

2025年国家网络安全宣传周 | 网络安全为人民 网络安全靠人民

在网络强国的重要思想指引下，我国网络安全政策法规体系不断健全，网络安全工作体制机制日益完善，网络安全保障体系和能力建设加快推进，已基本构建起网络安全政策法规体系的“四梁八柱”。

接下来带大家一起了解下
国家网络安全相关法律知识



法律

《中华人民共和国网络安全法》

2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过，自2017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，是让互联网在法治轨道上健康运行的重要保障。



《中华人民共和国数据安全法》

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行。是我国数据领域的基础性法律，也是国家安全领域的一部重要法律。



《中华人民共和国个人信息保护法》

2021年8月20日，第十三届全国人大常委会第三十次会议通过，自2021年11月1日起施行。是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理

利用而制定的法律。



行政法规

《关键信息基础设施安全保护条例》

2021年9月1日起施行，是我国首部专门针对关键信息基础设施安全保护工作的行政法规，也是《中华人民共和国网络安全法》的重要配套法规。



《互联网政务应用安全管理规定》

2024年5月15日，中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部联合发布了《互联网政务应用安全管理规定》，自7月1日起正式施行。规定要求，建设运行互联网政务应用应当依照有关法律、行政法规的规定以及国家标准的强制性要求，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。



《网络数据安全管理条例》

2024年9月国务院总理李强日前签署国务院令，公布《网络数据安全管理条例》（以下简称《条例》），自2025年1月1日起施行。《条例》旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。



了解完相关政策法规

我们对网络安全
有了更进一步的认识
那么，我们在日常生活中
如何保证自己避免
网络上的不法侵害呢？
↓↓↓

一、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。



泄露途径





「温馨提示」

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。

二、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

小额任务佣金小“赚”，大额投入没法提现



虚假网络投资理财类诈骗

“旁门左道”迷双眼，试水投资有风险



冒充领导、熟人类诈骗

诈骗技术新升级，涉及资金要警惕



「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。

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。

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。

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。

三、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

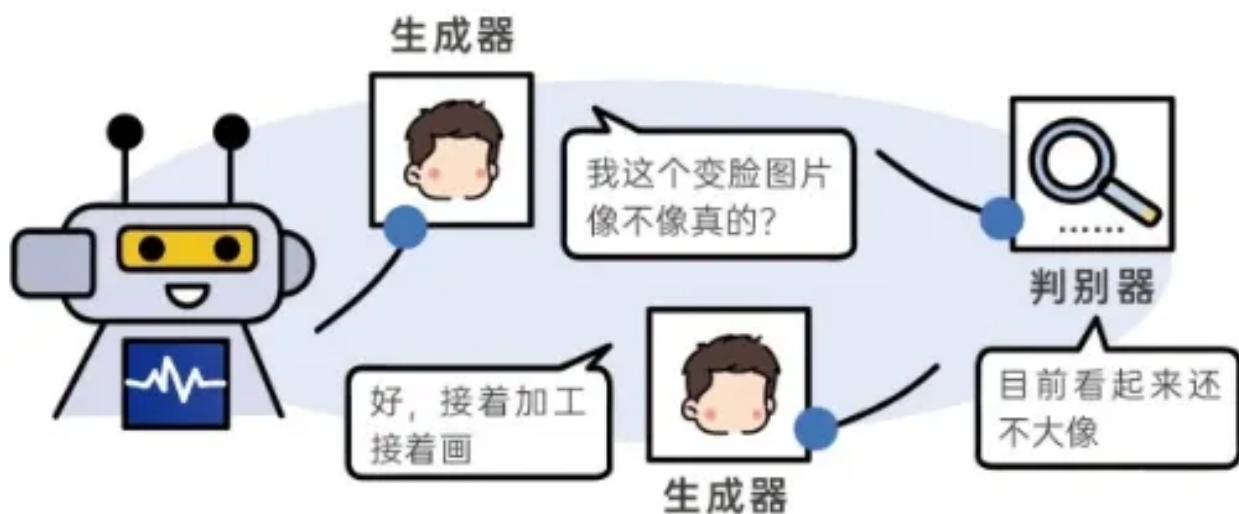


聊天机器人



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建新内容。



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。

（1）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。

（2）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。

（3）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。

以下是结合统计调查工作特点设计的网络安全宣传要点“五要五不要”，旨在帮助统计调查工作人员筑牢网络安全防线：

「网络安全“五要”」

设备与系统防护要严格

安装正版操作系统及杀毒软件，定期更新补丁和病毒库，确保系统漏洞及时修复。
关闭计算机高危端口（如135、139、445端口）及远程服务，避免外部攻击。

数据安全要规范

统计调查数据导出需审批，遵循“最少够用”原则分配权限，严禁越权访问。
使用加密移动存储设备备份数据，定期异地存储，防止数据丢失。

身份认证与访问控制要强化

设置强密码（10位以上，含大小写字母、数字及符号），定期更换密码，启用双因素认证。

在网计算机实行实名制管理，严禁外来人员非授权入网。

安全审计与应急响应要落实

定期开展网络隐患排查，重点检查邮箱使用、密码强度及设备漏洞。
制定网络安全事件应急预案，发现病毒入侵或数据泄露立即上报处置。

安全培训与意识要提升

结合“国家安全教育日”“网络安全宣传周”等活动，组织学习《网络安全法》及统计调查部门相关安全规范。
开展钓鱼邮件、AI诈骗模拟演练，提高对新型攻击手段的辨识能力。

「网络安全“五不要”」

网络设备使用不要违规

禁止私自架设Wi-Fi、无线路由器，统计业务网设备仅限有线连接。
不得关闭杀毒软件或终端管理程序，禁用未审批的VPN系统。

数据传输与存储不要暴露

不得通过微信、QQ、网盘等传输涉密数据，工作邮件仅限内部系统邮箱。
统计调查数据及原始账本禁止上传至云端或未审核的AI平台，严防数据外泄。

外部设备与链接不要轻信

不点击不明邮件链接、不扫描可疑二维码，防范钓鱼网站和木马病毒。
U盘等移动设备使用前须病毒扫描，禁用未授权的外接存储设备。

账号密码管理不要简化

禁用“弱口令”（如生日、123456），避免多账户共用同一密码。
不得在办公电脑保存密码或开启自动登录功能。

个人行为规范不要越界

不在社交媒体晒工作文件、统计报表等敏感信息。

离开办公电脑必锁屏（ Windows电脑快捷键Win+L，国产电脑Linux系统快捷键Ctrl+Alt+L），涉密设备专人专管。

网络安全是统计工作的“生命线”，需全员参与、常抓不懈。

通过制度约束、技术防护和意识提升三重保障，
实现“以安全之盾护统计网络，以精准之笔绘数据蓝图”。
