# 2024年全民国家安全教育日相关学习资料（大全五篇）

来源：网络 作者：流年似水 更新时间：2024-08-03

*第一篇：2024年全民国家安全教育日相关学习资料2024年全民国家安全教育日相关学习资料2024年“4·15”全民国家安全教育日1.国家安全是头等大事，维护国家安全人人有责。2.国家安全是安邦定国的重要基石，维护国家安全是全国各族人民根本...*

**第一篇：2024年全民国家安全教育日相关学习资料**

2024年全民国家安全教育日相关学习资料

2024年“4·15”全民国家安全教育日

1.国家安全是头等大事，维护国家安全人人有责。

2.国家安全是安邦定国的重要基石，维护国家安全是全国各族人民根本利益所在。

3.防范化解各类安全风险，不断提高人民群众的安全感、幸福感。

4.自觉践行总体国家安全观，筑牢坚如磐石的首都政治“护城河”。

5.统筹传统安全和非传统安全，为决胜全面建成高质量小康社会提供坚强保障。

6.把生物安全纳入国家安全体系，全面提高国家生物安全治理能力。

7.始终把人民群众生命安全和身体健康放在第一位。

8.文明祭扫，平安清明。

9.坚决革除滥食野生动物的陋习，从源头上控制重大公共卫生风险事。

什么是国家安全?

根据《国家安全法》第二条规定，国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

国家安全包括哪些方面?

国家安全领域主要包括政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、网络安全、生态安全、资源安全、核安全、海外利益安全、太空安全、深海安全、极地安全和生物安全等领域。

国家安全教育日的由来?

2024年7月1日全国人大常委会通过的《国家安全法》将每年4月15日定为全民国家安全教育日，全民国家安全教育日是为了增强全民国家安全意识，维护国家安全而设立的节日。

公民在维护国家安全中的义务有哪些?

《国家安全法》第七十七条规定：公民和组织应当履行下列维护国家安全的义务：

(1)遵守宪法、法律法规关于国家安全的有关规定;

(2)及时报告危害国家安全活动的线索;

(3)如实提供所知悉的涉及危害国家安全活动的证据;

(4)为国家安全工作提供便利条件或者其他协助;

(5)向国家安全机关、公安机关和有关军事机关提供必要的支持和协助;

(6)保守所知悉的国家秘密;

(7)法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

公民在维护国家安全中有哪些权利?

(1)公民和组织支持、协助国家安全工作的行为受法律保护。因支持、协助国家安全工作，本人或者其近亲属的人身安全面临危险的，可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

(2)公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿;造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待。

(3)公民和组织对国家安全工作有向国家机关提出批评建议的权利，对国家机关及其工作人员

日常生活中应警惕哪些危害国家安全的活动?

(1)一些可疑人员未经批准到内部作调查，进行科技、经济、企业等情况搜集。发现这种情况不能随意提供，并向当地公安机关或国家安全机关报告。

(2)警惕境外电台、电视、网络等传媒的煽动、造谣。

(3)一些境外组织和人员经常出现在我军事、保密单位周边，乘机盗取秘密情报和信息。如遇有可疑人员要立即报告。

(4)一些有境外背景的组织和个人，利用一些群众不满情绪，煽动与政府对抗。遇到这些情况，应立即报告。

发现国家秘密已经或可能泄露时，我们应当采取哪些措施?

(1)拾获属于国家秘密的文件、资料和其他物品，应当及时送交有关机关、单位或保密工作部门。

(2)发现有人买卖属于国家秘密的文件、资料和其他物品，应当及时报告保密工作部门或者国家安全机关、公安机关处理。

(3)发现有人盗窃、抢夺属于国家秘密的文件、资料和其他物品，有权制止，并应当立即报告。

(4)发现泄露或可能泄露国家秘密的线索，应当及时向国家安全机关举报。

什么是12339?

“12339”是国家安全机关受理公民和组织举报电话。这条热线是由国家安全部设立的，以方便公民和组织向国家安全机关举报间谍行为或线索。

《中华人民共和国网络安全法》由全国人民代表大会常务委员会于2024年11月7日发布，自2024年6月1日起施行。是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。《网络安全法》将近年来一些成熟的好做法制度化，并为将来可能的制度创新做了原则性规定，为网络安全工作提供切实法律保障。

本法在以下几个方面值得特别关注：

一、《网络安全法》的基本原则：第一，网络空间主权原则。第二，网络安全与信息化发展并重原则。第三，共同治理原则。

二、《网络安全法》提出制定网络安全战略，明确网络空间治理目标，提高了我国网络安全政策的透明度;

三、《网络安全法》进一步明确了政府各部门的职责权限，完善了网络安全监管体制;

四、《网络安全法》强化了网络运行安全，重点保护关键信息基础设施;五、《网络安全法》完善了网络安全义务和责任，加大了违法惩处力度;六、《网络安全法》将监测预警与应急处置措施制度化、法制化。

《中华人民共和国网络安全法》全文

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理;不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;

(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;

(三)采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;

(四)采取数据分类、重要数据备份和加密等措施;

(五)法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序;发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护;在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意;涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动;不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具;明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

(一)设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查;

(二)定期对从业人员进行网络安全教育、技术培训和技能考核;

(三)对重要系统和数据库进行容灾备份;

(四)制定网络安全事件应急预案，并定期进行演练;

(五)法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估;法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

(一)对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

(二)定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力;

(三)促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;

(四)对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息;发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录;对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

(一)要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测;

(二)组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度;

(三)向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

(一)设置恶意程序的;

(二)对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的;

(三)擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正;拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告;拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款;情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作;受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款;情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款;情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得;拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正;拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

(一)不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的;

(二)拒绝、阻碍有关部门依法实施的监督检查的;

(三)拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正;对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚;构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任;国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

(一)网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

(二)网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

(三)网络运营者，是指网络的所有者、管理者和网络服务提供者。

(四)网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(五)个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自2024年6月1日起施行。

**第二篇：2024全民国家安全教育日宣传资料**

2024全民国家安全教育日宣传资料

《国家安全法》第十四条规定：“每年4月15日为全民国家安全教育日。”

古语云：生于忧患，死于安乐。历史也一再证明：盛世并不意味着永享太平。当今世界正处在大变革大调整时期，虽然和平发展仍是时代主题，但各种可以预见和难以预见的安全风险挑战前所未有。国家安全不仅关乎国家的兴亡，还关乎每个公民的切身利益；维护好了国家安全，既能保护国家利益，也能保护个体利益，而一旦国家安全受损，我们就有可能付出巨大的代价。在国家安全法中设立全民国家安全教育日，有助于帮助全体公民认清国家安全形势、增强危机忧患意识、树立国家安全观念，认真贯彻执行国家安全法和相关法律，积极支持配合国家安全机关履行职责，为维护国家安全作出应有贡献。

下面我们就一起了解国家安全，学习国家安全法知识。

一、《国家安全法》什么时候通过和生效的？

新的《国家安全法》是XX年7月1日十二届全国人大常委会第十五次会议表决通过的。以法律对政治安全、国土安全、军事安全、文化安全、科技安全等11个领域的国家安全任务进行了明确，自公布之日起实施。

二、公民在维护国家安全中的义务有哪些？

《国家安全法》第七十七条规定：公民和组织应当履行下列维护国家安全的义务：

(1)遵守宪法、法律法规关于国家安全的有关规定；

(2)及时报告危害国家安全活动的线索；

(3)如实提供所知悉的涉及危害国家安全活动的证据；

(4)为国家安全工作提供便利条件或者其他协助；

(5)向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；

(6)保守所知悉的国家秘密；

(7)法律、行zd规规定的其他义务。

任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

三、公民在维护国家安全中有哪些权利？

(1)公民和组织支持、协助国家安全工作的行为受法律保护。因支持、协助国家安全工作，本人或者其近亲属的人身安全面临危险的，可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

(2)公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿；造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待。

(3)公民和组织对国家安全工作有向国家机关提出批评建议的权利，对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

四、公民在日常工作生活中应提高警惕注意发现哪些危害国家安全的活动？

(1)一些可疑人员未经批准到内部作调查，进行科技、经济、企业等情况搜集。发现这种情况不能随意提供，并向当地公安机关或国家安全机关报告。

(2)警惕境外电台、电视、网络等传媒的煽动、造谣。

(3)一些境外组织和人员经常出现在我军事、保密单位周边，乘机盗取秘密情报和信息。如遇有可疑人员要立即报告。

(4)一些有境外背景的组织和个人，利用一些群众不满情绪，煽动与政府对抗。遇到这些情况，应立即报告。

五、发现国家秘密已经或可能泄露时，我们应当采取哪些措施？

(1)拾获属于国家秘密的文件、资料和其他物品，应当及时送交有关机关、单位或保密工作部门。

(2)发现有人买卖属于国家秘密的文件、资料和其他物品，应当及时报告保密工作部门或者国家安全机关、公安机关处理。

(3)发现有人盗窃、抢夺属于国家秘密的文件、资料和其他物品，有权制止，并应当立即报告。

(4)发现泄露或可能泄露国家秘密的线索，应当及时向国家安全机关举报。

六、《反恐怖主义法》什么时候生效的？

《反恐怖主义法》是XX年12月27日第十二届全国人民代表大会常务委员会第十八次会议通过的，自XX年1月1日起施行。

七、公民在反恐怖主义中义务和权利？

(1)任何单位和个人都有协助、配合有关部门开展反恐怖主义工作的义务，发现恐怖活动嫌疑或者恐怖活动嫌疑人员的，应当及时向公安机关或者有关部门报告。

(2)对举报恐怖活动或者协助防范、制止恐怖活动有突出贡献的单位和个人，以及在反恐怖主义工作中作出其他突出贡献的单位和个人，按照国家有关规定给予表彰、奖励。

八、《反间谍法》什么时候通过和生效的？

《反间谍法》是XX年12月27日第十二届全国人民代表大会常务委员会第十八次会议通过的，自XX年1月1日起施行。

九、公民在反间谍工作中有哪些义务和权利？

(1)公民和组织应当为反间谍工作提供便利或者其他协助。因协助反间谍工作，本人或者其近亲属的人身安全面临危险的，可以向国家安全机关请求予以保护。国家安全机关应当会同有关部门依法采取保护措施。

(2)公民和组织发现间谍行为，应当及时向国家安全机关报告；向公安机关等其他国家机关、组织报告的，相关国家机关、组织应当立即移送国家安全机关处理。

(3)在国家安全机关调查了解有关间谍行为的情况、收集有关证据时，有关组织和个人应当如实提供，不得拒绝。

(4)任何公民和组织都应当保守所知悉的有关反间谍工作的国家秘密。

(5)任何个人和组织都不得非法持有属于国家秘密的文件、资料和其他物品。

(6)任何个人和组织都不得非法持有、使用间谍活动特殊需要的专用间谍器材。

(7)对协助国家安全机关工作或者依法检举、控告的个人和组织，任何个人和组织不得压制和打击报复。

十、公民或组织发现危害国家安全可疑行为或其他破坏活动时，请拨打举报电话：12339。

**第三篇：全民国家安全教育日演讲稿**

全民国家安全教育日演讲稿：

国家安全,由我们共同守护!居安思危,思则有备,备则无患。

2024年4月15日,是《中华人民共和国国家安全法》颁布实施以来的第三个全民国家安全教育日。也许您觉得这部法律很陌生,国家安全,这话题太大了,但事实上它与我们每个人的利益息息相关。

一、增强维护国家安全意识

国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态,以及保障持续安全状态的能力。国家安全包括:政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、网络安全、生态安全、资源安全、核安全。

二、总体国家安全观

一方面,不能以一己私利危害国家安全;另一方面,要为国家安全工作提供必要的配合,因支持、协助国家安全工作,个体的利益受到威胁时可以向国家寻求保护。

三。、什么是间谍行为

根据《中华人民共和国反间谍法》,间谍行为是指下列行为:

间谍组织及其代理人实施或者指使、资助他人实施,或者境内外机构、组织、个人与其相勾结实施的危害中华人民共和国国家安全的活动;

参加间谍组织或者接受间谍组织及其代理人的任务的;

间谍组织及其代理人以外的其他境外机构、组织、个人实施或者指使、资助他人实施,或者境内机构、组织、个人与其相勾结实施的窃取、刺探、收买或者非法提供国家秘密或者情报,或者策动、引诱、收买国家工作人员叛变的活动;

为敌人指示攻击目标的;

进行其他间谍活动的。

近年来,在日常生活中,危害国家安全的案件层出不穷,比如无意中为国外间谍当向导而泄密、军迷在社交网站晒资料泄密、国家机关工作人员朋友圈发涉密信息等。

国家安全不仅关乎国家的兴亡,还关乎每个公民的切身利益。一旦国家安全受损,我们就有可能付出巨大的代价。而维护国家安全,需要发挥每个公民的力量,打一场“人民战争”。公民或组织发现危害国家安全可疑行为或其他破坏活动时请拨打由国家安全部设立的12339举报电话。

2024年4月12日

**第四篇：2024全民国家安全教育日讲稿**

全民国家安全教育日

2024年4月15日，是《中华人民共和国国家安全法》颁布实施以来的第三个全民国家安全教育日。也许您觉得这部法律很陌生，国家安全，这话题太大了，与咱们普通老百姓的生活，离得太远。然而，事实上，真的如此吗？

近年来，在日常生活中，危害国家安全的案件层出不穷，比如无意中为国外间谍当向导而泄密、军迷在社交网站晒资料泄密、国家机关工作人员朋友圈发涉密信息等。所以国家安全，和我们每个人的生活，息息相关。

问题一：全民国家安全教育日咋来的？

答：2024年7月1日，第十二届全国人民代表大会常务委员会第十五次会议通过了《中华人民共和国国家安全法》，该法自公布之日起施行。国家安全法第14条规定：每年4月15日为全民国家安全教育日。

问题二：什么是国家安全？

答：根据《国家安全法》第2条规定，国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

问题三：国家安全包括哪些方面？

答：为了体现总体国家安全观的要求，《中华人民共和国国家安全法》从政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等11个领域 对国家安全任务进行了明确。

问题四：什么是12339？

答：2024年11月，全国国家安全机关向社会发出通告，12339，是国家安全机关受理公民和组织举报电话。这条热线是由国家安全部设立的，以方便公民和组织向国家安全机关举报间谍行为或线索。

说起危害国家安全，大家可能首先想到的就是间谍，这也是电影大片里演得比较多的，如007、FBI、CIA之类的人物。不要以为间谍行为离我们很远。给大家分享两个真实的案例。

案例一：90后廖某因为受QQ好友的蛊惑，拍摄军港停泊的军舰舰号来获取报酬，触犯了法律。

案例二：李某受境外间谍“飞哥”指示，成为境外间谍情报机关的窃密工具，长期为其订购和提供境内内部军事刊物，并对重要军事基地进行长期定点定时观察，大量军事基地动态情况和军事装备的照片通过他的手流向境外，对国家军事安全造成严重威胁。据不完全统计，2024年以来，“飞哥”利用“网上书店”、军事爱好者网站等网络渠道，在广东省策反运用12人，在全国范围内更有20多个省市40名境内人员被“飞哥”策反运用。事后以上人员均被法律制裁。

危害国家安全的行为有哪些？ 根据《国家安全法》规定，危害国家安全的行为有以下五个方面：①阴谋颠覆政府、分裂国家、推翻社会主义制度的；②参加间谍组织或者接受间谍组织及其代理人任务的；③窃取、刺探、收买、非法提供国家秘密的；④策动、勾引、收买国家工作人员叛变的；⑤进行危害国家安全的其他破坏活动的。

设立全民国家安全教育日的意义

首先，有利于贯彻落实总书记提出的“总体国家安全观”。2024年4月15日，总书记在中央国家安全委员会第一次会议上首次明确提出了“总体国家安全观”，这是新时期中国共产党维护国家安全的根本方针政策。国家安全法规定：国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。公众广泛参与全民国家安全教育日，将获得弘扬总体国家安全观的良好效果。

其次，有利于提高政府和社会公众维护国家安全的法律意识。国家安全法以“总体国家安全观”作为指导思想，规定了一系列不同于传统国家安全观的国家安全制度，将国家安全的内涵扩展到政治、经济、文化和社会各领域，突出强调了维护国家安全不仅仅是专门机关的任务，而是所有国家机关、社会组织和公民的义务和职责。通过全民国家安全教育日的一系列活动，可以让政府和社会公众有效地了解国家安全法提出的各项要求，从而强化责任意识，提高大家维护国家安全的能力。

最后，有利于增强国家安全法普法宣传的效果。国家安全法设立全民国家安全教育日，是为了集中地向社会公众传播国家安全方面的知识，便于在短时间内起到良好的宣传效果，让更多的社会公众接触和了解到国家安全方面的法律知识，特别是懂得如何依法履行自身的维护国家安全方面的职责和义务。

由此可见，国家安全法确立全民国家安全教育日，其中最重要的实践意义，就是要动员政府和全社会共同参与到维护国家安全的各项工作中来。维护国家安全与每个人的切身利益密切相关，以人民安全为宗旨也是“总体国家安全观”的核心价值。只有人人参与，人人负责，国家安全才能真正获得巨大的人民性基础，也才能有坚实的制度保障。

关于社会组织和公民个人在维护国家安全方面的义务，国家安全法第77条明确规定了以下几个方面：

（一）遵守宪法、法律法规关于国家安全的有关规定；

（二）及时报告危害国家安全活动的线索；

（三）如实提供所知悉的涉及危害国家安全活动的证据；

（四）为国家安全工作提供便利条件或者其他协助；

（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；

（六）保守所知悉的国家秘密；

（七）法律、行政法规规定的其他义务。此外，该条还明确规定：任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。国家安全不仅关乎国家的兴亡，还关乎每个公民的切身利益；维护好了国家安全，既能保护国家利益，也能保护个体利益，而一旦国家安全受损，我们就有可能付出巨大的代价。

维护国家安全，是为了维护最广大人民的根本利益；维护国家安全，也需要发挥每个公民的力量，打一场“人民战争”。

**第五篇：全民国家安全教育日演讲稿**

提高全民国家安全意识，增强全民国家安全责任

2024年7月1日，确定每年4月15日为全民国家安全教育日。今年的4月15日是新国家安全法实施以来的第二个全民国家安全教育日。

国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。我国当前面临着对外维护国家主权、安全、发展利益，对内维护政治安全和社会稳定的双重压力，各种可以预见和难以预见的风险因素明显增多，非传统领域安全日益凸显，2024年4月15日，总书记在中央国家安全委员会第一次会议上首次明确提出了“总体国家安全观”，这是新时期中国共产党维护国家安全的根本方针政策。2024年7月1日起实施的新国家安全法，国家安全法规定：国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。

郭健利用自己曾经在某研究所工作，参加了我国某项军工项目的设计的经历，为了向网友显示自己掌握的国产某型先进战斗机的专业技术水准。把我国当时在研的歼十战机的秘密公布在网上。

美国情报机构对解放军的某型潜艇十分感兴趣，但对其是否已经投产一直搞不清楚。直到2024年，有关该潜艇的照片出现在中国某军事网站的论坛上，让美国情报机构“得来全不费功夫”。

林兆伟，男，台湾制内间谍人员，他请学生出来吃饭、游乐，还送些本土特色礼物，一段时间之后大家成了“朋友”，请求学生帮忙搜集大陆政治、经济、军事内幕信息和红头文件，“帮忙公司作出决策”。大陆学生的能力其实很难满足林的期望，但“朋友”之邀，学生们很难说不。

象这种经意或不经意的一些行为，都给国家安全造成了巨大的危害。同学们，国家安全不仅关乎国家的兴亡，还关乎每个公民的切身利益；维护好了国家安全，既能保护国家利益，也能保护个体利益，而一旦国家安全受损，我们就有可能付出巨大的代价。维护国家安全，是为了维护最广大人民的根本利益；维护国家安全，也需要发挥每个公民的力量，打一场“人民战争”。国家安全法确立全民国家安全教育日，其中最重要的实践意义，就是要动员政府和全社会共同参与到维护国家安全的各项工作中来。

在此，提醒同学们要树立强烈的国家安全意识，树立国家安全观念，下面再重申国家安全法第77条的规定：

（一）遵守宪法、法律法规关于国家安全的有关规定；

（二）及时报告危害国家安全活动的线索；

（三）如实提供所知悉的涉及危害国家安全活动的证据；

（四）为国家安全工作提供便利条件或者其他协助；

（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；

（六）保守所知悉的国家秘密；

（七）法律、行政法规规定的其他义务。此外，该条还明确规定：任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找