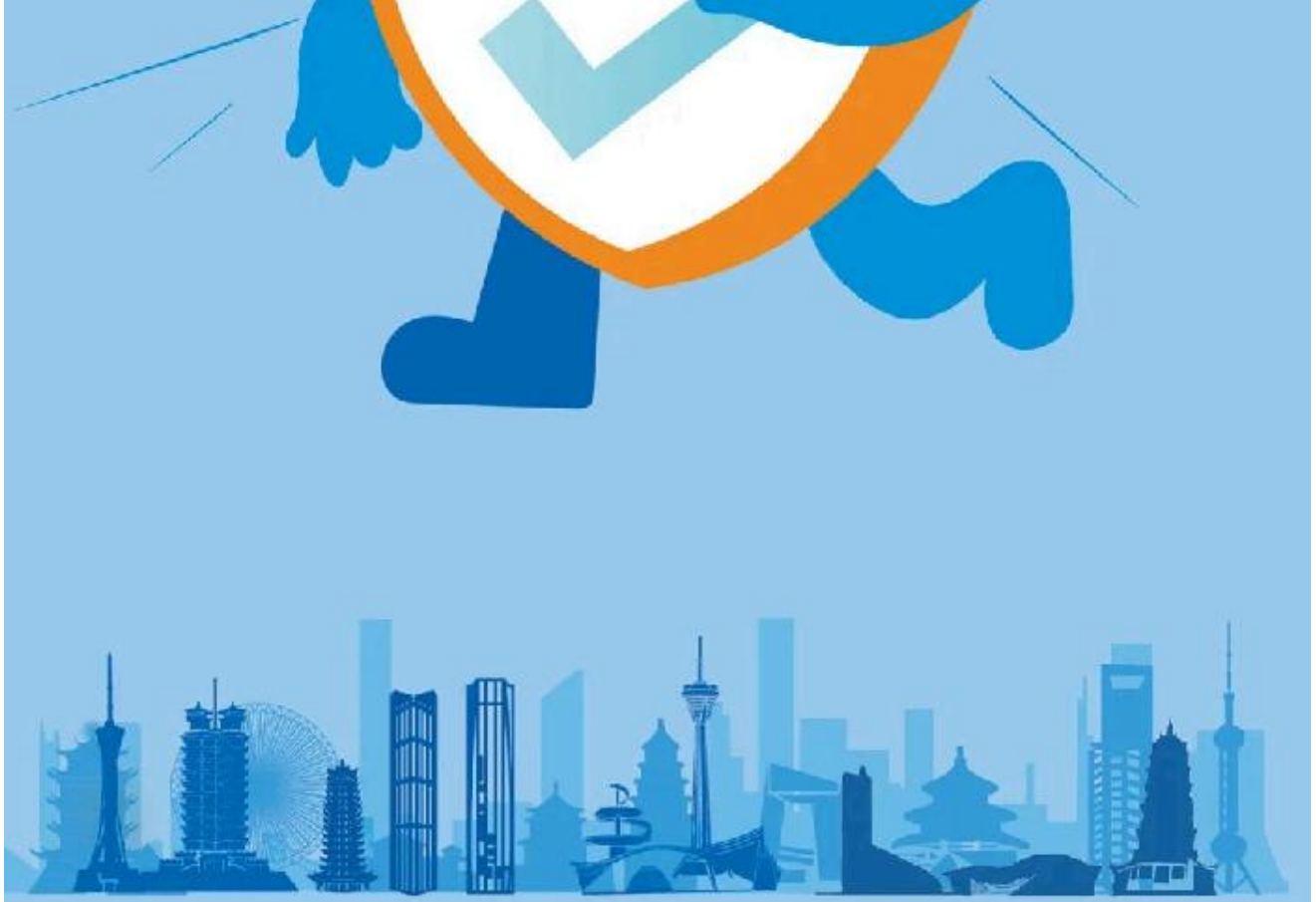
国家网络安全宣传周
China Cybersecurity Week

网络安全为人民
网络安全靠人民

网络安全知识宣传手册



网络安全法律法规体系

《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。

《关键信息基础设施安全保护条例》

2021年4月27日，经国务院第133次常务会议通过，2021年7月30日，国务院总理签署中华人民共和国国务院令第745号公布，自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。

《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。

《汽车数据安全管理若干规定（试行）》

2021年7月5日，国家互联网信息办公室2021年第10次室务会议审议通过，并经国家发展和改革委员会、工业和信息化部、公安部、交通运输部同意，自2021年10月1日起施行。

用于规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用。

《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。

《网络安全审查办法》

2020年4月13日，《网络安全审查办法》公布。2021年11月16日，国家互联网信息办公室 2021 年第 20 次室务会议审议通过新修订的《网络安全审查办法》，自2022年2月15日起施行。

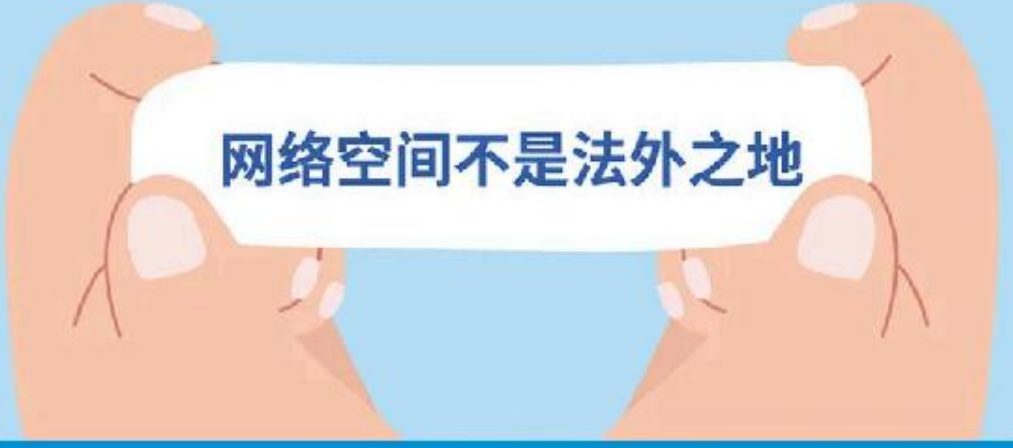
是为了进一步保障网络安全和数据安全，维护国家安全而制定的部门规章。

《生成式人工智能服务管理暂行办法》

2023年5月23日，国家互联网信息办公室2023年第12次室务会会议审议通过，并经国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局同意，自2023年8月15日起施行。

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。

我国网络安全法律法规体系已基本形成。



关键信息基础设施安全保护

什么是关键信息基础设施

是指能源、交通、水利、金融、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

- 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；
- 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；
- 对其他行业和领域的关联性影响。

典型关键信息基础设施安全事件

1. 2015年12月，乌克兰配电公司约60座变电站遭到网络攻击，140万名居民遭遇数小时停电。
2. 2016年10月，美国域名服务器管理机构Dyn遭到Mirai病毒攻击，美国大半个互联网瘫痪。
3. 2021年5月，美国最大成品油运输管道运营商Colonial Pipeline公司工控系统遭勒索病毒攻击导致停机，造成成品油运输管道运营中断。
4. 2022年7月，欧洲天然气管道遭遇勒索软件攻击。

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要。

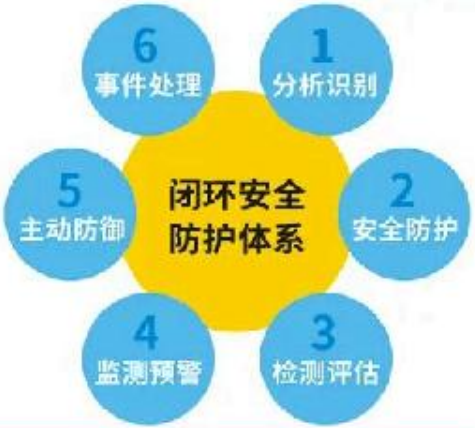
2022年11月7日，我国关键信息基础设施安全保护要求国家标准（GB/T 39204-2022）发布，2023年5月1日，正式实施。

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。

坚持综合协调

坚持分工负责

坚持依法保护



各部门职责

- **国家网信部门：**统筹协调；
- **国务院公安部门：**负责指导监督关键信息基础设施安全保护工作；
- **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键信息基础设施安全保护和监督管理工作；
- **省级人民政府有关部门：**依据各自职责对关键信息基础设施实施安全保护和监督管理。

运营者责任义务

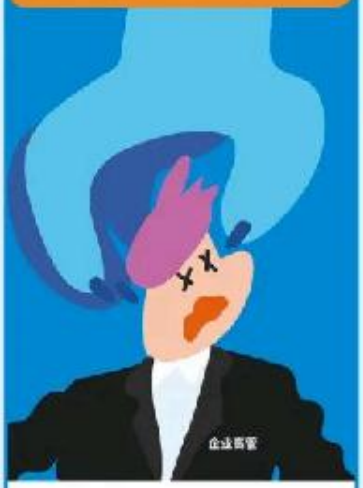
- 落实网络安全保护制度和责任制
- 与关键信息基础设施同步规划、同步建设、同步使用安全保护措施
- 建立健全网络安全保护制度
- 设置专门安全管理机构
- 开展安全监测和风险评估
- 报告网络安全事件或网络安全威胁
- 规范网络产品和服务采购活动

保护关键信息基础设施
筑牢网络安全屏障

钓鱼邮件

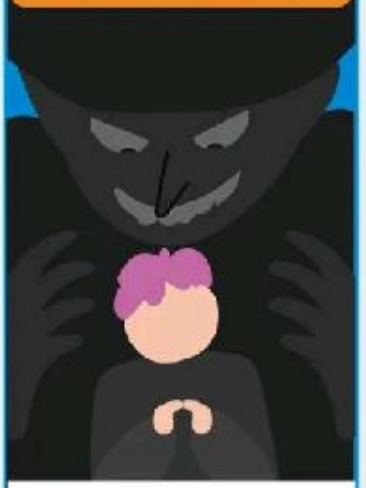
钓鱼邮件是指黑客**伪装成同事、合作伙伴、朋友、家人等用户信任的人**，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而**窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。**

鲸钓攻击



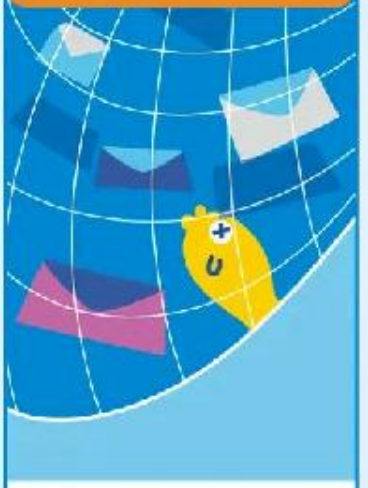
针对高层管理人员

鱼叉式网络钓鱼



针对组织内的特定

商业邮件诈骗



针对公司财务等要

人员

职人员

电子邮件是怎么泄露的

- 黑客搜索爬取求职、婚恋交友、论文数据库等特定网站上包含的邮箱地址；
- 黑客攻击网站，批量窃取用户信息数据库中的邮箱地址；
- 黑客之间通过暗网买卖交换。

钓鱼邮件伪装术

伪造发件人地址以假乱真

利用“l”和“1”，“m”和“rn”等之间的视觉差异性较小的特点，来欺骗收件人。

量身定制邮件正文骗取信任

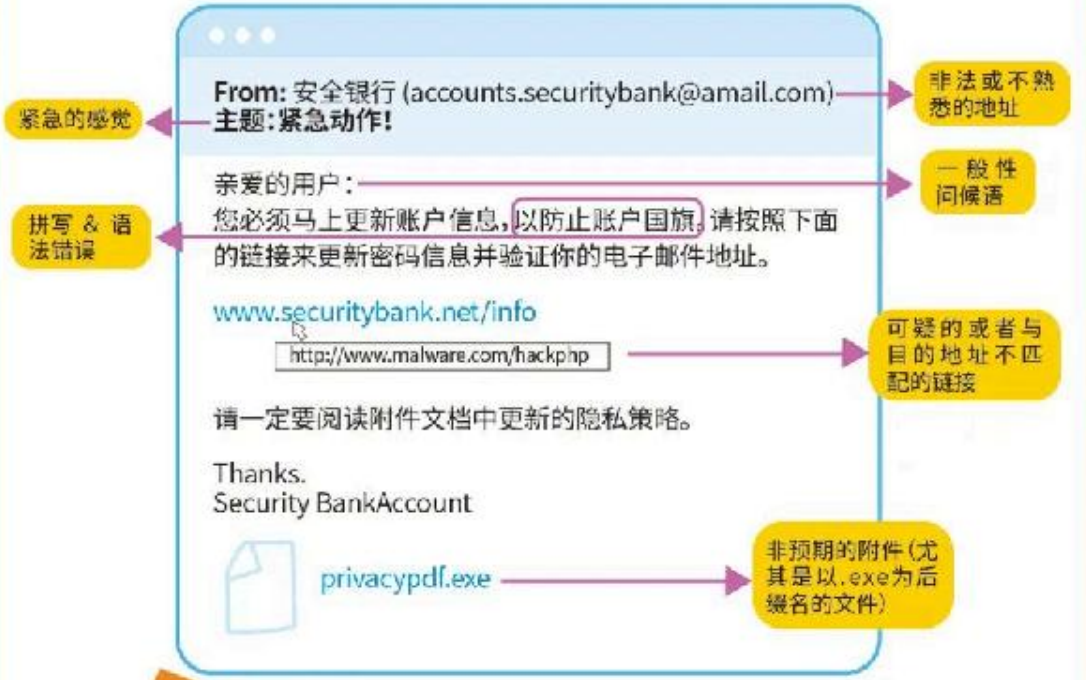
根据用户个人信息、工作情况、习惯等针对性设计邮件文本。

隐藏恶意链接暗度陈仓

使用引用性文字，引诱收件人点击访问恶意网站。

降低用户戒备，添加恶意程序为邮件附件

用超长文件名来隐藏后缀、伪造附件图标，发送带有病毒的文件、程序。



防护建议

- 要将公私邮箱分开，不要轻易注册邮箱地址；
- 要仔细辨认发件人地址，不要轻易点击陌生邮箱发来的邮件；
- 多渠道核实来自熟人的转账汇款请求；
- 悬停鼠标在链接上，检查其指向的网址，不轻易提交用户名、密码等账户信息；
- 及时安装杀毒软件，不轻易下载来历不明的邮件附件；
- 要绑定邮箱账户和手机，便于必要时找回密码，接收"异地登录或账户被锁状态。

数据安全

- 个人网购产生的交易记录

- 快递物流信息

- 网约车行车轨迹及服务信息

- 大型互联网平台处理的海量数据信息

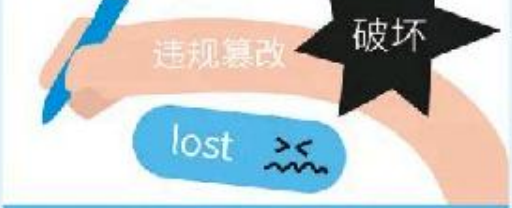
- **数据**，是指任何以电子或者其他方式对信息的记录。
- **数据处理**，包括数据的收集、存储、使用、加工、传输、提供、公开等。
- **数据安全**，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据安全威胁

数据窃取或泄露

数据毁损

黑客攻击、员工窃取、数据安全能力不足、内部违规操作、违规共享等。



违规篡改、破坏、丢失等。

数据非法利用

滥用大数据技术进行分析挖掘，任意共享或发布等。

数据非法出境

赴国外上市的公司，被要求提供审计细节、工作底稿等信息等。

危害重要数据安全的典型案例

- 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。
- 2022年6月，西北工业大学遭受美国国家安全局网络攻击，持续窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。

数据分级

按照《中华人民共和国数据安全法》要求，根据数据一旦遭到**篡改、破坏、泄露或者非法获取、非法利用，**对**国家安全、公共利益或者个人、组织合法权益**造成的危害程度，将数据分为**一般数据、重要数据、核心数据共三个级别。**

怎样加强数据安全保护

数据处理者

备份、加密、访问控制、数据安全应急处置机制、申报网

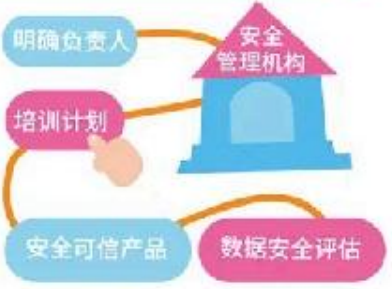
互联网平台运营者

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

络安全审查

序、裁决程序，保障平台规则、隐私政策、算法公平公正

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、每年开展一次数据安全评估。

数据安全服务美好数字生活