关智能家居设备的教程。

在一个名为“家庭摄像头”的QQ群中,群主和管理员不定期贴出被破解的家用摄像头所拍摄的画面。为了躲避执法部门的侦查,其成员使用“闪照”功能展示用户隐私画面,该画面必须使用手机QQ查看,在查看时无法截屏,且查看后自动销毁。

因为智能家居设备破解难度低、用户使用率高、隐私信息集中,“黑入”智能家居设备盗卖个人隐私渐成“产业”。从已经侦破的相关案件来看,破解、搜集、兜售这一系列不法行为往往由一个人完成,在通过QQ群、百度贴吧等渠道将售卖信息发布后,来自各地的买家就会主动与之联系,所耗费的时间和金钱成本极低。

### 用户在家时可切断电源 避免隐私泄露

安全提醒

网络安全专家提醒用户,在选购智能家居设备时,应尽可能选择大品牌和大厂商生产的正规产品。对于诸如家用摄像头之类可收集用户画面、声音等隐私信息的设备,当用户在家时,可切断电源,离家后再重新打开,以避免隐私信息泄露。

## 敲黑板! 安全性是智能家居设备生命线

针对当前智能家居设备泄露用户个人隐私的情况,有关专家呼吁,智能家居设备制造业应尽快设立行业标准,有关部门的监管也亟待上线。

王阳东建议,应在智能家居设备的设计阶段即把安全性作为重要考量因素纳入,产品研发也应遵循代码安全开发规范进行。

家电设备智能化和网络化已成大势所趋,诸多曾从事传统家电制造的企业纷纷投身智能设备领域。国内某知名家电制造企业相关负责人表示,随着越来越多的传统家电制造企业“抢滩”智能家居设备制造,层出不穷的“功能性大战”也应进入冷思考期,企业应注重研究在智能化道路上如何保护好用户的个人隐私,而不是一味强调甚至夸大功能性。

他建议,应尽快出台智能家居产品的安全规范,进一步加强对市面上在售产品的安全性测试,探索建立企业隐私保护的信用机制。

在上海信息安全行业协会专委会副主任张威看来,当前智能家居设备频繁泄露用户隐私与执法缺失有一定关系。

“一来是网络取证难度大,二来是犯罪人员位置分散,不仅对执法者的网络调查能力提出挑战,还对执法者的执行意识做出拷问。”张威说,国家针对互联网的个人信息已有相关立法,在涉及隐私权益上的“执法必严、违法必究”仍需进一步强化。

(据新华社)