国家网络安全
宣传周
China Cybersecurity Week

智能时代
网安护航

网络安全为人民　网络安全靠人民

2026年南京市
网络安全宣传周

网络安全知识宣传手册

01

网络安全政策法规

颁布《网络安全法》《数据安全法》《个人信息保护法》等法律法规。

颁布《关键信息基础设施安全保护条例》《网络数据安全管理条例》《互联网政务应用安全管理规定》《国家网络身份认证公共服务管理办法》《国家网络安全事件报告管理办法》《网络安全标识管理办法》等政策文件。

建立关键信息基础设施安全保护云计算服务安全评估、数据出境安全管理、网络安全服务认证等一系列重要制度。

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；根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改〈中华人民共和国网络安全法〉的决定》修正，决定自2026年1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》

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《网络安全法》的重要配套法规。

《生成式人工智能服务管理暂行办法》

是我国首个针对生成式人工智能服务的规范性政策，用于促进生成式人工智能健康发展和规范应用，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

《互联网政务应用安全管理规定》

旨在提高互联网政务应用安全防护水平，保障和促进互联网政务应用安全稳定运行。《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，落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”原则，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。

《国家网络身份认证公共服务管理办法》

为实施可信数字身份战略，推进国家网络身份认证公共服务建设，保护公民身份信息安全，支撑数字经济健康有序发展，国家根据法定身份证件信息，依托国家统一建设的网络身份认证公共服务平台，为自然人提供申领网号、网证以及进行身份核验等服务。

《网络数据安全管理条例》

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，适用于在中华人民共和国境内开展，以及在中华人民共和国境外，处理中华人民共和国境内自然人个人信息，或者损害国家安

全、公共利益或公民、组织合法权益的网络数据处理活动。

《国家网络安全事件报告管理办法》

在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照办法规定，依据《网络安全事件分级指南》，按程序研判报告。

《网络安全标识管理办法》

为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，鼓励产品生产者依据本办法提升产品网络安全能力，标注网络安全标识，鼓励消费者优先选用标注网络安全标识的产品。

02

关键信息基础设施网络安全保护

什么是关键信息基础设施

是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

怎样认定关键信息基础设施

重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门，保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则。

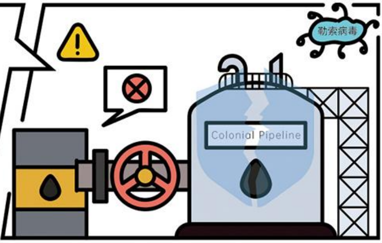
制定认定规则主要考虑因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

2021年5月，美国最大成品油运输管道运营商科洛尼尔管道运输公司的工控系统，遭勒索软件攻击，导致该公司被迫关闭了5500英里的运输管道，炼油、制造、航运等多个产业受到波及影响。


勒索病毒
Colonial Pipeline

近年来，我国有关电信运营商、航空公司等单位内网和信息系统先后多次出现越权登录、数据外传等异常网络行为，疑似遭受网络攻击。

03

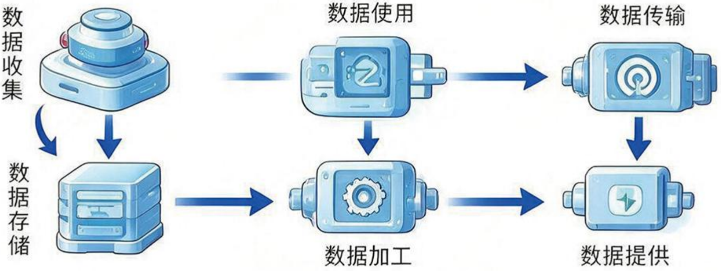
数据安全

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

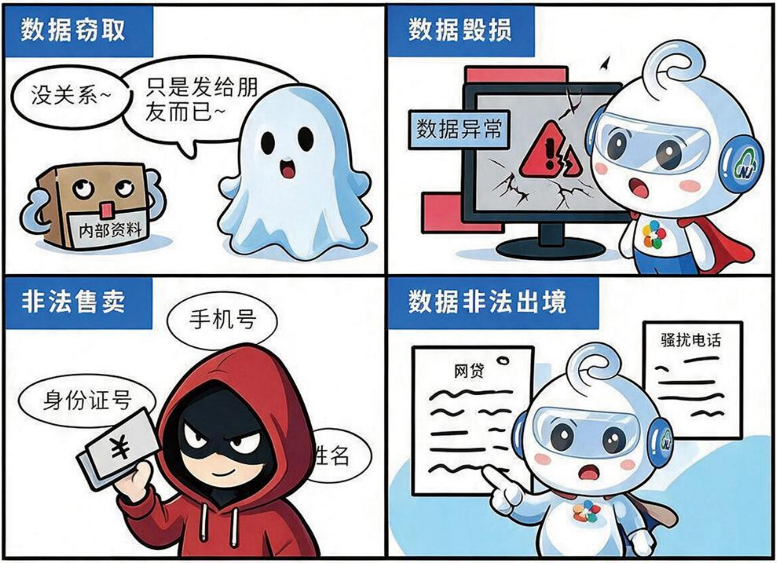
数据是什么

- 个人网购产生的交易记录
- 快递物流信息
- 大型互联网平台处理的海量数据信息
- 网约车共享单车的地图轨迹

数据处理


数据收集
数据使用
数据传输
数据存储
数据加工
数据提供

突出问题


数据窃取
没关系~
只是发给朋友而已~
内部资料
数据毁损
数据异常
非法售卖
手机号
身份证号
¥
生名
数据非法出境
网贷
骚扰电话

危害数据安全的典型案例

2020年1月，某航空公司数据被境外间谍情报机关网络攻击窃取。

2021年3月，李某等人私自在某重要军事基地周边架设气象观测设备，采集并向境外传送敏感气象数据。

2021年5月，某境外咨询调查公司秘密搜集窃取航运数据。

怎样加强数据安全保护

数据处理者：

备份、加密、访问控制、应急处置、风险评估。

重要数据的处理者：

明确数据安全负责人，成立数据安全管理机构；制定数据安全培训计划，组织开展全员数据安全教育培训；优先采购安全可信的网络产品和服务、定期开展数据安全评估。

互联网平台运营者：

建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序，保障平台规则、隐私政策、算法公平公正。

《促进和规范数据跨境流动规定》

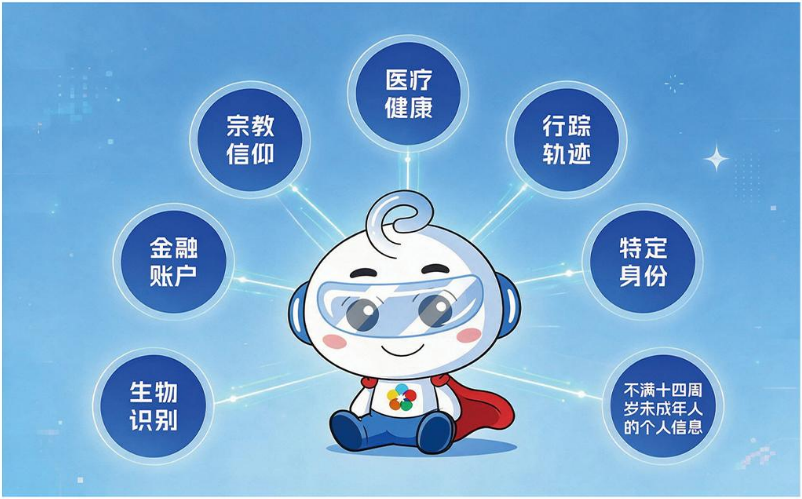
主要内容

- 明确重要数据出境安全评估申报标准
- 明确免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。
- 设立自由贸易试验区负面清单制度。
- 调整应当申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。
- 延长数据出境安全评估结果有效期，增加数据处理者可以申请延长评估结果有效期的规定。

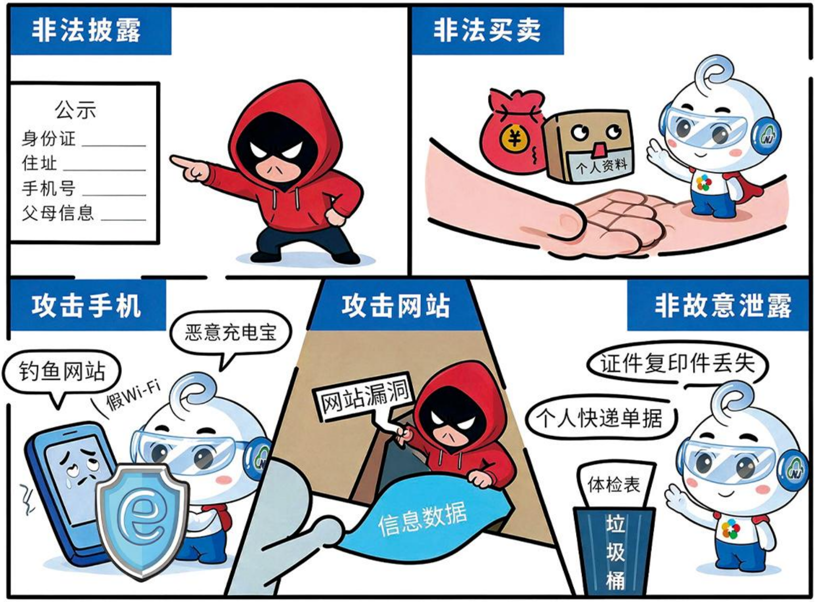
04 个人信息保护

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。


医疗健康
宗教信仰
行踪轨迹
金融账户
特定身份
生物识别
不满十四周岁未成年人的个人信息

泄露途径


非法披露
公示
身份证
住址
手机号
父母信息
非法买卖
¥
个人资料
攻击手机
钓鱼网站
恶意充电宝
假Wi-Fi
攻击网站
网站漏洞
信息数据
非故意泄露
证件复印件丢失
个人快递单据
体检表
垃圾桶

关键信息基础设施安全保护举措

2021年8月17日，国务院公布《关键信息基础设施安全保护条例》，自2021年9月1日起施行。
是落实《网络安全法》要求、构建国家关键信息基础设施安全保护体系的顶层设计和重要举措，更是保障国家安全、社会稳定和经济发展的现实需求。

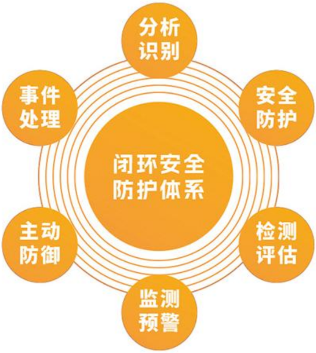
2022年11月7日，我国《关键信息基础设施安全保护要求》国家标准（GB/T 39204-2022）发布，2023年5月1日，正式实施。
是我国第一项关键信息基础设施安全保护的国家标准，对于我国关键信息基础设施安全保护有着重要的指导意义。

明责任 强举措 护安全

坚持**综合协调**

坚持**分工负责**

坚持**依法保护**


闭环安全防护体系
分析识别
安全防护
检测评估
监测预警
主动防御
事件处理

各部门职责

国家网信部门：统筹协调；

国务院公安部门：指导监督安全保护工作；

国务院电信主管部门和其他有关部门：依照相关规定，在各自职责范围内负责关基安全保护和监督管理工作；

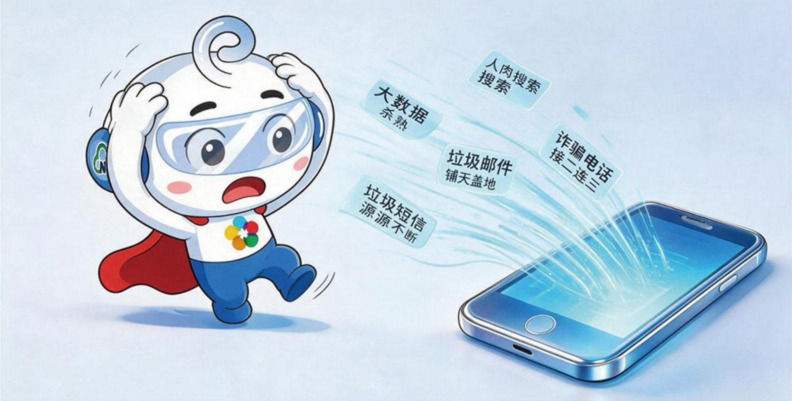
省级人民政府有关部门：依据各自职责对关基设施实施安全保护和监督管理。

运营者责任义务

- 落实网络安全保护制度和责任制；
- 与关键信息基础设施同步规划、同步建设、同步使用安全保护措施；
- 建立健全网络安全保护制度；
- 设置专门安全管理机构；
- 开展安全监测和风险评估；
- 报告网络安全事件或网络安全威胁；
- 规范网络产品和服务采购活动。

保护关键信息基础设施 筑牢网络安全屏障

信息泄露危害


人肉搜索
大数据杀熟
诈骗电话接二连三
垃圾邮件铺天盖地
垃圾短信源源不断

防范建议

① 要优先选择尊重个人信息保护的产品、服务。

② 要仔细审核 App 请求授权的权限内容，并谨慎授权。

③ 要对重要信息进行加密保护。

④ 要差异化设置社交平台好友的信息访问权限。

⑤ 不要随意连接免费 Wi-Fi 热点。

⑥ 不访问陌生网站并留下个人信息。

⑦ 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。

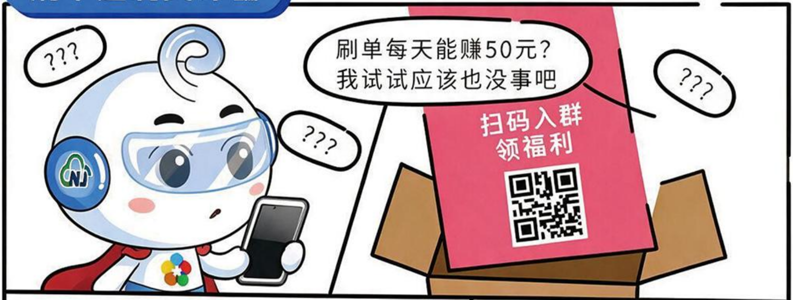
⑧ 尊重他人隐私，不随意披露他人隐私信息。

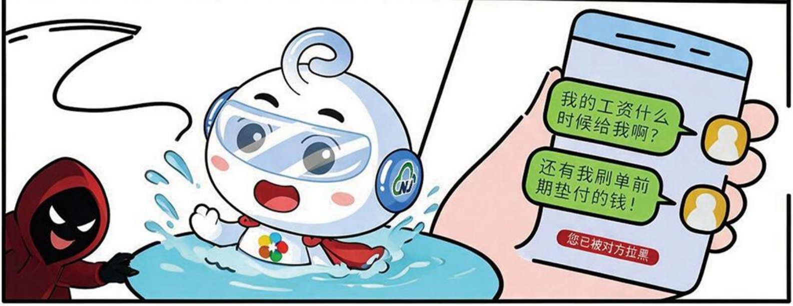
05 电信网络诈骗

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。

刷单返利类诈骗

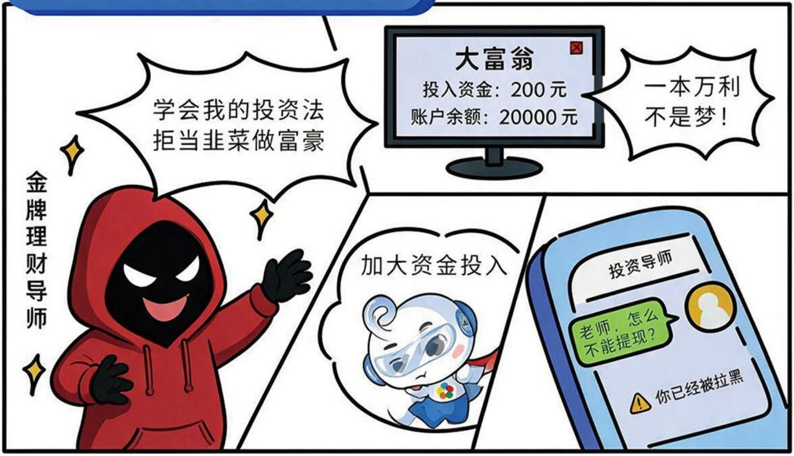
小额任务佣金小“赚”，大额投入没法提现


???
???
刷单每天能赚50元？
我试试应该也没事吧
???
扫码入群
领福利


我的工资什么时候给我啊？
还有我刷单前期垫付的钱！
您已被对方拉黑

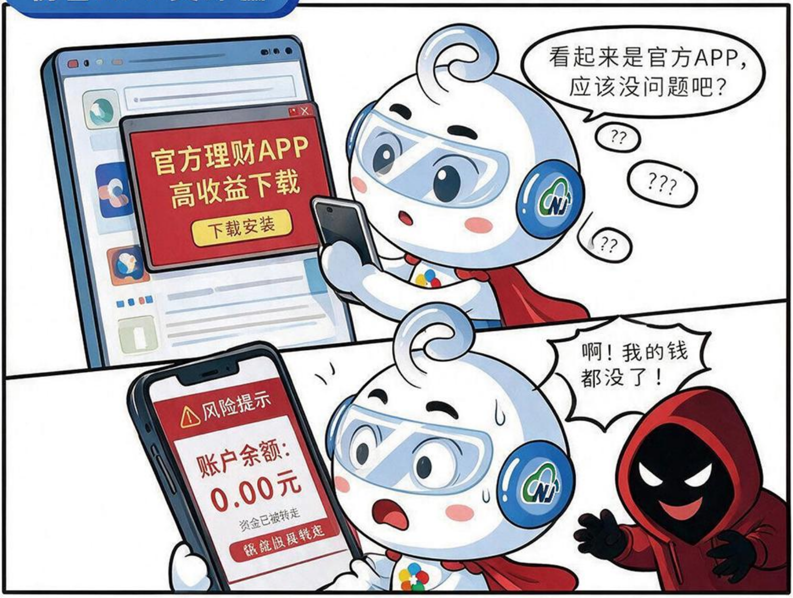
虚假网络投资理财类诈骗

“旁门左道”迷双眼，试水投资有风险


学会我的投资法
拒当韭菜做富豪
金牌理财导师
大富翁
投入资金：200 元
账户余额：20000 元
一本万利
不是梦！
加大资金投入
投资导师
老师，怎么不能提现？
你已经被拉黑

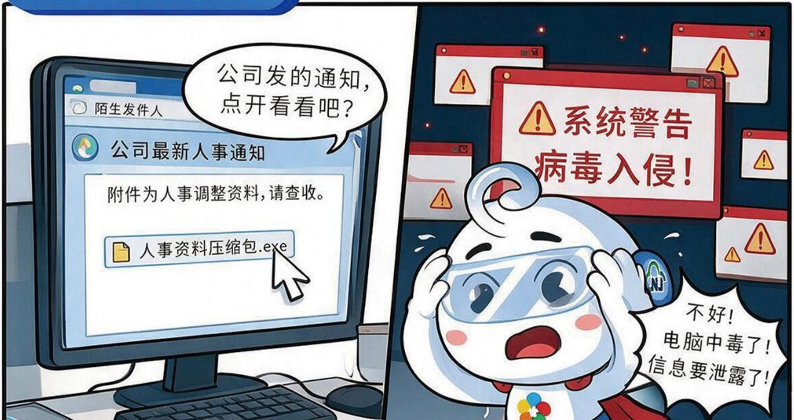
仿冒APP类诈骗

盗版仿冒藏病毒，下载安装有风险


官方理财APP
高收益下载
下载安装
看起来是官方APP，应该没问题吧？
??
???
??
风险提示
账户余额：
0.00元
资金已被转走
啊！我的钱都没了！

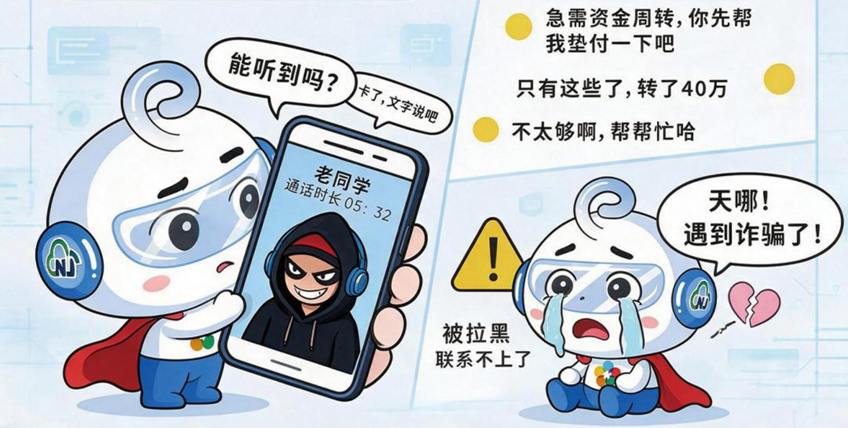
钓鱼邮件类诈骗

陌生邮件藏陷阱，附件链接别乱点


陌生发件人
公司最新人事通知
附件为人事调整资料，请查收。
人事资料压缩包.exe
公司发的通知，点开看看吧？
系统警告
病毒入侵！
不好！电脑中毒了！信息要泄露了！

冒充领导、熟人类诈骗

诈骗技术新升级，涉及资金要警惕


急需资金周转，你先帮我垫付一下吧
只有这些了，转了40万
不太够啊，帮帮忙哈
能听到吗？
卡了，文字说吧
老同学
通话时长 05：32
天哪！遇到诈骗了！
被拉黑
联系不上了

防范建议

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它形式动态密码。

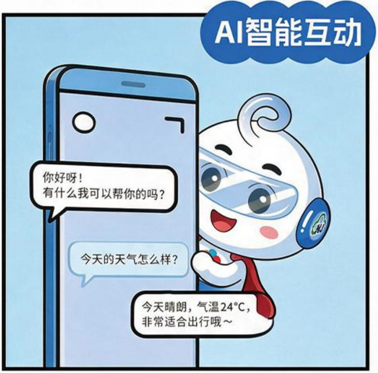
官方渠道办业务：办理银行信用卡及额度提升等业务，一定要通过银行官方平台等可靠渠道进行申请。在网购平台办理退款、退货要通过官方App渠道。

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。

下载和使用手机应用程序：在手机官方应用商店下载App，避免从未知渠道下载。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。

06 人工智能安全

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。

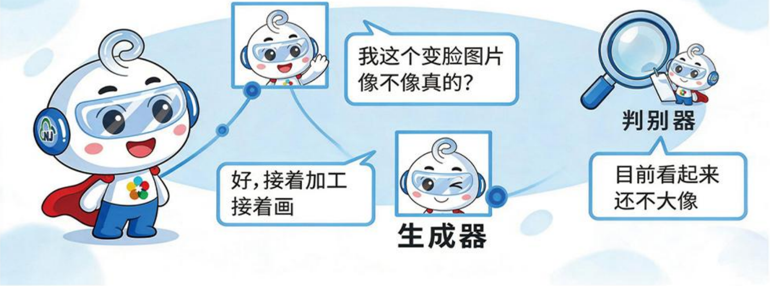


AI智能互动
你好呀！
有什么我可以帮你的吗？
今天的天气怎么样？
今天晴朗，气温24°C，
非常适合出行哦～

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。

生成器


我这个变脸图片
像不像真的?
好，接着加工
接着画
生成器
判别器
目前看起来
还不大像

生成式人工智能带来网络安全风险

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。

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。

AI智能体部署安全风险：部分智能体应用在架构设计、默认配置、漏洞管理、插件生态、行为管控等方面存在安全风险，一旦被攻击者利用，可能导致服务器被控制、敏感数据泄露等严重安全问题。

AI生成内容侵权：部分AI短剧、漫剧未经授权，使用明星、游戏、漫画角色形象、声音建模，侵犯版权、肖像权。

人工智能治理

2023年10月18日，中国政府发布《全球人工智能治理倡议》，围绕人工智能发展、安全、治理三方面系统阐述了人工智能治理中国方案。倡议：

——发展人工智能应坚持“以人为本”理念；

——发展人工智能应坚持“智能向善”的宗旨；

——发展人工智能应坚持相互尊重、平等互利的原则；

——坚持公平性和非歧视性原则；

——坚持广泛参与、协商一致、循序渐进的原则。

《生成式人工智能服务管理暂行办法》自2023年8月15日起施行。该办法突显了中国特色的人工智能治理之道，为世界人工智能治理贡献中国智慧。

鼓励生成式人工智能创新应用；

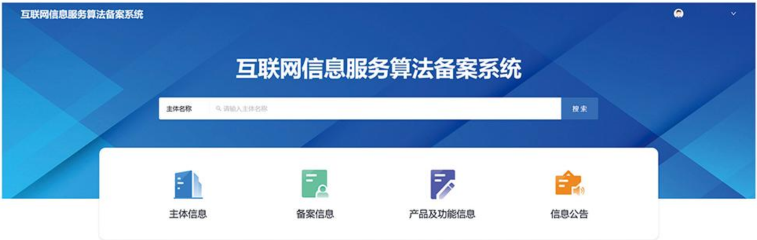
强化风险治理，突出分类分级监管；

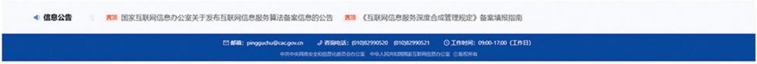
强调个人信息保护、知识产权保护；

明确生成式人工智能服务提供者的内容安全主体责任。

备案管理

根据《生成式人工智能服务管理暂行办法》《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》，提供具有舆论属性或者社会动员能力的生成式人工智能服务、算法推荐服务、深度合成服务，应当按照国家有关规定开展安全评估，履行算法备案和变更、注销备案手续。


互联网信息服务算法备案系统
互联网信息服务算法备案系统
主体名称
请输入主体名称
搜索
主体信息
备案信息
产品及功能信息
信息公告



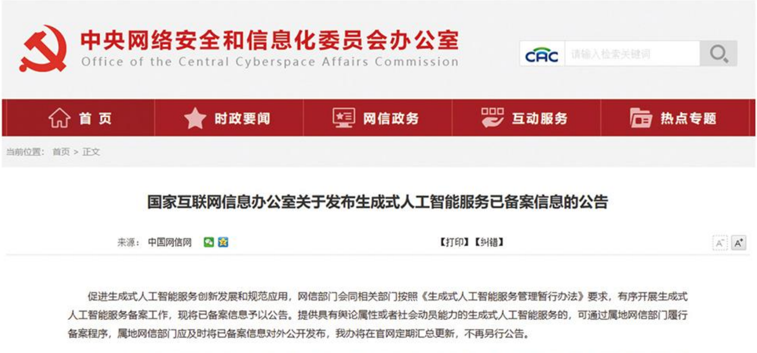
置顶 国家互联网信息办公室关于发布互联网信息服务算法备案信息的公告

置顶 《互联网信息服务深度合成管理规定》备案填报指南

邮箱：pingguchu@cac.gov.cn 咨询电话：(010)82990520 (010)82990521 工作时间：09:00-17:00（工作日）

中共中央网络安全和信息化委员会办公室 中华人民共和国国家互联网信息办公室 ©版权所有

算法备案入口：https://beian.cac.gov.cn/#/index


中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission
CAC
请输入检索关键词
首 页
时政要闻
网信政务
互动服务
热点专题
当前位置： 首页 > 正文
【打印】【纠错】

国家互联网信息办公室关于发布生成式人工智能服务已备案信息的公告

来源：中国网信网

促进生成式人工智能服务创新发展和规范应用，网信部门会同相关部门按照《生成式人工智能服务管理暂行办法》要求，有序开展生成式人工智能服务备案工作，现将已备案信息予以公告。提供具有舆论属性或者社会动员能力的生成式人工智能服务的，可通过属地网信部门履行备案程序，属地网信部门应及时将已备案信息对外公开发布，我办将在官网定期汇总更新，不再另行公告。

已上线的生成式人工智能应用或功能，应在显著位置或产品详情页面公示所使用已备案生成式人工智能服务情况，注明模型名称及备案号。

大模型备案需向省委网信办线下提交，详情可见“网信江苏”微信公众号相关公告。

国家网络安全宣传周

China Cybersecurity Week

国家网络安全宣传周
官方微信账号

网信南京微信公众号

南京网络辟谣
微信公众号

南京网络违法和有害
不良信息举报平台