

安全和发展是一体之两翼、驱动之双轮。纵观人类社会发展历程,每一次重大技术革新,既带来发展动能,也带来新的安全挑战。

党的十八大以来,习近平总书记高度重视发展和安全,强调要“坚持统筹发展和安全,坚持发展和安全并重”“必须坚持高质量发展和高水平安全良性互动,以高质量发展促进高水平安全,以高水平安全保障高质量发展”。

安而不忘危,治而不忘乱。当前,人工智能等新兴技术蓬勃发展,正深度重构国家安全的边界与体系。如何科学研判网络安全领域的新形势新特征新挑战,有效防范化解智能化带来的各类安全风险,牢牢守住网络空间安全防线,已经成为新时代必须回答好的重大现实课题。

9月14日,以“网络安全为人民,网络安全靠人民——智能时代 网安护航”为主题的2026年国家网络安全宣传周开幕式在山东济南举行。同日,网络安全技术高峰论坛主论坛举办。9月14日至20日,宣传周将在全国范围内统一开展。来自政、产、学、研、用各界的嘉宾齐聚泉城,围绕人工智能安全、关键信息基础设施防护、网络身份认证、数据跨境流动等前沿议题深入研讨,为智能时代网络安全治理建言献策。

发布《人工智能安全治理框架3.0》

开幕式上,全国网络安全标准化技术委员会发布《人工智能安全治理框架3.0》,受到各界广泛关注。这是贯彻落实《全球人工智能治理倡议》的又一重要举措。2024年、2025年,网安标委先后发布《人工智能安全治理框架1.0》《人工智能安全治理框架2.0》,为人工智能安全治理提供了基础支撑。

为应对人工智能发展新趋势、回应安全治理新挑战,在国家互联网信息办公室指导下,网安标委组织中国网络空间研究院、国家互联网信息办公室数据与技术保障中心等专业机构、科研院所、行业企业,研究编制了《人工智能安全治理框架3.0》。该框架秉持以人为本、向上向善理念,坚持强化风险意识、确保安全可控的指导原则,延续“风险分类、技术应对、综合治理”的核心逻辑,与时俱进更新风险分类,优化调整技术应对和综合治理措施,以促进提升人工智能安全治理共识和风险防范应对能力,确保人工智能技术造福于人类。

提前布局未成年人保护

网络安全技术高峰论坛发布了《青少年发展蓝皮书:全国未成年人互联网使用情况调查报告》。报告显示,我国未成年网民规模已达1.98亿人,互联网普及率高达98.3%,城乡未成年人互联网普及率差距缩小至0.4个百分点,网络普惠成效显著进一步显现。

人工智能的快速普及,为未成年人网络安全带来新的课题。调查数据表明,78.5%的受访未成年网民已在学习、创作或娱乐中使用过AI工具,未成年人成为AI应用的高频群体。但与此同时,不少未成年人缺乏识别AI生成内容、甄别算法偏见、把握伦理边界的能力,83%的受访教师对学生滥用AI的风险表示担忧。

共青团中央书记处第一书记阿东表示,要引领

论坛上,中国工程院院士、中关村实验室首席科学家云晓春聚焦AI供应链安全展开探讨。他指出,AI供应链涵盖数据、模型、软件、算力、平台、工具、服务7类相互依赖资产,任何一类资产发生来源变更、版本迭代,都可能改变最终安全状态。相较传统软件供应链,AI供应链还面临数据、模型和运行时三类新风险。“AI供应链不是一次构建、一次验收,而是持续的配置与行为管理。”他建议安全工作应前置,在开源构建阶段开展验证,同时强化运行时风险发现和处置。

“人工智能正在重塑数据安全治理逻辑,传统安全防护体系已难以适应新形势。”中孚信息股份有限公司董事长、总裁魏东晓则从数据安全治理角度分析,攻击者已能利用大模型将窃取行为伪装成正常业务,治理思路必须从“看异常”转向“识风险”,解析人、机、数、权、事之间的动态关联。据悉,中孚信息据此构建了完整体系,并在省市网信部门指导下推动安全能力向基层落地。

青年积极参与网络生态治理,营造安全有序、风清气正的网络空间,依法打击利用网络侵害青少年行为,培养青少年适应数智时代的全面发展能力,引领青年争做“中国青年好网民”,发挥中外青年网络交往活跃优势,为构建公正合理的全球人工智能治理体系和网络空间命运共同体作出积极贡献。

在网络安全意识与素养提升分论坛上,奇安信集团副总裁张龙表示,网络安全意识的培养应从青少年时期抓起。据他介绍,为提升青少年网络安全素养、培养未来科技人才,该企业不仅举办“天枢杯”青少年人工智能安全创新大赛,每年还开展50余场网络安全研学实践活动,通过沉浸式讲解、专题讲座等形式,帮助孩子们在实践中拓宽科技视野、夯实安全认知。

视角从开发态延伸到运营态,围绕网络安全运营、网络韧性、自动化规避做好特性开发;通过AI加持,使安全运营更可视、可管、可控;同时,通过运营者和供应商之间围绕漏洞及安全事件的信息共享,把安全事件溯源结果反馈到设备前端,使已知风险类型得到系统性修复。

中国联合网络通信集团有限公司副总经理苗守野建议,打破行业壁垒和技术隔阂,从上游基础设施安全到中游平台服务安全,再到下游应用场景安全,实现全链条贯通与协同;推动“安全AI化”和“AI安全化”双向发力,共建产业技术创新新规则,完善安全治理体系,推进人工智能安全国家标准规范建设;深入推进网络安全生态联动共治,持续深化政产学研用协同创新,健全政府、高校、企业多维联动机制,建立联合实验室,以安全产业园等创新载体为依托,推动网络安全与实体经济深度融合。

(据《光明日报》)

筑牢智能时代的网络安全防线

——二〇二六年国家网络安全宣传周亮点观察



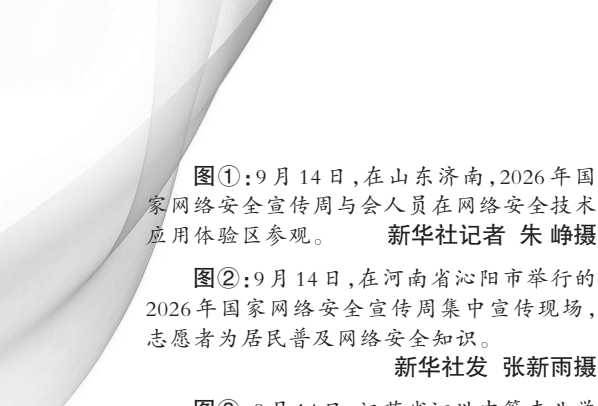
图①:9月14日,在山东济南,2026年国家网络安全宣传周与会人员网络安全技术应用体验区参观。

新华社记者 朱峥摄



图②:9月14日,在河南省沁阳市举行的2026年国家网络安全宣传周集中宣传现场,志愿者为居民普及网络安全知识。

新华社发 张新雨摄



图③:9月14日,江苏省泗洪中等专业学校的学生挑战网络安全知识趣味答题。

新华社发 许昌亮摄

让安全与智能相互赋能

网络安全是人工智能行稳致远的重要基础和现实保障。“进入智能时代,网络安全的风险边界正在变化。”中孚信息股份有限公司副总裁王金国认为,过去更多关注服务器、终端和网络边界,如今攻击对象进一步向智能应用、数据、模型和智能体延伸,数据流动、权限调用、智能体执行等都可能成为新的风险点。“智能时代 网安护航”,就是一手抓AI技术赋能安全,一手抓AI安全治理,让安全更智能,也让AI应用更安全。

“数字时代的安全必须坚持共建共享,构建立体协同防御体系,尽快建立AI时代的风险共识。”华为技术有限公司全球网络安全官杨晓宁认为,人工智能时代需要更加关注训练数据、AI模型、Agent智能体等数字化资产的统一管理,需要对Agent等“数字员工”的身份和权限进行有效管理,提升机制化管理能力。

杨晓宁建议,在产品开发中,把安全运营维

延伸阅读

网安周是个什么“周”? 今年为何选择在山东?

点开手机扫码支付,居家设备联网值守,政务事项线上办理,工厂车间智能调度……数字生活早已融入普通人的日常。可便利背后,电信诈骗、信息泄露、算法陷阱等风险如影随形。

每年九月,国家网络安全宣传周如约而至,这场全民盛会,正是守护亿万网民数字生活的一道重要防线。2026年网安周将于9月14日至20日在全国范围内统一开展,开幕式与核心高峰论坛落地山东济南。不少人好奇:年年刷屏的网安周,到底是个什么“周”?关乎民生、关乎产业、关乎国家安全的重磅活动,今年为何偏偏花落山东?

很多人会误以为,网安周只是一场行业展会,或是一次简单的科普宣讲。事实上,它是国内规格最高、覆盖最广的年度网络安全全民活动,由十部门联合举办,自创办起就传递一个朴素认知:网络安全从来不是技术专家、企业机构的独角戏,而是人人有责、人人受益的公共事业。

今年主题定为“网络安全为人民,网络安全靠人民——智能时代 网安护航”,精准锚定当下时代特征。人工智能、大模型、算力网络加速落地,万物互

联重塑生产生活。但技术是双刃剑,越是数字化走向深入,安全的缺口越不能忽视。一次随意的App权限授权,一条轻信的陌生短信,都可能造成个人财产、隐私受损;工业互联网、城市算力平台一旦遭遇网络攻击,影响的则是产业运转乃至公共治理。

网安周存在的意义,就是打破大众的认知误区:很多人觉得网络安全离自己很远,实则每一次点击、每一次授权、每一次线上交易,都与安全息息相关。它一边向全社会普及网络安全知识、传授防护技能,筑牢全民安全意识“防火墙”;一边集中展示我国网安技术成果、产业实力、治理成效等,凝聚政企社多方合力,补齐智能时代网络安全短板。

厘清了网安周的价值内核,更值得探究的是:全国省市众多,这场国家级重磅盛会,今年为何锁定山东、落地济南?

国家级盛会选址,从来不是随机抽签,而是对区域数字实力、产业生态、治理能力的综合考量。网安周落地山东、主会场放在济南,背后是层层递进的硬核支撑。

山东是名副其实的数字与算力大

省,拥有济南、青岛两大国家级骨干互联网直联点,是国内少有的“双枢纽”省份。全省16市全部建成千兆城市,5G基础设施遍布城乡,总算力规模突破2.73万P,智能算力占比超过60%。济南、青岛、枣庄三大算力枢纽承载全省65%的算力资源,大模型产品达到317个,人工智能持续赋能矿山、交通、制造等实体经济。数字化场景越丰富,安全需求就越迫切。在这里举办网安周,既是直面智能时代的安全挑战,也能为全国探索可复制、可推广的网安治理经验。

济南更是承接本次盛会的核心支点。作为全国第二个中国软件名城,这里还是国内唯一同时拥有国家人工智能先导区、试验区、工业互联网示范区的城市。全市集聚200余家网安相关企业,2025年网安核心产业规模突破190亿元,占据全省六成份额。济南高新区作为首批国家网络安全教育技术产业创新发展试验区之一,更是全国唯一一个拿下国家网信人才培养基地项目的试验区。从算力平台“泉惠算一济南词元工厂”上线,到公共数据授权运营平台打通数百项公共数据资源,济南在数据要素流通、算力安全管控、网安人才

引育上持续破局,形成技术、产业、人才联动的完整生态。

不止产业底座,亿级人口的民生场景,是山东承办网安周独有的价值。山东经济体量稳居全国前列,海量网民、千万市场主体,构成了网络安全宣传最好的试验场。在这里普及网络安全知识,能触达更广的普通群众,在真实场景中检验网络安全技术,让网络安全走出实验室,真正扎根民生。多年来,山东持续推进网信科普、网络风险常态化治理,兼顾制造业大省的厚重根基与数字创新的活力。

“备豫不虞,为国常道。”网络安全早已不是事后堵漏的被动补救,而是数字发展的前置压舱石。小到个人隐私,中到企业经营数据,大到国家数字空间安全,安全防线片刻不能松懈。

风起齐鲁,网安护航。以此次盛会为契机,山东将汇聚全国顶尖人才、技术与资源,持续打磨算力安全、数据安全、工业互联网安全防护能力,让数字发展的红利更安稳、更普惠、更持久地惠及千家万户,为高质量发展撑起可靠的数字安全屏障。

(据闪电新闻)

2026年国家网络安全宣传周校园日见闻

■ 新华社记者 萧海川

点开陌生链接获得“幸运大奖”却要先垫付钱款、陌生网友声称有“内部渠道”可超低价购买虚拟人物皮肤……主人公就要落入网络诈骗陷阱,所幸身边好友、在线网警及时出手揭露诈骗图谋。

2026年国家网络安全宣传周校园日活动9月15日在山东省济南信息工程学校举行。在活动日启动仪式上,一部由小学生们排演的网络安全情景短剧,情节生动、表演传神,引得观众阵阵掌声。

“网络安全与每个人都息息相关,网络诈骗离我们并不遥远。”济南信息工程学校2025级计算机网络技术二班学生张盛烨说,借助在课堂上所学知识,自己曾为家人识别出一个假冒的常用软件分发网站,避免家人遭遇钓鱼诈骗,“经过这件事,更加觉得每个人都要有足够的网络安全知识和警惕性”。

“教好一个孩子,更能保护好一个家庭。学生能成功预防网络诈骗,也让老师十分欣慰。”有31年教龄的济南信息工程学校计算机网络专业负责人

楚扬告诉记者,网络安全知识已被有机融入到学校日常教学中。相关课程设置既有面向国家级竞赛的实训课,也有针对日常生活细节的通识课。

此次活动日现场突出体验感和互动性。在校园网络安全科普互动展上,专业的网络安全企业带来多项模拟设备,学生可亲身体验针孔摄像头窃密、黑客改号、AI换脸等技术,进一步绷紧网络安全风险弦。

“随着用网人群低龄化,网络安全教育更应当从小抓起。”校园日活动当天,齐鲁工业大学(山东省科学院)网络安全学院院长马宾为济南市部分中小學生带来一场网络安全专题讲座。他认为,网络越触手可及,风险教育越不能片刻松懈;安全知识越普及,青少年群体越能更多享受智能时代的红利。

“当前中小學生群体触网更早、用网更深,意味着网络安全素养必须及时跟上。”济南市电化教育馆馆长隋东庆表示,近年来,济南市采取线上专家授课、线下主题班会等多种形式,推动中小学校的网络安全教育走进课堂。同时积极适应人工智能的迅猛发展,协助学生会用,用好人工智能工具。

■ 李政璇

步入人工智能时代,网络安全早已不再是单纯的技术攻防命题,而是关乎国家安全、社会治理、民生福祉的综合性时代考题。面对人工智能衍生的新风险、新挑战,筑牢网络安全屏障的重要性越发凸显。2026年国家网络安全宣传周以“网络安全为人民,网络安全靠人民——智能时代 网安护航”为主题,正是立足技术变革大势,凝聚全社会力量共护数字家的重要实践。

人工智能技术迭代普及,也衍生出新的安全风险。过去网络攻击往往需要攻击者掌握较高的专业技术,如今生成式人工智能大幅降低攻击门槛,模糊攻击主体边界,网络威胁朝着智能化、规模化、隐蔽化方向演进。比如,不法分子依托大模型批量炮制高仿真钓鱼邮件、定制诈骗话术,借助深度伪造技术合成音视频,冒充亲友、相关部门实施诈骗,成为侵害广大人民群众财产安全的突出隐患;深度伪造内容还能够编造虚假信息,混淆公众认知,扰动网络舆论,影响社会公共秩序。

此外,数据安全与隐私泄露风险也在伴随人工智能应用同步放大。人工智能训练运行高度依赖海量数据,个人画像、商业资料、政务信息等一旦被随意采集、投喂模型,极易造成敏感信息外泄。与此同时,各类高权限智能体快速兴起,一旦被恶意利用,就可能越权访问系统,执行高危操作,成为网络攻击的“跳板”与“木马”。

风险形态迭代升级,不断倒逼安全防护思路全方位革新。近年来,我国不断探索适配智能时代的新应对路径。基于“以AI对抗AI”的攻防现实,加快构建智能化主动防御体系成为必由之路,推动网络安全防护模式从事后处置转向事前预警、动态感知的主动免疫,补齐传统安全工具应对未知风险的短板,不断提升整体安全防护韧性。

近年来,我国出台《生成式人工智能服务管理暂行办法》,开展大模型备案管理;迭代更新《人工智能安全治理框架》,配套出台多项国家标准,对训练数据、模型服务、政务大模型应用划定安全基线,今年宣传周期间发布《人工智能安全治理框架3.0》,为行业实践提供新指引;不断建设中文互联网语料资源平台,输出高质量权威数据集,为大模型价值观纠偏提供支撑;监管模式由静态合规向动态运行合规转变,推动落实算法设计、数据训练、模型部署全生命周期风险评估,引导技术创新始终行走在法治轨道之上。

网络安全治理从来不是政府、企业、平台的独角戏,人民群众既是网络安全的受益者,更是参与者、守护者。政府、企业、机构、社会公众多方协同发力,才能织密全方位的网络安全防护网。面对人工智能带来的机遇与考验,我们既要积极拥抱技术变革,释放数字技术赋能千行百业的巨大动能;也要时刻绷紧网络安全之弦,清醒地识别各类新型风险隐患。坚持统筹发展和安全,推动技术防护、制度建设、全民参与同向发力。(据《光明日报》)