



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

2025年国家网络安全宣传周

2025年9月15日- 2025年9月21日

培养良好的网络安全习惯防范常见威胁

培养良好的网络安全习惯能让公民在网络空间防患于未然，保障公民的财产、隐私和身份安全，是成本最低且最有效的自我防护。



好奇害死猫，乱点会中招

病毒



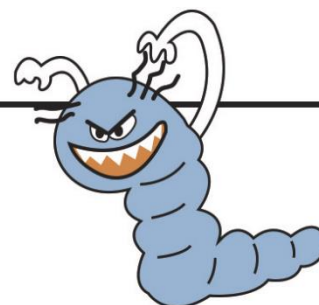
通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的。

木马



以盗取用户个人信息，甚至是远程控制用户计算机为主要目的，如盗号木马、网银木马等。

蠕虫



能自我复制和广泛传播，以占用系统和网络资源为主要目的。

逻辑炸弹



当计算机系统运行的过程中恰好某个条件得到满足，就触发执行并产生异常甚至灾难性后果。

培养良好的网络安全习惯防范常见威胁



上网冲浪贴士

- 确认要求你提供敏感信息的网站，网址是以https开头的，并且显示了绿色的挂锁图标；
- 点击链接或打开附件之前要三思，避免使用公用电脑和Wi-Fi来登录账户和访问敏感信息；
- 离开设备时，按下“Ctrl-Alt-Del”或者“Win+L”键及时锁屏，及时登出账户、关闭电脑或移动设备。



个人数据保护贴士

- 利用计算机的计划任务功能，定期自动备份；
- 对备份进行加密，并存储在安全的、干燥的、隔离的物理空间；
- 经常测试你的备份，确保可以在需要的时候成功恢复数据；
- 通过设置社交媒体信息访问权限保护个人信息；
- 不通过邮件或电话提供个人信息，尤其是医疗、金融类的敏感信息。

培养良好的网络安全习惯防范常见威胁



企业数据保护贴士

- 最小化收集个人可识别信息，按需尽量最短保留这些信息；
- 通过制定政策、开展培训引导员工正确保护数据；
- 对于传输和存储的敏感数据进行加密；
- 远程访问公司网络和特权访问系统时，通过多种方式认证；
- 使用密码或PIN号保护视频会议，只有受邀请者才能访问；
- 使用虚化、模糊处理等方式隐藏企业敏感信息。



设备安全贴士

- 不要将个人U盘插入到工作计算机，也不要将工作U盘插入到个人计算机；
- 不要将不明来路的U盘插入到自己或他人的计算机；
- 从正规渠道、正规厂商处购买U盘等设备；
- 不要使用同一设备存储个人文件和工作文件；
- 禁用计算机的自动运行功能，阻止U盘插入时自动运行。



Right By You