



2022年青柴院网络安全知识科普

网络安全为人民 ★ 网络安全靠人民

信息技术服务中心



使用WiFi要谨慎

1.谨慎使用免费Wi-Fi。尽量使用可靠的Wi-Fi接入点，关闭手机和平板电脑等设备的无线网络自动连接功能，仅在需要时开启；

2.警惕公共场所免费的无线信号为不法分子设置的钓鱼陷阱，尤其是一些和公共场所内已开放的Wi-Fi同名的信号。在公共场所使用陌生的无线网络时，尽量不要进行与资金有关的银行转账与支付；

3.修改无线路由器默认的管理员用户名和密码，将家中无线路由器的密码设置得复杂一些，并采用强密码，最好是字母和数字的组合；

4.启用WPA/WEP加密方式；

5.修改默认SSID号，关闭SSID广播；

6.启用MAC地址过滤；

7.无人使用时，关闭无线路由器电源。



智能手机要加密



手机使用

为手机设置访问密码是保护手机安全的第一道防线，以防智能手机丢失时，犯罪分子可能会获得通讯录、文件等重要信息并加以利用；

为手机设置锁屏密码，并将手机随身携带。
不要轻易打开陌生人通过手机发送的链接和文件；



手机信息防泄露



01

利用手机中的各种安全保护功能，为手机、SIM卡设置密码并安装安全软件，减少手机中的本地分享，对程序执行权限加以限制；

02

谨慎下载应用，尽量从正规网站下载手机应用程序和升级包，对手机中的Web站点提高警惕；

03

禁用Wi-Fi自动连接到网络功能，使用公共Wi-Fi有可能被盗用资料；

04

下载软件或游戏时，应仔细阅读授权内容，防止将木马带到手机中；

05

勿见码就刷



个人信息要保密

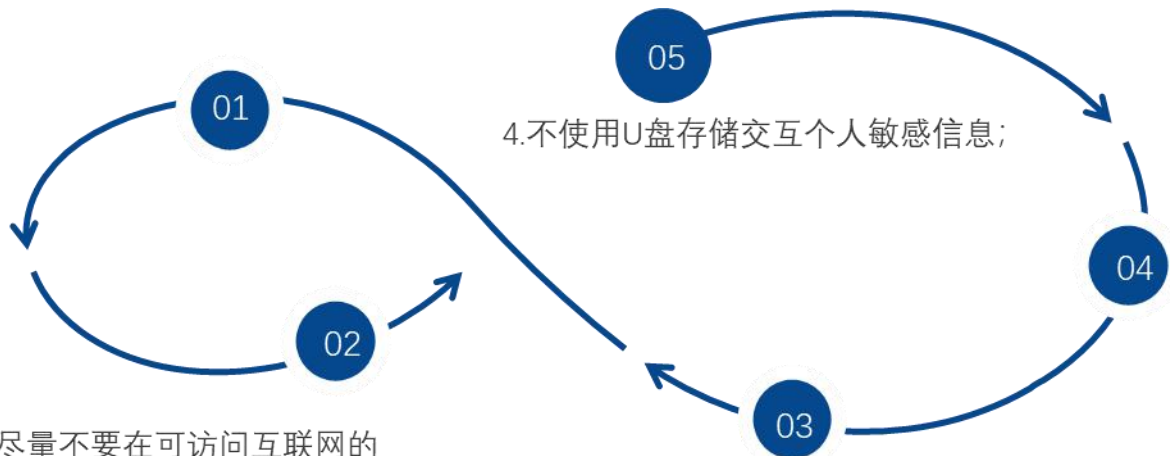
1. 在安全级别较高的物理或逻辑区域内处理个人敏感信息；

2. 尽量不要在可访问互联网的设备上保存或处理个人敏感信息；

5. 敏感个人信息需加密保存；

4. 不使用U盘存储交互个人敏感信息；

3. 只将个人信息转移给合法的接收者；

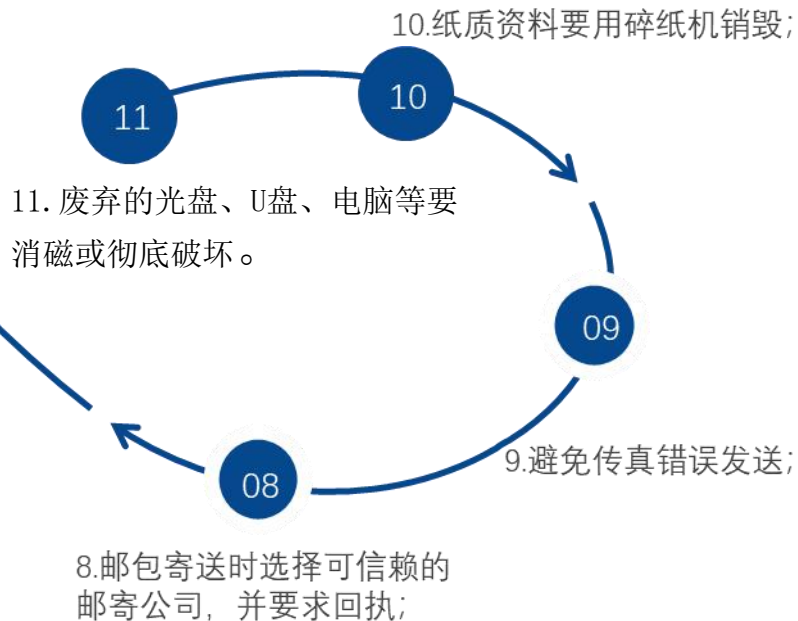




个人信息要保密

6. 个人敏感信息需带出单位时要防止被盗、丢失；

7. 电子邮件发送时要加密，并注意不要错发；





手机支付重安全

- 1.保证手机随身携带，建议手机支付客户端与手机绑定，使用数字证书，开启实名认证；
- 2.最好从官方网站下载手机支付客户端和网上商城应用；
- 3.使用手机支付服务前，按要求在手机上安装专门用于安全防范的插件；
- 4.登录手机支付应用、网上商城时，勿选择“记住密码”选项；
- 5.经常查看手机任务管理器，检查是否有恶意程序在后台运行，并定期使用手机安全软件扫描手机系统。

手机支付
重安全



骚扰诈骗要明辨

01

克服“贪利”思想，不要轻信，谨防上当；

02

不要轻易将自己或家人的身份、通讯信息等家庭、个人资料泄露给他人，对涉及亲人和朋友求助、借钱等内容的短信和电话，要仔细核对；

03

接到培训通知、以银行信用卡中心名义声称银行卡升级、招工、婚介类等信息时，要多做调查；

04

不要轻信涉及加害、举报、反洗钱等内容的陌生短信或电话，既不要理睬，更不要为“消灾”将钱款汇入犯罪分子指定的账户；





骚扰诈骗要明辨

05

对于广告“推销”特殊器材、违禁品的短信和电话，应不予理睬并及时清除，不要汇款购买；

06

到银行自动取款机（ATM机）存取遇到银行卡被堵、被吞等意外情况，应认真识别自动取款机“提示”的真伪，不要轻信，可拨打95516银联中心客服电话的人工服务台了解查询；

07

遇见诈骗类电话或信息，应及时记下诈骗犯罪分子的电话号码、电子邮件地址、QQ号及银行卡账号，并记住犯罪分子的口音、语言特征和诈骗的手段和经过，及时到公安机关报案，积极配合公安机关开展侦查破案和追缴被骗款等工作。





信息泄露有途径



旅馆住宿、保险公司投保、租赁公司、银行办证、电信、移动、联通、房地产、邮政部门等需要身份证件实名登记的部门、场所，个别人员利用登记的便利条件，泄露客户个人信息；

个别违规打字店、复印店利用复印、打字之便，将个人信息资料存档留底，装订成册，对外出售；



信息泄露有途径

借各种“问卷调查”之名，窃取群众个人信息，他们宣称只要在“调查问卷表”上填写详细联系方式、收入情况、信用卡情况等内容，以及简单的“勾挑式”调查，就能获得不等奖次的奖品，以此诱使群众填写个人信息；

在抽奖券的正副页上填写姓名、家庭住址、联系方式等可能会导致个人信息泄露；

在购买电子产品、车辆等物品时，在一些非正规的商家填写非正规的“售后服务单”，从而被人利用了个人信息；

超市、商场通过向群众邮寄免费资料、申办会员卡时掌握群众信息向外泄露。



投诉举报



中国互联网违法和不良信息举报中心

12377



谢谢观看！