# 常见网络安全风险防范小知识

目前，我国网络安全面临层出不穷的新问题，维护网络安全是全社会共同的责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。只有把网络安全意识上升并贯彻到全社会的层面中，网络安全的防线才能牢驻不倒。2020年国家网络安全宣传周主题是“网络安全为人民，网络安全靠人民”。如何提升大家的网络安全防范意识，加强各类网络诈骗行为防范能力？今天，我们与大家一起学习网络安全风险防范这方面的知识，帮助大家应对常见的网络安全风险。

1. 钓鱼WI-FI

举例：攻击者利用人们节省流量费的心理，架设假冒的free-WiFi热点，或者发送断连信号给受害人计算机，强制使其下线，然后将其吸引到同名恶意热点上，对受害人进行窃取数据、注入恶意软件、下载有害内容等侵害。

防范建议：不要使用公共Wi-Fi进行购物、网上银行转账等操作；关闭Wi-Fi自动连接；安装安全软件，进行Wi-Fi环境的安全扫描，降低安全威胁。

1. 恶意软件

恶意软件指可以中断用户的计算机、手机、平板电脑或其他设备的正常运行或对其造成危害的软件。主要包括：病毒、蠕虫、木马等。

防范建议：安装防火墙和防病毒软件，并及时更新病毒特征库；从官方市场下载正版软件；定期备份电脑、手机的数据，留意异常告警，及时修复恢复；不要打开来历不明的网页、邮箱链接或短信中的短链接等。

三、个人信息保护

个人敏感信息一旦遭到泄露、非法提供或滥用可能危害人身和财产安全，导致个人名誉、身心健康受到损害。

举例：随手乱丢快递单；星座、性格测试，泄漏姓名、出生年月；分享送流量，不法分子确认手机号是有效的；抢红包输入个人信息；机构数据泄露导致个人账户信息泄露等。

防范建议：要利用社交网站的安全与隐私设置保护敏感信息；要仔细阅读用户许可，只授权将个人信息转移给合法的接收者；要注意保存或及时销毁存有个人信息的纸质资料、快递单、废弃的光盘、U盘、电脑；不要在微博、朋友圈等处随意晒出个人敏感信息。

四、网络电信诈骗

网络电信诈骗包括：信任类诈骗、同情类诈骗、威胁类诈骗、情感类诈骗等。

防范建议：凡是声称缴纳数十元、上百元会费就能获利很多的各类APP、项目，均是诈骗；要选择信誉良好的网站购物；不要轻信以各种名义要求你先付款的信息；不要轻信任何号码发来的涉及银行转账及个人财产的短信。