共建网络信息安全

近年来，随着互联网络的普及与发展，我们的生活和工作都越来越依赖于网络。国家政府机构、各企事业单位不仅建立了自己的局域网系统，而且通过各种方式与互联网相连。但是，我们不得不注意到，网络虽然功能强大，也有其脆弱易受到攻击的一面。所以，我们在利用网络的同时，也应该关注网络安全问题，加强网络安全防范，防止网络的侵害，让网络更好的为人们服务。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。当今世界，信息技术革命日新月异，对国际政治、经济、文化、社会、军事等领域发展产生了深刻影响。信息化和经济全球化相互促进，互联网已经融入社会生活方方面面，深刻改变了人们的生产和生活方式。我国正处在这个大潮之中，受到的影响越来越深。我国网民数量世界第一，俨然已成为网络大国。但是伴随着互联网技术的迅猛发展，网络与信息安全的问题也日益突出，已经成为事关国家的政治安全、经济安全、社会安全、文化安全和国防安全的重大问题。每年都举办的网络安全宣传周，有多少人知晓，在网络信息快速发

展的今天，网络安全关系到我们每一个人，每一天我们都离不开网络的存在。维护网络安全是全社会的责任，维护网络安全不仅需要政府、企业、社会组织，更需要广大网民的参与，网络安全这道防线才能筑牢固。为进一步提升广大网民的安全和防范意识，我国已经连续举办多次网络安全宣传周，并充分利用电视、广播、报刊杂志、网络等平台，向广大人民群众宣传网络安全知识，开展多种多样的网络宣传活动。

网络安全宣传教育要从小抓起，加强对青少年的网络教育，将网络安全教育纳入到学校教学内容当中，促使青少年依法上网、文明上网、安全上网。网络安全宣传教育不仅仅局限于网络安全宣传周期间，更多的还是需要长期不断的日常宣传。网络安全与我们个人信息安全、网络安全有着紧密的关系，面向广大公众开展网络安全科普宣传，进一步提高网络安全意识。

传播背后的心理学

乐观主义者： 网海一粒米，哪会盯上你，不用去搭理

悲观主义者： 黑客黑科技，想防没实力

现实主义者： 人在网上漂，难免会挨刀；不等黑客下手，先备份数据、打补丁、堵端口

防范建议

拒付赎金： 支付赎金会助长攻击者的气焰。攻击者还会通过用户支付赎金速度对用户财务、数据价值等情况进行分析，可能从此被盯上。

防毒杀毒： 尽量到官方网站下载软件，安装正规杀毒软件，运行下载软件之前先进行病毒扫描。

及时更新： 关注操作系统安全公告，及时安装安全补丁，尽早堵住漏洞。

封堵端口： 关闭无用的计算机服务/端口，开启Windows防火墙，减少被攻击的“通道”。

做好备份： 使用光盘/移动硬盘等介质，对文档、邮件、数据库、源代码、图片、压缩文件等各种类型的数据资产定期进行备份，并脱机保存。

数据备份至最新　不怕勒索要赎金

1. 仔细辨认真伪：向公共场合Wi-Fi提供方确认热点名称和密码；无需密码就可以访问的Wi-Fi风险较高，尽量不要使用。

2. 避免敏感业务：不要使用公共Wi-Fi进行购物、网上银行转账等操作，避免登录帐户和输入个人敏感信息。如果安全性要求高，有条件的话可以使用 VPN服务。

3. 关闭Wi-Fi自动链接：防止手机自动连接到合法Wi-Fi热点的“邪恶双胞胎”，造成信息泄露。

4. 注意安全加固：为Wi-Fi路由器设置强口令以及开启WPA2，关闭WPS，是最有效的Wi-Fi安全设置。

5. 运行安全扫描：安装安全软件，进行Wi-Fi环境等安全扫描，降低安全威胁。

假冒热点

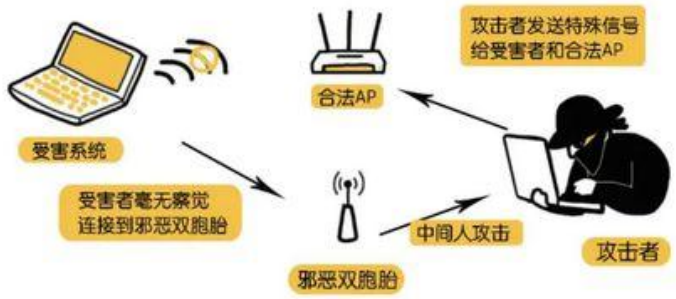
定义

无线接入点（Access Point，AP）俗称“热点”，扮演无线工作站和有线局域网的桥梁。有的一体设备同时执行接入和路由工作；而纯接入设备只负责无线客户端的接入，与其他AP或者主AP连接以扩大无线覆盖范围。

风险

手机上网有点贵，蹭网可省流量费。
免费热点见就连，当心背后有风险！

1. 攻击者架设假冒/高仿/山寨Wi-Fi热点，用相近的名字吸引用户连接（如：李逵机场免费Wi-Fi VS 李鬼机场免费Wi-Fi），你的所有上传下载内容都被黑客掌握！可谓，IC、IP、IQ卡，统统可能丢密码。



2.攻击者架设的Wi-Fi热点和真的同名，通过发送特殊数据包强制断开受害人电脑与合法AP之间的连接，转而连到“邪恶双胞胎”热点上。

钓鱼网站

定义

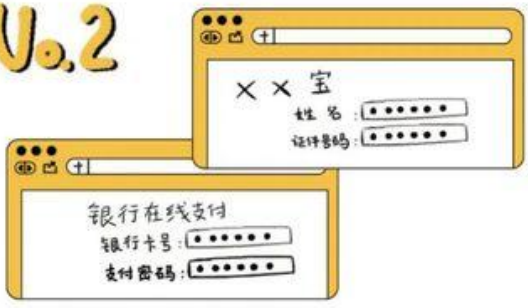
网络套路深，遍地都是坑。网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿冒的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

表现形式

No.1

以“公司周年庆”、“幸运观众”、低价机票、电话充值、征婚交友为名，诱骗用户填写身份证号码、银行账户等信息。

No.2



模仿支付宝、网上银行等网站，窃取用户的账号及密码等信息。

1 察颜观色：留意网站配色、内容、链接等细微之处。但对攻击者完整克隆网站的钓鱼方式无法适用。

2 注意提示：已被举报加入黑名单的网站，安全浏览器会提示“危险网站”。

3 安全标志：支付相关的网站一般网址以https开头，在网络地址栏会有彩色图标或锁头，可点击查看网站被权威机构认证的信息。

4 悬停鼠标：不盲目相信搜索引擎的推荐，不乱点击邮件、微信、微博、短信中的网址，尤其是短网址。

5 细辨网址：如工商银行网址icbc.com.cn被混淆为lcbc.com.cn；www.microsoft.com被混淆为ww-w.rncrosoft.com。

6 高级技巧：从http://开始向右遇到第一个斜线，从该斜线向左至第二个“.”之间的网址是网站的真正域名。例如：http://www.sina.com.cn.sinainfo.cc/log-in/sina.com/index.html的域名是sinainfo.cc，而不是新浪。