

网络安全为人民 网络安全靠人民

2025年网络安全宣传周

守护网络空间，筑牢安全防线

2025年9月15日-21日

天津市劳动经济学校



- 一. 什么是网络安全
- 二. 网络安全工作职责
- 三. 公民、组织的权利和义务
- 四. 注重个人信息保护
- 五. 防范电信网络诈骗
- 六. 警惕人工智能网络安全风险

目录

CONTENTS

★★★★★



第一部分

什么是网络安全

守护网络空间，筑牢安全防线

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



什么是网络安全

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，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。



第二部分



网络安全工作职责

守护网络空间，筑牢安全防线

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



网络安全工作职责



国家网信部门：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。**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：**网络安全保护和监督管理职责按照国家有关规定确定。



国家支持与促进网络安全工作



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。



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，保护网络知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

国家支持与促进网络安全工作



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。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。



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向社会进行网络安全宣传教育。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。



第三部分

公民、组织的权力和义务

守护网络空间，筑牢安全防线

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



公民、组织的权利和义务

权利

01

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。

02

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。



公民、组织的权利和义务



义务

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

义务

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。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



公民、组织的权利和义务

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。

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。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

第四部分

注重个人信息保护

守护网络空间，筑牢安全防线

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



注重个人信息保护

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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。大家个人信息一旦泄露，便容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。



注重个人信息保护



要优先选择尊重个人信息保护的产品、服务。要仔细审核App请求授权的权限内容，并谨慎授权。要对重要信息进行加密保护。要差异化设置社交平台好友的信息访问权限。不要随意连接免费Wi-Fi热点。不访问陌生网站并留下个人信息。不要在网上随意发布个人照片或其他涉及个人隐私的影像。尊重他人隐私，不随意披露他人隐私信息。

温馨提示

第五部分



防范电信网络诈骗

守护网络空间，筑牢安全防线

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



防范电信网络诈骗



电信网络诈骗是指以非法占有为目的，利用电信网络技术手段，通过远程，非接触等方式，诈骗公私财物的行为。近几年来，此类案件在全国各地频发，涉案金额巨大，成为普法宣传的重点。刷单返利类诈骗，虚假网络投资理财类诈骗，冒充领导、熟人类诈骗。

防范电信网络诈骗

防范小妙招

保护个人信息：不在社交平台随意发布身份证、家庭住址、车票等涉及个人信息的影像资料。不将自拍照等个人照片发给陌生人。

官方渠道办业务：办理银行信用卡及额度提升等业务，一定要通过银行官方平台等可靠渠道进行申请。在网购平台办理退款、退货要通过官方App渠道。

不透露密码：为银行卡、网上银行、手机银行设置复杂程度较高的密码，不向任何人透露或转发短信验证码或其他形式动态密码。

加强对电话、短信或社交媒体信息真实性甄别：尤其在接到涉及钱款的电话、语音或视频时，要通过挂断当前通话，主动拨打联系人或官方客服电话等方式确认。也可以让视频中的人做一些复杂动作，比如张大嘴巴、扮鬼脸、用手在人脸前来回摆动等，以观察人脸是否出现形变。下载和使用官方渠道的手机应用程序：在手机官方应用商店下载App，避免从非官方渠道下载。网购退款等操作一定要通过官方App进行，电商物流客服人员说要给你私下汇款的很可能是诈骗。



第六部分



警惕人工智能网络安全风险

守护网络空间，筑牢安全防线

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



警惕人工智能网络安全风险



人工智能（AI）是一种模拟人类智能的技术，它通过学习、推理和自我修正来执行各种任务。生成式人工智能技术是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。主要是利用机器学习模型，通过对大量数据的学习来理解并创造新内容。AI电商直播，AI自动驾驶，AI合成照片，聊天机器人。

警惕人工智能网络安全风险

生成式人工智能技术在各行业、各领域都具有广泛的应用前景，它不仅影响着人类的生活和生产方式，还为各种行业的创新和发展提供了新的工具和视角，但也潜藏了系列网络安全风险问题。

- 一 利用人工智能技术进行诈骗：诈骗分子通过AI换脸、拟声手段。佯装亲属或好友拨打视频电话，博取信任后，谎称急需资金周转等实施诈骗。
- 二 利用人工智能技术编造谣言：违法行为人往往为了博取流量获得收益，利用AI软件输入关键词生成谣言文章并对外发布，引发大量网络关注，造成不良社会影响
- 三 AI换脸直播带货：有直播间利用AI换脸技术“以假乱真”实现“明星”代言，来增加流量，提高销量。但也侵犯了他人的肖像权、名誉权等权益。



警惕人工智能网络安全风险

网络无边，安全有界
在全社会的共同努力下
网络安全“防火墙”愈加牢固
“保护网”越织越密
亿万民众在网络空间享有更多
获得感、幸福感、安全感

