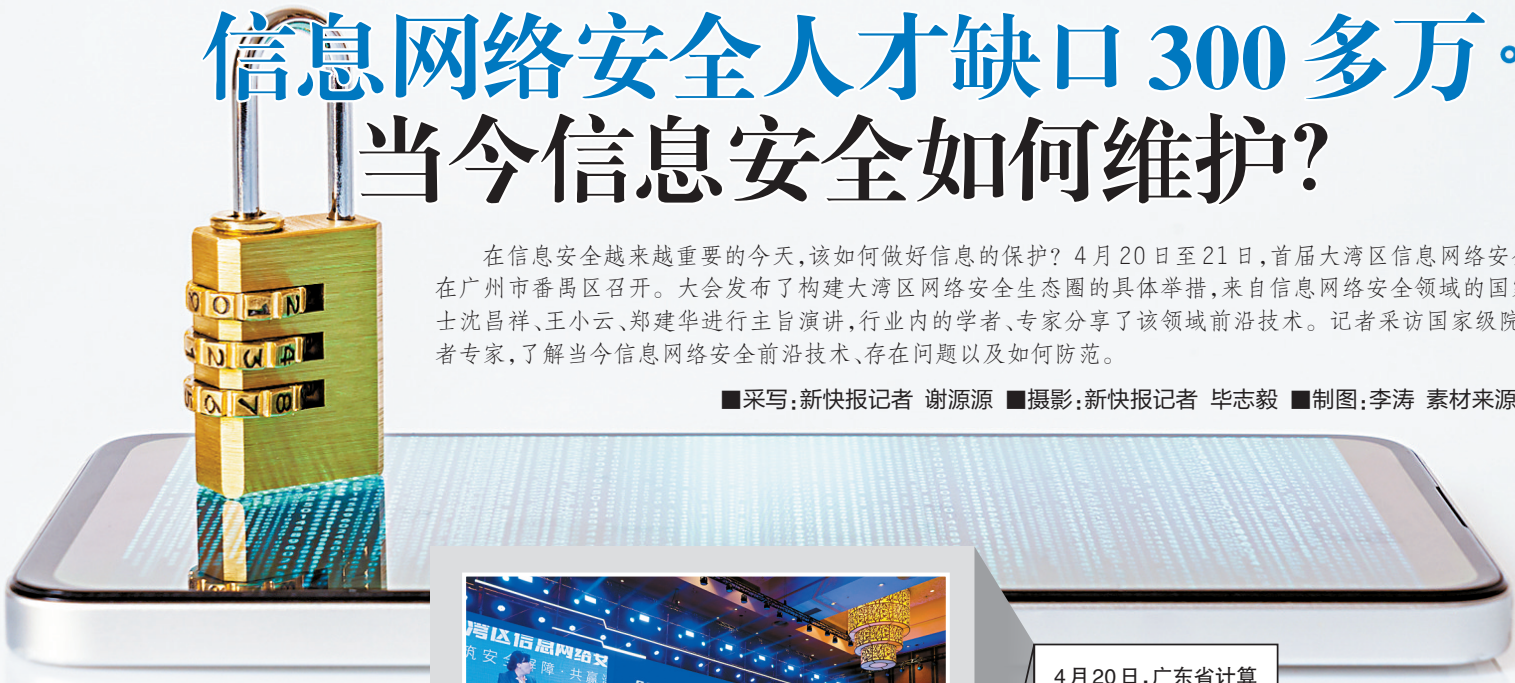
首届大湾区信息网络安全大会在广州举行

信息网络安全人才缺口300多万 当今信息安全如何维护?

在信息安全越来越重要的今天,该如何做好信息的保护?4月20日至21日,首届大湾区信息网络安全大会在广州市番禺区召开。大会发布了构建大湾区网络安全生态圈的具体举措,来自信息网络安全领域的国家级院士沈昌祥、王小云、郑建华进行主旨演讲,行业内的学者、专家分享了该领域前沿技术。记者采访国家级院士、学者专家,了解当今信息网络安全前沿技术、存在问题以及如何防范。

■采写:新快报记者 谢源源 ■摄影:新快报记者 毕志毅 ■制图:李涛 素材来源:VCG



4月20日,广东省计算机信息网络安全协会联合广东省粤港澳合作促进会主办的首届大湾区信息网络安全大会在广州举行。

数字化带来的安全威胁

"我们用什么能确保网络空间安全?"中国工程院院士沈昌祥接受采访时表示,网络安全与个人的安全保障休戚相关,对社会健康安全非常重要。当出现病毒、黑客、漏洞时找漏洞打补丁仅是表面工作,关键是要构建主动免疫安全保障体系。他认为,网络安全等保制度2.0标准及关键信息基础设施安全保护条例要求,应当优先采购、全面使用安全可信的产品和服务,来构建关键信息基础设施安全保障体系。

中国科学院郑建华院士在《充分发挥密码技术在网络安全中的作用》主旨演讲中分享了一些医疗领域案例。其中,2019年,某公司宣布召回系列胰岛素泵,原因是这些设备存在安全漏洞,黑客可以篡改设备设置并控制胰岛素的输送,FDA发出警报,预计至少4000名糖尿病患者受影响。研究人员还发现,某医疗公司的两款设备麻醉系统,固件存在安全漏洞,攻击者进行降级攻击,最终实现远程关闭警报、改变记录,另外还可以被滥用来改变呼吸器和麻醉机中吸入气体的成分,攻击后果可以达到遥控杀人。

"没有网络安全就没有国家安全。"郑建华指出,当前面临的网络安全问题有三个特点:网络攻防水涨船高;从信息攻防到设备设施攻防;云计算、大数据、人工智能、区块链等新技术发展拓展网络安全领域。他认为,要做好网络安全,需要注重密码技术在整个网络安全中的作用发挥。

提高密码等安全技术措施

网络安全行业未来的发展趋势是数字化、智能化、服务化,这将对行业的发展和创新带来深远的影响,推动行业向更高层次迈进,带动行业的技术和产业升级。

"密码的核心作用是解决现实社会的身份问题、隐私问题。"深圳网安计算机安全监测工程技术有限公司总师杨宏志介绍说,疫情加速了数字时代的来临,文明的数字时代迫切需要解决数字化的身份问题、隐私问题,而解决这些问题就是要使用安全的密码技术。

如何做好个人信息保护?杨宏志表示,合规的密码产品和服务是提供安全保障的基础。在合规这个前提下,使用密码产品/服务的过程中,正确使用是关键,比如输入口令时进行必要的遮掩\口令的设置规则等。

"安全和效率本身是相互制约的,牺牲一定的便利换取必要的安全也是必要的。对用户而言,设置复杂口令就是这个范畴,对厂商而言,则需要在安全和效率两者找到折衷的办法,既不影响用户的使用感受,同时提供必要的安全强度,这本身也是密码应用的挑战问题之一。"

"可以说,以前的社会依赖于宗族、血缘,依赖于法律、合同建立信任,随着数字时代的来临,未来的社会需要依赖安全的密码技术构建网络信任体系。"杨宏志说。

信息网络安全人才缺口大

"数字化程度越高,安全事件危害越大。"华为公司安全产品领域总裁马烨在《建设可信安全网络和集约式安全服务,护航大湾区数字经济发展》演讲中介绍了网络安全体系现状及存在问题。对于如何防范ChatGPT等引发的数据泄露问题,马烨表示,需要从立法层面进行解决。

马烨介绍说,未来几年,我国信息网络安全人才缺口达300多万。"未来的网络安全形势将会更加复杂和严峻,因此企业应该加强网络安全建设,提高技术和人才储备,加强技术研发和创新,及时发现和修复漏洞,加强安全意识教育和技术培训。"

在人才培养方面,目前已有不少高校及职业院校开设网络安全相关专业。自2016年起,广东省计算机信息网络安全协会通过选拔"红帽先锋"网络安全人才团队、构建"红帽杯"网络安全大赛品牌项目,不断探索网络安全人才培养新模式。未来还将持续围绕"红帽先锋"网安人才团队志愿者、"红帽杯"网络安全大赛、"红帽社区"、"红帽"人才培训认证等"红帽"系列工程,不断提高粤港澳大湾区网络安全人才培养水平,打造网络安全人才培养高地。

声音

"不要把刷脸当成洪水猛兽,涉及公民敏感信息要重点保护"

公安部信息安全等级保护评估中心原副主任、研究员毕马宁表示,数据的应用是未来发展的一个必然趋势,需要我们在认知上提升安全意识,并采取相应的措施把个人的信息安全保障好。"我们进入了一个网络时代,原来出门必须带的东西,现在只要带一部手机,这是数字化给我们个人生活带来的变化,同时对我们生活的安全威胁也发生了变化。"

如何做好个人信息安全保护?毕马宁介绍说,国家建立网络安全等级保护制度,就是为了保护公民、法人的合法权益,就是为了保护人民福祉、社会秩序、公共利益和国家安全。在当前信息爆炸的时代,个人数据安全应该得到高度重视和保障,企业在采集、使用个人数据时应该遵循合法、正当、必要的原则,确保用户知情,并采取相应的安全保护措施,避免数据泄露和滥用。

谈及人脸识别,毕马宁认为,刷脸技术本身提升了生活的便捷性,也为提高网络应用服务的安全性提供了帮助,不要把刷脸技术当成洪水猛兽,而是应该安全、有序、按规则地使用。"刷脸技术应该在法律框架下,在相应的技术标准约束下进行。人脸信息是一个特别敏感的个人信息,不能当成一般的数据,人脸数据的泄露和丢失可能会给公众带来很大的影响。国家在这方面已陆续出台了相应的技术标准,个人信息保护法也讲了,涉及到公民特定信息和敏感信息的,需要重点保护。而且需要有第三方的评价机构,来监督使用者是否尽到了保护好的责任。"

关注

青少年如何保护个人信息不被网络诈骗者盗取?

答:青少年应该保护好自己的个人信息,不要轻易泄露自己的手机号码、身份证号码、银行卡号码等敏感信息。同时,不要点击来自陌生人或不信任的网站的链接,不要相信不明来源的电子邮件或社交媒体消息。

如何防止青少年成为网络欺凌的受害者?

答:青少年应该避免在社交媒体上公开自己的真实姓名、地址、学校等信息,同时要学会保护自己的隐私。如果遭遇网络欺凌,应及时向家长、老师或警方求助。

青少年在使用手机或电脑时,如何避免沉迷网络?

答:家长可以通过设置限制使用网络的时间来避免青少年沉迷网络。此外,也可以引导青少年多参与有益的课外活动,如体育运动、音乐、绘画等,帮助他们保持身心健康。