

《中华人民共和国网络安全法》

网络安全知识

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、破坏和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。

国家支持与促进网络安全工作

- ★ 建立和完善网络安全标准体系
- ★ 相关部门组织制定并修订国家标准、行业标准
- ★ 支持企业、研究机构、高等学校、相关行业组织参与标准制定
- ★ 国务院和各级政府应做好扶持、推广工作，保护网络技术知识产权
- ★ 推进网络安全社会化服务体系建设
- ★ 鼓励开发网络安全数据保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展
- ★ 支持创新网络安全管理方式，运用新技术，提升保护水平
- ★ 组织开展网络安全宣传教育
- ★ 支持教育培训机构开展网络安全相关教育与培训，促进网络安全人才交流

公民、组织的义务和权利

义务

- 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，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
- 不得从事危害网络安全的活动，亦不得为之提供程序、工具和帮助
- 不得设立用于实施违法犯罪活动的网站、通讯群组，不得利用网络发布涉及违法犯罪活动的信息
- 在电子信息、应用软件中，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

网络安全工作职责

国家网信部门 负责统筹协调网络安全工作和相关监督管理工作



在各自职责范围内负责网络安全保护和监督管理工作

县级以上地方政府有关部门

按照国家规定确定网络安全保护和监督管理职责

权利

- 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
- 对危害网络安全的行为有权向网信、电信、公安等部门举报

安全上网，从日常做起

日常八大安全隐患

- 网络诈骗
- 隐私泄露
- 黑客攻击
- 移动支付
- 手机病毒
- 恶意软件
- 骚扰电话
- 垃圾短信

如何预防网络诈骗？

- 1 不贪便宜，天上掉馅饼的事情别信
- 2 使用比较安全的支付工具，如支付宝、U盾等
- 3 仔细甄别，严加防范
- 4 千万不要在网上购买非正当产品；
- 5 不要轻信以各种名义要求你先付款的信息，也不要轻易把银行卡借给他人；
- 6 妥善保管自己的私人信息，避免在公共场所使用电子商务服务。

安全的使用智能手机

- 陌生的链接和文件不要点
- 设置访问密码
- 手机随身携带
- 关闭定位功能
- 安装防护软件
- 经常备份数据
- 需要时才开蓝牙
- 不要破解系统

剁手族如何安全的网上购物

- 1 不要在公共电脑上进行购物付款等操作
- 2 尽量到知名的、权威的网上商城购物，通过第三方支付平台交易，切忌与卖家私下交易
- 3 在购物时要注意商家的信誉、评价和联系方式
- 4 支付密码不要使用姓名、生日、电话号码等个人信息，或12345等
- 5 交易完成后要完整保存交易订单等信息
- 6 对单笔交易进行金额限制，并为开通短信提醒

如何防范骚扰电话、垃圾短信

- 1 克服“贪利”思想，不要轻信
- 2 不要轻易将自己或家人的身份信息泄露给他人
- 3 对亲人和朋友求助、借钱等短信、电话，要仔细核对
- 4 对于广告推销的短信、电话，不予理睬
- 5 存取款遇到银行卡被吞等情况，认真识别取款机“提示”的真伪，可拨打银联客服电话咨询
- 6 遇见诈骗类电话或者信息，记下犯罪份子的信息和诈骗手段，及时到公安机关报案

安全上网的五个建议

- 保持更新
- 密码安全
- 安全软件
- 时刻戒备
- 洁身自好