# “云”办公变助推器 数字化转型成常态

都2020年了，你还没到“云”上生活吗？今年，受疫情影响，云办公、云打卡、云会议、云展览等线上活动迅速流行了起来，为满足人们日常需求，加速复工复产做出了巨大贡献。许多政务活动也由线下转到了线上，在减少了人员聚集的同时，也提高了办事效率。在线办公的快速发展，不仅拓宽了数字化生产生活场景，助力企业降本增效，更为拉动经济开拓新增长点。只需要网络，便承载了人们生活的大部分，这就是2020年。

### 在线办公成为常态

许多数字转型领先的企业在今年受到疫情的影响比较小。成熟的线上运营机制让员工即使在家也能正常工作，保证企业的正常运行。为了应对疫情，多数企业、单位也开始做一些线下转线上的尝试。人们纷纷拿出了手机，打开了电脑，远程开会的开会，在线教育的上网课……其实，自2008年电商发展以来，企业便逐步开启在线办公；到了2017年，随着各类行业服务软件的崛起，在线办公工具也开始向专业化、垂直化方向发展；至今年初，在线办公平台呈爆发增长态势，逐渐普及。

在如今高效便捷的网络时代，许多企业正面临着数字化转型，在数字化管理方面的需求日益增大。今年更是因为疫情的原因，给在线办公市场投下了一个巨大的蛋糕。阿里钉钉、腾讯、华为WeLink、头条飞书、百度如流等巨头竞相出手，一时间，在线办公市场呈现出群雄逐鹿的态势。随着用户习惯的养成，在线办公市场还将挖掘出进一步的潜力。

### 助力政企降本增效

许多在线办公工具都具有远程打卡、云端会议、协同办公等功能，一方面提升了企业的工作效率，另一方面员工在家办公也可使企业节省下许多日常开支的成本。于员工而言，工作时间更有弹性，能够更灵活地安排工作。与此同时，一些习惯于线下办公的企业管理者面对线上作业，同样需要适应新的办公管理模式，加大信息化、数字化建设的投入，建立起远程办公协同的文化体系，以提升企业在线办公效率；员工则需要提高自身自律性，在家中为自己营造一个合适的办公环境以保证工作效率。在厦门埃菲铁件有限公司工作的林先生就是习惯线上办公的一员。日常工作中，他通过微信视频远程指导客户操作，或者利用QQ、向日葵等软件工具远程控制对方电脑，达到解决问题的效果。“利用网络足不出户便能完成日常工作，也使我能够更自由地安排自己的时间。即使公司在厦门，也不影响我在漳州办公。”林先生如是说。

今年2月份，漳州市税务局力推“零接触”办税，依托微信公众号、税企联络微信群等平台，发布疫情期间办税公告，广泛宣传、引导纳税人借助电子税务局、微电子税务局、闽税通App等，进行“非接触式”网上远程办税，实现绝大多数涉税事项“全程网上办，一趟不用跑”。“现在改成线上报税要比以往便捷多了，不用再找时间跑税务局了。”从事企业税务代办的陈先生说。他的公司为上百家企业代办税务。自从有了网上办税之后，不用经常奔波于税务局与公司之间让他节省了许多时间与成本，提高了办事效率。

为推动漳州智慧城市的建设，漳州市市监局大力推动智慧监管，于2018年底建成具备网络主体管理、网络市场检查、在线电子取证、商标广告监测等功能的网络交易监管服务平台。又打造了更具针对性的业务数据子库，在平台内建立了包括网络餐饮、食品生产、食品流通、特殊食品、药品、医疗器械、化妆品等涵盖全局十几个业务内容的子库，从而实现精准监管、靶向式监管。业务科室通过运用网监平台，检查监测我市食品生产、流通主体的网络经营行为，智能化发现涉嫌食品安全违法违规线索，及时分流给属地单位线上线下核查确认，从而规范我市食品主体的网络经营行为，提高市监局食品安全网络监管水平。

### 加强信息安全保护

在线办公终究是依托于网络之上的，而网络具有开放性，个人信息与单位信息若存于网上则会有被泄露的风险。若这些信息被泄露并被非法利用，就会造成极其严重的损失。近年来随着信息技术的快速发展与互联网的普及应用，也出现了对用户信息非法收集、滥用、泄露等问题。不仅是个人和企业用户隐私和权益遭到侵害，特别是一些重要数据甚至流向他国，信息安全威胁已经上升至国家安全层面。因此，提高网络安全意识与保密意识，保护网络信息安全非常重要。

网络信息人人共享，网络安全人人有责。关于个人如何维护网络信息安全的方面，漳州市反诈骗中心民警林芳宇提醒：要为自己的电脑装好杀毒软件与防火墙，实时更新病毒库，并定期为自己的电脑查杀病毒；要健康上网，文明上网，不浏览不良网站或高风险网站，防止病毒木马入侵；要提高防范意识，不轻信陌生来电与陌生人信息，不随意添加陌生人的微信或QQ好友，不向来路不明的应用或组织提供个人信息，不扫来路不明的二维码；如遇疑似骗子冒充友人小号添加自己微信或QQ好友的，请找友人当面核实；企业微信号申请门槛低，权威性不高，当谨防不法分子会利用企业微信进行诈骗；要提高鉴别能力，多学习防范网络诈骗的资料，谨防上当受骗；不要在公共网络上工作或发送私密信息；要有良好的保密意识，坚持涉密不上网，上网不涉密，还要为自己的账户设置足够复杂安全的密码；验证码是资金和信息安全的最后一道防线，不要将其泄露给他人。只有人人都有良好的网络安全意识，积极维护网络信息安全，才能切实维护自身利益，共筑国家信息安全的壁垒。

⊙本报记者 张昊填 文 郑睿宇 制图

# 把『智能』穿起来

随着网络的发展，人工智能技术的成熟，可穿戴设备成了生活的“标配”，从最初的电话手表、手环到如今的眼镜、服装、戒指等，可穿戴设备应用于更多的场景中。此外，可穿戴设备的监测功能也从最初的定位、步数拓展到监测血压、心率、睡眠等健康领域，也重新定义现代人的生活方式。

### 可穿戴设备让生活“联网”

可穿戴设备（又称可穿戴科技）是指一些植入衣物或饰品等且人们能够舒适穿戴的电子设备，这些设备能够完成诸如手机、笔记本电脑等具备的一些功能。记者了解到，目前，市场上已经出现的可穿戴设备有：智能手表、智能手环、智能眼镜、智能戒指、智能服饰等。在出行、运动、医疗、健康方面，都经常用到智能可穿戴设备。

“孩子上幼儿园，活动范围扩大，定位、防走失功能是吸引我的一个主要因素。”在女儿上幼儿园小班时，从事技术行业的戴智能就买了一款电话手表，起初主要是看中定位与通话功能。后来，随着电话手表的功能扩展，戴先生也跟着更新了孩子的设备，功能也从最初的定位需求，延续到了视频通话、学习等。

健康监测，也是吸引漳州市民购买可穿戴设备重要原因之一。

体育纳入中考，市民陈坤林就给上初中的孩子买了运动手环，只要有时间他都会陪孩子进行一些体育运动，“通过手机终端就能实时监测孩子的运动量，比如锻炼步数、实时心率、环境温度。”陈坤林说，手环还能及时有效采集学生的肺活量等数据，并给手机实时发送数据，如果孩子超量运动或运动不足时，系统会自动发出预警，陈坤林会根据情况及时做出调整。

“语音打电话”“测心率”“测血压”等功能的可穿戴设备也是不少漳州市民的选择。“我爸不爱跟我们住，我买了可穿戴设备，上班时候可以通过App实时查看老人的身体变化，老人不小心摔了，手表能自动给你手机中的App反馈信息，此外，还能进行一些健康指标的检测。”家有80岁的老人，可穿戴设备让蔡志扬先生放心不少。

记者了解到，目前的可穿戴设备功能仍处于健康监测范畴，可以对慢性疾病患者某些指征进行监测的设备，如血压仪、智能血糖仪、智能体温计等。也有部分可穿戴设备具有部分治疗功能，通过可穿戴设备对患者健康数据进行检测、收集、分析与处理，从而作为医生临床诊断的重要辅助依据，提高问诊效率。

### 可穿戴设备“智能相随”

“方便、可监控、可监测。”采访中，多数民众跟记者表达了对可穿戴设备的直观感受。“当你运动时，手环可以自动识别健走、跑步等状态，不需要手动设置，就可以记录相关数据。手表可以当做公交卡使用，出行更自由，还可以通过语音遥控家居设备，让生活更简单等。”“90后”杨星说，自己打算在新房配备智能系统，届时，只要动动手，就可以让自己的生活更加舒适。

业内人士表示，可穿戴设备一方面是硬件设备，更重要的在于通过软件的支持实现数据交互，只要有了屏幕，就可以用语音或是手指进行操控，为生活带来更大的便利。“智能可穿戴设备的作用有很多，不仅是监测身体各项数据，还可以用于钱款支付等，实用性很高。另外，它还是一个时尚装饰品，戴上还能彰显时尚范儿。”市区一家小米体验店的店员介绍说。

可穿戴设备逐渐渗透到医疗领域，与移动医疗相结合，也开启了健康管理的一种新模式。“可穿戴设备扩充监测内容，包括脑电波、血氧等情况能够实时、持续收集患者的监测信息。”护士张静说，这些客观的数据记录往往比患者向医生描述的感受或者对病情的表述更为精准，对患者的状态评估和支持临床决策提供了便利。

针对老人、儿童、孕妇等特殊人群，可穿戴设备还能提供安全监护方面的服务。比如，可穿戴设备能够自动预警，提醒存在健康风险的患者及时就诊，避免严重并发症的发生；能够监测跟踪胎心数据，收集和传输孕妇各项生理参数，确保孕妇安全，还可以监测胎儿生理参数，促进实现优生优育。

采访中，也有人提出，现在可穿戴设备大部分都要依赖于手机，通过智能手机实现，比如目前不少类似设备需与手机App等连接才可实现功能，对于年纪大点的人来说操作还有一定的局限性。“不过随着人工智能的发展，未来，可穿戴设备可能会替代手机。”陈坤林说。

另外，业内人士也表示，可穿戴设备大数据价值是未来的一个方向，但目前社会参与度并不高。“大数据的确会涉及个人隐私。”但是，无论是用于运动记录、锻炼还是辅助中老年的医学监测，或是为生活提供便利，可穿戴设备作为互联网与物联网深度融合的产物，民众需求将日益增长，“抬腕”就能开启智能生活、随时随地即可监测自身健康情况的时代已逐渐到来。

⊙本报记者 陈晓云

焦点网谈

郑睿宇 制图

# “数字生活”需警惕多重风险

移动支付、网络约车、线上办事……“数字生活”已在不知不觉中成为主流生活方式。但与此同时，网络安全问题也逐步显现，支付安全、网络安全、个人信息安全等每时每刻都在经历着考验。记者在网络安全周采访了解到，相关专家建议需警惕“数字生活”带来的多重风险。

国家互联网信息办公室印发的《数字中国建设发展进程报告（2019年）》提到，2019年我国数字经济增加值规模达到35.8万亿元，占国内生产总值（GDP）比重达到36.2%，对GDP增长的贡献率为67.7%。奇安信集团天津技术总监崔宗福介绍，二维码是数字经济的一个重要元素，人们在扫描二维码时需警惕“恶意二维码”。

崔宗福说，扫描“恶意二维码”会泄露个人信息，同时会威胁用户的财产安全，一些不法分子还将木马病毒程序植入二维码中，用户扫描后入侵用户的后台程序。针对这一问题，崔宗福建议广大用户要适当收起自己的好奇心。

“一是不要随意扫描来历不明的二维码，二是在支付时要反复确认收款人身份，三是可通过下载安全软件规避不良信息入侵电子产品的后台程序。”崔宗福说：“‘恶意二维码’就像一个鱼钩，静静地躺在那里等待‘鱼儿’上来。最好的防范措施就是提高自己的安全意识。”

与“恶意二维码”一样的“钓鱼陷阱”还有钓鱼短信。深信服科技股份有限公司天津区产品专家井雨晴介绍说，一些不法分子通过盗取用户的网购信息对物流进行跟踪，在快递到达时向用户发送短信，以快递状态异常为由诱导用户添加微信并提供个人相关信息，威胁用户的财产安全。

除了提高安全防护意识，给自己的个人信息“上保险”也必不可少。绿盟科技集团股份有限公司天津技术总监曹靖杰介绍，“该有密码的不设密码，设了密码也很容易被破解”是目前大部分电子账户存在的问题。

“很多人都会给手机设置开机密码，但很少有人会给SIM卡设置使用密码。”曹靖杰说，丢失手机后，不法分子可以通过SIM卡获取用户的手机号码，在一些防护较弱的App上通过手机验证码获取用户的账号密码。“如果这些App上绑定了支付信息，用户的财产安全就会受到威胁。”

目前很多用户在设置密码时喜欢“一组密码走天下”，崔宗福认为这是非常危险的行为。“不法分子在破解密码时一般会进行四种方式的尝试：一是暴力破解，即用一定的频率随机输入密码；二是在前期获取部分用户信息的基础上尝试目标用户的生日等信息进行破解；三是使用‘123456’等弱密码尝试破解；四是用已经破解的用户密码在其他账户上进行‘撞库’。一组密码走天下就会使得用户的个人信息存在更大的泄露风险。”

对此他建议，在设置密码时要尽量使用字母、数字和特殊符号组合而成的“强密码”。“尽量不要使用自己的生日、姓名作为账户密码。”崔宗福说。

（新华网）

@天下网闻

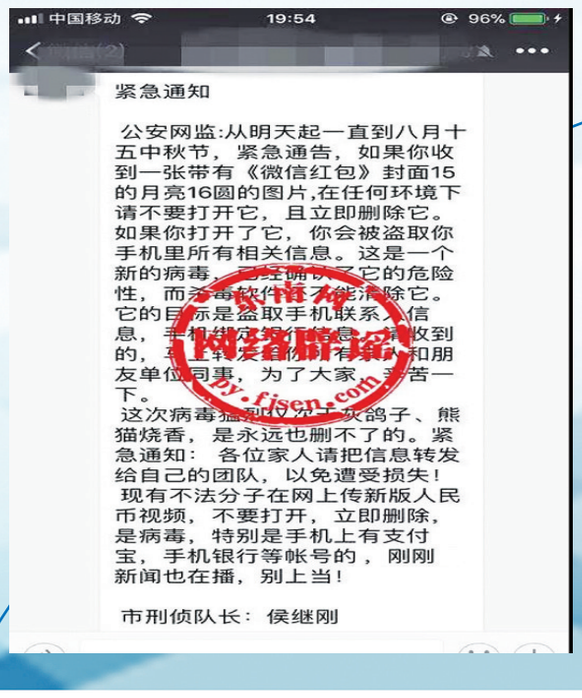
# 5G智能社区建设化解高空抛物治理难点

近日，银川首个5G智能社区产品发布会在美林睿府小区召开。该小区建设的高空抛物智能监测系统，成为化解高空抛物治理难点、预防和守卫业主安全的新型“智慧卫士”。

高空抛物长期以来是小区管理的难点和痛点。该小区建设的智能安防系统纳入了防高空抛物监控系统，在小区所有楼栋的南北两侧均安装有防高空抛物监控系统，分楼层将楼栋全部纳入监控范围，24小时不间断监测。一旦发生高空抛物事件，系统会自动拍摄视频取证，并准确定位高空抛物的具体位置，为高空抛物引发的法律问题提供有力的证据。同时，防高空抛物监控系统可实时连接到小区物业设备管理平台，后期还可纳入街道管理平台和辖区政府统一管理平台，能一定程度震慑随意抛物者，有效减少小区高空抛物事件的发生。

据了解，“美林睿府”智慧小区将物管、安防、服务、设备等集合为一体，通过对接社区监控视频、出入口人脸抓拍、车辆抓拍、门禁通行记录等相关技术的数据库，采集小区实有人口、实有房屋等数据，实现了通过小区感知数据找人、车的最后100米相关功能，并提供了人像比对、轨迹刻画、异常发现、车辆识别等多种研判分析手段，对信息检索、案件侦查、数据分析处理及关联应用提供有力的信息和技术支撑。

（新华网）




@一周辟谣

# “微信红包”暗藏手机病毒？谣言！

**谣言内容：**近日，一条自称为“公安网监”发布的网络安全防范通报在微信群流传。“明天起到八月十五中秋节，如果你收到一张带有《微信红包》封面15的月亮16圆的图片，在任何环境下请不要打开它，且立即删除它。如果你打开了它，你手机里所有相关信息将会被盗取。”并且提到了“这是一个新的病毒，且杀毒软件不能清除它。”这是真的吗？

**真相：**对此，微信团队表示：微信一直在努力提供各类安全防护技术来保护用户的社交安全，因此恶意链接和文件根本不存在大规模传播的可能性，用户转发正常的问候图片和小视频不会导致设备中毒或信息泄露。

同时，具有多年网络安全工作经验的资深网警庄警官辟谣称：相关部门发布的正规通报都会使用单位全称而不是简称，也不会以个人名义发布。网警只会通过在各大平台的官方账号发布网络安全防范的信息，而非以文字的形式在朋友圈传播，请网友以官方渠道的信息为准。

（腾讯新闻）