

网络安全 关乎你我

2025 年 9 月 15 日至 21 日是国家网络安全宣传周,今年的宣传主题是“网络安全为人民,网络安全靠人民——以高水平安全守护高质量发展”。从日常扫码支付时的资金安全、社交平

台上的个人信息保护,到网购收货时的地址隐私防范、孩子上网课期间的内容安全守护,再到老年人防范电信诈骗、职场中避免文件泄露,网络安全已渗透到生活和工作的每一

个细节。网络安全既是抵御钓鱼链接、恶意软件的“防火墙”,也是保障个人财产不被侵犯、隐私不被滥用、权益不被损害的“安全锁”。唯有重视网络安全,每个人才能安心享

受数字时代。

你对网络安全知识了解多少呢?今天,让我们一起来学习吧!

图片来源: 国家网络安全宣传周微信公众号

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 次常务会议审议通过,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 次常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 次常务会议审议通过,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。

网络空间不是法外之地

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 and 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。



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“n”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,添加信任程序为邮件附件
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,不要轻易泄露邮箱地址;
- 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;
- 提前安装杀毒软件,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“异地登录提醒”掌握状态。

数据安全

- 个人网际产生、快速物流信息、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: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。
- 数据损毁: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

- 数据处理器:备份、加密、访问控制、数据安全应急处置机制、申报网络安全审查
- 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

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

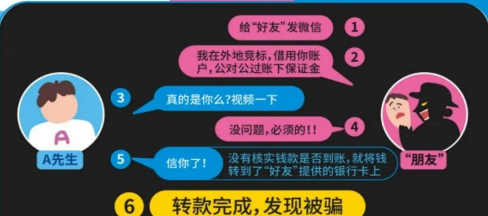
电信网络诈骗

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。

典型骗术

- 杀猪盘诈骗:甜言蜜语暖心房,卷钱跑路两茫茫
指通过婚恋平台、社交软件等方式寻找潜在受害者,通过聊天发展感情取得信任,然后将受害者引入博彩、理财等诈骗平台进行充值,骗取受害者钱财的骗局。
- 杀鸟盘诈骗:投资理财循正路,刷单兼职是骗术
指刷单诈骗、兼职诈骗,骗子通过发高薪兼职信息吸引受害者参与,再通过套路不断鼓动受害者投钱代刷,最终骗取所有投资钱财的骗术。

AI 换脸



AI换脸是一种基于人工智能技术的图像处理应用,可以将一个人的面部特征和表情应用到另一张图片或视频中,实现快速、高效的人脸替换。

新型AI诈骗



防范建议

- 保护个人信息:不向陌生人提供身份证号码、家庭住址等重要信息;尽量减少个人照片、视频的泄露;
- 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微信平台、官方网站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;
- 建议将转账汇款到账时间设定为“2小时到账”或“24小时到账”,以预留处理时间;
- 不要与他人共享屏幕;不要听信陌生人的转账汇款请求;遇熟人借款等情形,尽量通过多种方式(如主动拨打电话等)确认对方是否为本;
- 帮助信息网络犯罪活动罪(简称“帮信罪”)是《刑法》修正案(九)新增设的罪名,简单来说,就是在明知他人利用信息网络实施犯罪(电信诈骗)还为其提供帮助的行为。我们应妥善保管好自己的银行卡,万万不可随意出借、出售给他人使用,以免触犯法律。

防范诈骗并不难 不听忽悠不转钱

个人信息保护

个人信息是指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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

敏感个人信息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,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

泄露途径

- 非法披露:未经当事人同意擅自公开其个人信息,甚至非法出售、非法转让等。
- 非法买卖:有购买商家、信息打包、非法交易。
- 非故意泄露:证件复印件丢失、银行收款单丢失、设备不完善、管理不规范、技术不成熟。

攻击手机



信息泄露危害

- 1 垃圾短信源源不断;
- 2 骚扰、诈骗电话接二连三;
- 3 垃圾邮件铺天盖地;
- 4 大数据“杀熟”、“人肉搜索”等恶意披露特定对象的个人信息事件。

防护建议

- 要优先选择尊重个人信息保护的产品、服务;
- 要审核App要求的权限,并谨慎授权;
- 要在身份证复印件上标注“仅限办理某业务时使用”;
- 要对重要信息进行加密保护;
- 要设置他人对自己所分享信息的访问权限。

防护建议

- 不要随意连接免费Wi-Fi热点;
- 不要随意点击进入短信、邮件中的网站,提交个人敏感信息;
- 不在网上晒车票、证件,以及含有孩子学校、家庭住址、个人收入情况的照片。