

工业和信息化部办公厅关于做好疫情防控期间信息通信行业网络安全保障工作的通知

发文日期	2020年02月14日	文号	工信厅网安函[2020]22号
发文机关	工业和信息化部	有效范围	全国
时效性	现行有效	生效日期	2020年02月14日
所属分类	电信（ 通讯法->电信 ）, 公安法（ 公安法 ）, 计算机与互联网（ 科技法->计算机与互联网 ）		

工业和信息化部办公厅关于做好疫情防控期间信息通信行业网络安全保障工作的通知

工信厅网安函[2020]22号

2020年2月14日

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国铁塔股份有限公司、中国广播电视网络有限公司，中国信息通信研究院、中国软件评测中心、国家工业信息安全发展研究中心、中国工业互联网研究院，国家计算机网络与信息安全管理中心、中国互联网络信息中心，相关域名注册管理和服务机构、互联网企业、移动通信转售企业、网络安全企业：

为深入贯彻落实习近平总书记关于新型冠状病毒肺炎疫情防控工作的重要指示精神，切实做好疫情防控和经济社会运行的网络安全支撑保障工作，确保疫情防控期间网络基础设施安全，防止发生重大网络安全事件，现就有关事项通知如下：

一、全力保障重点地区重点用户网络系统安全

（一）加强重点用户网络安全技术支撑。充分发挥信息通信行业网络、技术和队伍优势，组织力量为党政机关、医疗机构、公共应急、教育教学等疫情联防联控单位以及重点工业互联网企业等用户提供网络安全技术支撑，主动沟通对接，及时为重点用户相关网站和信息系统提供网络链路保障、防拒绝服务攻击和防域名劫持等应急处置支撑。

（二）加强重点地区网络基础设施安全防护。加强涉疫情重点保障地区网络基础设施、重要域名系统等安全防护，利用远程检测等技术手段，强化对重点区域的网络安全风险评估和隐患排查，为疫情防控指挥调度、医疗救助、远程办公和人民群众生产生活提供安全可靠的基础网络服务。

（三）加强涉疫情网络安全威胁监测处置。按照公共互联网网络安全威胁与处置工作机制，对伪装成疫情信息传播网络病毒或相关钓鱼网站、恶意邮件、恶意程序，以及医疗机构、疫情防控物资生产企业所属网络系统存在受控、漏洞等情况加大监测力度，利用网络安全威胁信息共享平台及时通报有关情况，发布风险提示，协助相关单位采取有效处置措施，从源头上降低网络安全风险，维护疫情防控期间的网络秩序和公共利益。

（四）加强疫情期间电话用户入网服务保障。鼓励基础电信企业、移动通信转售企业通过网络渠道为用户办理电话入网实名登记手续，引导广大用户利用电信企业门户网站、手机APP、掌上营业厅等线上方式办理电话入网手续及手机卡。基础电信企业、移动通信转售企业应加大对网络渠道销售手机卡业务及办理流程的宣传，做好相关业务系统和平台的保障，切实为广大用户提供便利。

二、加强信息安全和网络数据保护

（五）加强涉疫情电信网络诈骗防范。充分发挥电信网、互联网诈骗技术防范系统等技术平台作用，切实强化对涉疫情诈骗电话、短信的精准分析和依法快速处置；针对涉防疫医疗物资购买、航班行程退改签等诈骗新手法新套路，及时研判预警，对相关涉诈网站、域名、APP、账户依法快速处置。进一步加强与公安机关工作配合和信息沟通，及时通报涉疫情电信网络诈骗信息线索。充分利用微信、微博、短彩信、APP等平台开展涉疫情电信网络诈骗的宣传引导和风险提示。

（六）加强网上涉疫情相关信息监测处置。严格落实维护网上信息安全主体责任，依托全国互联网信息安全管理系统等技术手段，配合相关部门及时做好网上涉疫情相关风险隐患信息动态监测、违法不实信息应急处置等支撑保障工作，及时发现、积极化解、稳妥处置因疫情引发的网上不安定不稳定因素。

（七）加强个人信息和数据安全保护。落实《中央网络安全和信息化委员会办公室关于做好个人信息保护利用大数据支撑联防联控工作的通知》等要求，在积极利用行业数据、平台等支撑联防联控工作中，切实处理好数据使用与数据保护的关系，进一步强化个人信息收集、使用等各环节的规范管理，将个人信息和数据安全保护各项要求落到实处。

三、进一步强化责任落实和工作协同

（八）加强网络安全责任落实。各地通信管理局要加强统一领导和统筹协调，做到守土有责、守土担责、守土尽责，指导督促地方信息通信行业做好疫情防控网络安全保障工作。各基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业要切实承担起网络安全主体责任，充分发挥网络安全技术支撑保障作用，为打赢疫情防控阻击战作出积极贡献。

（九）加强网络安全信息报送。湖北省通信管理局、基础电信企业集团有限公司在疫情防控期间每日向部（网络安全管理局）报送疫情防控重点用户网络安全保障情况、涉疫情网络安全监测预警信息、针对疫情防控开展的网络安全防护工作情况和其他重大事项。各单位发生或发现重大网络安全事件要第一时间报部（网络安全管理局）。

特此通知。