科普时报

2017年10月6日
星期五
第4期

主管主办单位:科技日报社
国内统一刊号:
CN11-0303
邮发代号:1-178

社　长　尹宏群
总编辑　尹传红

本期要目

剩菜剩饭摇身变宝贝　2版
科普剧应在“剧”上下功夫　3版
地球将遭遇第六次物种大灭绝　4版
打造科普精品离不开工匠精神　5版
科普大咖怎么看?　6版
重新认识方便面　7版
航空器制造应从法规上鼓励创新　8版

消费金融增速过快需警惕

科普时报讯 电子商务的快速发展在改造传统商业模式的同时，也进一步升级人们的消费观念，在支付宝花呗、京东白条等金融产品的全力进攻下，电商消费金融在国内也呈现一片野蛮生长之势。

日前，趣店集团向美国证券交易委员会(SEC)首次公开递交招股书，计划在纽约证券交易所上市。作为最早的校园贷市场试水者和领头羊，趣店在网贷平台涉足校园贷这一业态被监管叫停后，短短一年内实现从校园贷市场到蓝领市场的全面转型。其除了小额现金信用贷款以外，趣店同时运营着由第三方供货的网络商品分期平台。而且随着趣店业务量越做越大，它已经成了一个很难被忽视的电商渠道。

从趣店IPO路线不难看出，消费已成为经济增长的主要驱动力，我国的消费金融进入爆发期。有数据显示，今年1至8月，我国居民新增消费性短期贷款达1.28万亿元，新增总额已达去年全年的1.54倍。多方预测显示，“十三五”期间我国的消费信贷余额将达到10万亿级的规模，年化增长率在20%以上。

消费金融市场的巨大潜力正吸引各大机构“跑步”进入这一领域，除了商业银行、持牌消费金融公司，大型电商平台和部分类似于趣店的网贷平台也纷纷杀入这一领域。这就需要提醒消费者，在消费金融特别是电商消费金融太过野蛮生长之时，要重点注意“恶意欺诈”、“过度消费”等问题，特别是一些机构的业务违规发展、过度授信也给整个行业蒙上一层阴影。

当然，避免消费金融以及电商消费金融过快发展带来的风险，需要金融机构、监管机构以及消费者三方合力。从金融机构的角度出发，宜借助金融科技的发展，加强自身风控能力；从监管的角度而言，则应加快整个社会征信体系的建设，推动消费金融市场的健康发展；而从消旨者的角度来看，最好是能做到量力而为，拒绝冲动消费。　（科文）

白头叶猴母子相依

这张白头叶猴母子照片拍摄于“崇左白头叶猴国家级自然保护区”，该保护区位于广西西南部，地处崇左市江州区和扶绥县境内，面积25578公顷。

白头叶猴保护区属野生动物类型自然保护区，保护国家一级重点保护动物、全球25种最濒危和最需要保护的灵长类动物之一白头叶猴及黑叶猴、猕猴等国家一、二级保护动物和苏铁、金花茶等珍稀濒危野生植物种群及其赖以生存的喀斯特石山森林生态系统，是我国35个生物多样性优先保护区域之一。

近年来，随着国家重视生态文明建设，人们对白头叶猴的关注度和白头叶猴的影响力不断提升。崇左市被中国野生动物保护协会授予“中国白头叶猴之乡”，白头叶猴保护区被授予“全国野生动物保护科普教育基地”。多家大学和研究所在白头叶猴保护区建立科研基地、实习基地、户外体验基地等。

李子健　文/摄

解决城市停车难　共享停车有优势

□ 科普时报特约撰稿　**焦　言**

随着我国经济快速发展，城市化进程不断加快，机动车保有量急剧增长，大量的停车需求与有限的停车泊位资源严重不匹配，导致城市重点停车区域停车供需矛盾突出，城市正常交通秩序受到干扰。基于此，共享停车作为解决停车问题的一种新型尝试开始流行起来。究竟什么是共享停车？能否有效缓解停车难题？车位共享背后又面临哪些问题?

解决停车难有了新思路

根据国家发改委公布数据显示，目前我国大城市小汽车与停车位的比例约为1：0.8，中小城市约为1：0.5，缺口非常严重。同时，在机动车保有量持续快速增长和城市停车设施建设严重滞后的双重约束下，“停车难、停车乱”问题已愈发凸显。简而言之，可用停车位几乎是各大城市的刚需性需求，共享停车位目的也是要解决这个困局。

那么究竟什么是共享停车？共享停车模式是基于地理位置，通过互联网来实现就近共享停车。车位主人可分享自己的空闲时段车位到APP管理软件上进行分时出租，增加收益，并能方便身边车主；小区物业或停车管理公司也可通过APP管理软件进行安全高效的车位错时出租管理。

当前共享停车的主流思路是，错开小区与商业区停车位的停车高峰，并根据情况进行优化将停车资源错时共享，以缓解“停车难”问题。譬如上班时间，小区的居民把车开到写字楼等商业区，小区则存在大量闲置停车位，小区个人便可通过共享平台将车位开放租赁出去，附近写字楼、公司上班族可在共享平台查看、预定适合自己的小区车位，把车开进小区共享闲置车位。一般共享停车采取即时计费，汽车离场时停车场系统会自动起杆，费用从手机自动扣除、结算。当然，商业区亦可采用同样的错峰停车思路。

各地相继尝试发展共享停车

为更好地解决“停车难”问题,各地相继出台了相关政策以鼓励、引导共享停车的发展。2016年下半年，上海市发布了《关于促进本市停车资源共享利用的指导意见》，计划在2017年建立50个共享停车示范点。2017年7月，北京市人大审议的《北京市机动车停车管理条例（草案）》提出：个人或单位可以开展停车位有偿错时共享。居住小区在满足本小区居民停车需要情况下，可将配建停车设施向社会开放。2017年8月初，在网上听证的《广州市停车场建设和管理规定（草案）》也提出：鼓励住宅停车场在满足本住宅区居民停车需求的前提下向社会开放，有条件的单位可以将自用停车场向社会开放。

（下转第二版）

医疗信息安全再添新保障

□ 科普时报记者　**陈　杰**

近年来，新型数字化医疗系统在全国医疗机构持续落地，互联网医疗等新型医疗模式不断浮现，尤其是病历电子化、医院上云、远程问诊等在医疗界轰轰烈烈展开，患者信息、病历等也从纸面转化为电子版，通过互联网医疗、远程问诊等新型医疗模式，医院内网的数据走向公网，这些基于互联网或移动互联网为基础的业态以其独有的方便逐渐为普通大众所接受。

然而，人们在享受这些新型医疗服务的同时，也不得不面对越来越多的医疗信息安全问题。由于数据量庞大、使用价值高、大量医疗机构安全保障和风险管理措施较落后等因素，使医疗行业数据成为黑客们钟爱的攻击目标，医疗数据泄露等安全事件不断发生，对医疗行业构成了巨大挑战。

中国医师协会副秘书长谢启麟认为，在大数据时代，数据结构化与数据的安全保障是对医疗数据进一步挖掘和应用的前提。开展临床数据结构化、标准化和规范化的工作是打通“数据孤岛”，实现数据互联互通的基础，也是未来中国制定自己的临床指南的必由路径，而在医疗大数据的应用和发展过程中通过网络安全技术加强数据安全，以及患者隐私的保护，是推动医疗大数据健康发展的关键，只有切实做到以上两个方面才能真正实现数据融合共享、开放应用。

如何解决这些安全威胁，便成为摆在医疗机构以及相对应的系统提供商们面前的难题。

基于这种需求，云与大数据安全的技术领导者亚信安全与AI及医疗大数据平台零氪科技达成战略合作，双方将在医疗行业混合云安全、移动应用安全防护、数据隐私保护、态势感知平台、数据脱敏及攻防演练、渗透测试等方面开展深入合作，并共同推出“中国医疗信息安全全流程解决方案”，以帮助医疗机构保护医疗业务与数据的安全性。

零氪科技拥有全球领先的AI与医疗大数据平台，以及国内体量与规模最大的数据资源库和卓越的技术支撑体系，已经成为医疗行业备受信赖的数据解决方案提供商。双方的战略合作将结合零氪科技在医疗大数据方面的优势，与亚信安全在信息安全方面的优势，化解病毒、黑客攻击、人员管理等因素对医疗数据构成的威胁，携手创造更安全的医疗信息环境，助力政府实现健康中国2030目标。

此外，双方将与公安部、卫计委开展深入合作，除了推出医疗行业数据安全等级定义及管理办法之外，还将推动China HIPPA（中国健康保险可移植性与可责性法案）的制定。此外，亚信安全的混合云安全解决方案还将与零氪云平台服务进行整合，将零氪公有云与医院内网的安全系统对接，实现医院对零氪公有云提供服务的监测和管理。在医疗大数据方面，双方将结合亚信安全的安全解决方案与零氪的医疗大数据解决方案，形成全新的“医疗大数据平台解决方案”，满足医疗大数据应用与大数据安全防护的需求。

在医疗机构推动数字化转型的今天，亚信安全与零氪科技的合作将为医疗机构提供高度整合的数据应用与安全防护整体解决方案，这将进一步推动医疗机构应对日渐肆虐的网络安全威胁，保护珍贵的医疗数据资产。

编辑视点

不必对公共WiFi畏之如虎

□ 陈　杰

随着万物互联时代的到来，移动互联网也迎来了全面视频化热潮，对应的各运营商4G网络套餐不论是流量上还是在速度上都已经很难满足“低头族”的需求，WiFi似乎是唯一的选择。然而，除了家里和单位自建的WiFi外，“公共Wifi不安全”“不能在公共Wifi下使用移动支付”等各种安全专家的警告频出，这一论调也渐渐为越来越多的网民所接受。虽然，很多人并不真正了解缘由，但“宁可信其有，不可信其无”依然是主流。

公共WIFI果真“凶猛如虎”吗?

日前，一份《2017年上半年中国公共WiFi安全报告》显示，2017年上半年国内风险WiFi热点仅占比0.81%。

不仅如此，在这一足百分之一的风险WiFi中，超过99%的风险WiFi带给用户的损失是“在被动的情况下链接了广告页面”，而用户遇到真正有威胁的中高风险WiFi热点的概率不到万分之八。

显然，认知很重要，所以很有必要对风险WIFI的相关知识做做普及，目前来看风险热点主要通过两种方式达到该目的，一种是通过最常见的广告链接形式，使用户在浏览网页时，并未主动点击却有广告弹出；另一种则是通过暗链的形式，在用户手机后台点击广告，达到恶意推广、广告刷量等目的，同时由于是在手机后台操作，用户对此并无感知。而真正的高风险WiFi热点会将用户引向钓鱼网站，或者进行SSL篡改，借机窥伺用户的账号密码等数据。但是这两类高风险热点占比微乎其微，加上中等风险的DNS劫持和ARP异常风险热点，在所有热点的占比仅为0.0076%。

所以，只要对风险WiFi的产生机制有一定了解，大部分风险WiFi也是比较容易识别及防范的。上述报显示，目前风险WiFi中有15.3%的风险热点为正常WiFi被不法分子入侵形成，高达84.7%的风险热点为不法分子冒充可信热点架设。这类“山寨”WiFi一般无密码，也无认证机制，最多冒充的是三大运营商热点、知名商家默认热点以及知名路由器系统默认热点这三类。如果用户发现热点，无需任何验证机制即可连接，或者附近没有星巴克的店面，却搜索到了名为Starbucks的热点，就需要对此提高警惕。

基于对于共享WiFi的不信认，有不少用户认为连接风险热点时使用网银等支付软件，黑客便能盗取自己的账号密码，然后进行盗刷等违法行为。但事实却被盗刷银行卡等案例的出现，大多是由于用户在没有察觉的情况下登陆了钓鱼网站，或者是手机、电脑已经中毒。其实，目前几乎所有的正规支付类软件和大部分知名品牌的软件在核心数据交换时都采用双向加密通信。而加密通信即便发生流量挟持，黑客也难以对此进行解读以及篡改。

当然，被动点击广告这种危害对用户没有造成直接损失，但仍旧是对用户正常浏览行为的一种骚扰。中高风险的热点尽管占比极少，但是也不容忽视。

显然，公共WiFi尽管有风险，但用户平时只要稍加留意，就能规避。

有数据统计，2016年全球信息安全支出就达816亿美元，预计至2020年这一投入将高达1700亿美元，政府、机构、企业在安全方面的投入呈全面上升之势。

不能否定WiFi风险的确存在，但广大网民不必对此过于担忧，目前WiFi行业及企业都在加强自身安全防护实力保障用户联网安全。此外，在面对占比较低的风险热点之时，用户更多的还应该提升自身的防范意识，普及更多的安全知识，就一定能有效地防范移动互联网新形势下的各种网络威胁。