网络信息安全宣传
知识手册

南京农业大学图书与信息中心
2016. 9

在由中央网信办、教育部、工业和信息化部、公安部、新闻出版广电总局、共青团中央等部委联合举办的第三届国家网络安全宣传周（9.19-9.25）来临之际，图书与信息中心谨以此手册提醒给广大校园网用户注意网络安全，文明健康上网。

网络安全为人民

网络安全靠人民

目录

四、个人信息安全

计算机安全篇

一、在使用电脑过程中应该采取哪些网络安全防范措施

1. 新装操作系统应安装启用防火墙和防病毒软件后再联网，经常升级防护软件；

2. 注意使用最新版本操作系统，并经常给操作系统、应用程序打补丁，堵塞软件漏洞；

3. 不要执行从网上下载后未经杀毒处理的软件，不要打开邮箱或者 QQ 传送过来的不明文件等。

二、如何防范 U 盘、移动硬盘泄密

1. 及时查杀木马与病毒；

2. 从正规商家购买可移动存储介质；

3. 定期备份并加密重要数据；

4. 不要将办公与个人的可移动存储介质混用。

三、如何确保 Windows 操作系统用户安全

在“用户账户”中为用户账户创建密

码，禁用 Guest 账户。

四、如何将网页浏览器配置得更安全

1. 设置统一、可信的浏览器初始页面；

2. 定期清理浏览器中本地缓存、历史记录以及临时文件内容；

3. 利用病毒防护软件定期进行恶意代码扫描。

五、为什么要定期进行补丁升级

编写程序不可能十全十美，小到软件，大到操作系统都免不了会出现 BUG（缺陷），而补丁是专门用于修复这些 BUG 的。因为原来发布的软件存在缺陷，发现之后另外编制一个小程序使其完善，这种小程序俗称补丁。定期进行补丁升级，可以有效地防止软件运行故障、操作系统被非法入侵等。校园网可提供 Windows 操作系统本地补丁更新服务，详情参见：http://10.0.1.110。

六、计算机中毒有哪些症状

1. 经常死机；

2. 文件打不开；
3. 经常报告内存不够；
4. 提示硬盘空间不够；
5. 出现大量来历不明的文件；
6. 数据丢失；
7. 系统运行速度变慢；
8. 操作系统自动执行操作。

七、为什么不要打开来历不明的网页、电子邮件链接或附件

互联网上充斥着各种钓鱼网站、病毒、木马程序。不明来历的网页、电子邮件链接、附件中，很可能隐藏着大量的病毒、木马，一旦打开，这些病毒、木马会自动进入电脑并隐藏在电脑中，会造成文件丢失损坏，甚至导致系统锁死瘫痪。

八、接入移动存储设备(如移动硬盘和 U 盘) 前为什么要进行病毒扫描

外接存储设备具有便携、易存取信息的特点，但也很容易传播各种病毒，如果将带有病毒的外接存储介质接入电脑，很容易将病毒传播到电脑中。

九、计算机日常使用中为何会出现异常情况

计算机出现故障可能是由计算机自身硬件故障、软件故障、误操作或病毒引起的，主要包括系统无法启动、系统运行变慢、无故死机、频繁重启等异常现象，找出原因才能解决问题。

十、Cookies 文件会导致怎样的安全隐患

当用户访问一个网站时，Cookies 将自动储存于用户 IE 内，其中包含用户访问该网站的种种活动、个人资料、浏览习惯、消费习惯，甚至信用记录等。这些信息用户无法看到，当浏览器向此网址的其他主页发出访问请求时，此 Cookies 信息也会随之发送过去，这些信息可能被不法分子获得。为保障个人隐私安全，可以在 IE 设置中对 Cookies 的使用做出限制。

上网安全篇

一、如何防范病毒或木马的攻击

1. 为电脑安装杀毒软件，定期扫描系统、查杀病毒；及时更新病毒库、更新系统补丁；校园网目前提供了 360 安全卫士企业版（http://10.0.1.100）和 TimeOn 云杀毒（http://202.195.240.90）防病毒系统；

2. 下载软件时尽量到官方网站或大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒； 校园网络信息服务网站提供了常用软件下载服务（http://ftp.njau.edu.cn/）；

3. 不随意打开不明网页链接，尤其是不良网站的链接，陌生人通过 QQ 给自己传链接时，尽量不要打开；

4. 使用网络通信工具时不随意接收陌生人的文件，若接收可取消“隐藏已知文件类型扩展名”功能来查看文件类型；

5. 对公共磁盘空间加强权限管理，定期查杀病毒；

6. 打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建立名为 autorun.inf 的文件夹(可防 U 盘病毒启

动)；

7. 需要从互联网等公共网络上下载资料转入内网计算机时，建议用刻录光盘的方式实现转存；

8. 对计算机系统的各个账号要设置强口令，及时删除或禁用过期账号；

9. 定期备份系统和数据，当遭到病毒严重破坏后能迅速修复。

二、如何防范 QQ、微博等账号被盗

1. 账户和密码尽量不要相同，定期修改密码，增加密码的复杂度，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码；

2. 密码尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换；

3. 不同用途的网络应用，应该设置不同的用户名和密码；

4．在网吧使用电脑前重启机器，警惕输入账号密码时被人偷看；为防账号被侦听，可先输入部分账户名、部分密码，然后再输入剩下的账户名、密码；

5. 涉及网络交易时，要注意通过电话

与交易对象本人确认。

三、如何安全使用电子邮件

1. 不要随意点击不明邮件中的链接、图片、文件；

2.使用电子邮件地址作为网站注册的用户名时，应设置与原邮件密码不相同的网站密码；

3. 设置安全的电子邮件系统登录密码，并设置适当的找回密码提示问题；

4. 当收到与个人信息和金钱相关（如中奖、集资等）的邮件时要提高警惕。

四、如何防范钓鱼网站

1. 通过查询网站备案信息等方式核实网站资质的真伪；

2. 安装安全防护软件；

3. 警惕中奖、修改网银密码的通知邮件、短信，不轻意点击未经核实的陌生链接；

4. 不在多人共用的电脑上进行金融业务操作，如网吧等。

五、如何保证网络游戏安全

1. 输入密码时尽量使用软键盘，并防止他人偷窥；

2. 为电脑安装安全防护软件，从正规网站上下载网游插件；

3. 注意核实网游地址；

4. 如发现账号异常，应立即与游戏运营商联系。

六、如何防范网络虚假、有害信息

1. 及时举报疑似谣言信息；

2. 不造谣、不信谣、不传谣；

3. 注意辨别信息的来源和可靠度，通过经第三方可信网站认证的网站获取信息；

4. 注意辨别打着“发财致富”、“普及科学”、传授“新技术”等幌子的信息；

5. 在获得相关信息后，应先去函或去电与当地工商、质检等部门联系，核实情况。

七、当前网络诈骗类型及如何预防

常见网络诈骗类型有如下四种：

一是利用 QQ 盗号和网络游戏交易进行诈骗，冒充好友借钱；

二是网络购物诈骗，收取订金骗钱；

三是网上中奖诈骗，指犯罪分子利用传播软件随意向互联网 QQ 用户、MSN 用户、电子邮箱用户、网络游戏用户、淘宝用户等发布中奖提示信息；

四是“网络钓鱼”诈骗，利用欺骗性的电子邮件和伪造的互联网站进行诈骗活动，获得受骗者财务信息进而窃取资金。

预防网络诈骗的措施如下:

1. 不贪便宜；

2. 使用比较安全的支付工具；

3. 仔细甄别，严加防范；

4. 不在网上购买非正当产品，如手机监听器、毕业证书、考题答案等；

5. 不要轻信以各种名义要求你先付款的信息，不要轻易把自己的银行卡借给他人；

6. 提高自我保护意识，注意妥善保管自己的私人信息，不向他人透露本人证件号码、账号、密码等，尽量避免在网吧等公共场所使用网上电子商务服务。

八、如何防范社交网站信息泄露

1. 利用社交网站的安全与隐私设置保护敏感信息；

2. 不要轻意点击未经核实的链接；

3. 在社交网站谨慎发布个人信息；

4. 根据自己对网站的需求选择注册。

九、如何保护网银安全

网上支付的安全威胁主要表现在以下三个方面：

一是密码被破解，如果用户设置的密码是“弱密码”，且在所有网站上使用相同密码或者有限的几个密码，易遭受攻击者暴力破解；

二是病毒、木马攻击，木马程序会监视浏览器正在访问的网页，获取用户账户、密码信息或者弹出伪造的登录对话框，诱骗用户输入相关信息，然后将窃取的信息发送出去；

三是钓鱼平台，攻击者利用欺骗性的电子邮件和伪造的Web 站点来进行诈骗，如将自己伪装成知名银行或信用卡公司等可信的品牌，获取用户的银行卡号、口令等信息。

保护网银安全的防范措施如下：

1. 尽量不要在多人共用的计算机（如网吧等)上进行银行业务，发现账号有异常情况，应及时修改交易密码并向银行求助；

2. 核实银行的正确网址，安全登录网上银行，不要随意点击未经核实的陌生链接；

3. 在登录时不选择“记住密码”选项，登录交易系统时尽量使用软键盘输入交易账号及密码，并使用该银行提供的数字证书增强安全性，核对交易信息；

4. 交易完成后要完整保存交易记录；

5. 网上银行交易完成后，应点击“退出”按钮，使用 U 盾购物时，交易完成后要立即拔下 U 盾；

6. 对网络单笔消费和网上转账进行金额限制，并为网银开通短信提醒功能，在发生交易异常时及时联系相关客服；

7. 通过正规渠道申请办理银行卡及信用卡；

8. 不要使用存储额较大的储蓄卡或信用额度较大的信用卡开通网上银行；

9. 支付密码最好不要使用姓名、生日、电话号码，也不要使用 12345 等默认

密码或与用户名相同的密码；

10. 应注意保护自己的银行卡信息资料，不要把相关资料随便留给不熟悉的公司或个人。

十、如何保护网上购物安全

网上购物面临的安全风险主要有如下方面：

一是通过网络进行诈骗，部分商家恶意在网络上销售自己没有的商品，因为绝大多数网络销售是先付款后发货，等收到款项后便销声匿迹；

二是钓鱼欺诈网站，以不良网址导航网站、不良下载网站、钓鱼欺诈网站为代表的“流氓网站”群体正在形成一个庞大的灰色利益链，使消费者面临网购风险；

三是支付风险，一些诈骗网站盗取消费者的银行账号、密码、口令卡等，同时，消费者购买前的支付程序繁琐以及退货流程复杂、时间长，货款只退到网站账号不退到银行账号等，也使网购出现安全风险。

保护网上购物安全的主要措施如下：

1. 核实网站资质及网站联系方式的

真伪，尽量到知名、权威的网上商城购物；

2. 尽量通过网上第三方支付平台交易，切忌直接与卖家私下交易；

3. 在购物时要注意商家的信誉、评价和联系方式；

4. 在交易完成后要完整保存交易订单等信息；

5. 在填写支付信息时，一定要检查支付网站的真实性；

6. 注意保护个人隐私，直接使用个人的银行账号、密码和证件号码等敏感信息时要慎重；

7. 不要轻信网上低价推销广告，也不要随意点击未经核实的陌生链接。

十一、如何防范网络传销

网络传销一般有两种形式：

一是利用网页进行宣传，鼓吹轻松赚大钱的思想，如网页上“轻点鼠标，您就是富翁”、“坐在家里，也能赚钱”等信息；

二是建立网上交易平台，靠发展会员聚敛财富，主要通过交纳一定资金或购买一定数量的产品作为“入门费”，获得加入资格，或通过发展他人加入其中，形成

上下线的层级关系，以直接或间接发展的下线所交纳的资金或者销售业绩为计算报酬的依据。

防范网络传销需注意以下方面：

1. 在遇到相关创业、投资项目时，要仔细研究其商业模式。无论打着什么样的旗号，如果其经营的项目并不创造任何财富，却许诺只要交钱入会，发展人员就能获取“回报”，请提高警惕；

2. 克服贪欲，不要幻想“一夜暴富”。如果抱着侥幸心理参与其中，最终只会落得血本无归、倾家荡产，甚至走向犯罪的道路。

十二、如何防范假冒网站

假冒网站的主要表现形式有两种：

一是假冒网站的网址与真网站网址较为接近；

二是假冒网站的页面形式和内容与真网站较为相似。

不法分子欺诈的手法通常有如下三种：

一是将假冒网站地址发送到客户的电脑上或放在搜索网站上诱骗客户登录，

窃取客户信息；

二是通过手机短信、邮箱等，冒充银行名义发送诈骗短信，诱骗客户登录假冒网站；

三是建立假冒电子商务网站，通过假的支付页面窃取客户网上银行信息。

防范假冒网站的措施如下：

1. 直接输入所要登录网站的网址，不通过其他链接进入；

2. 登录网站后留意核对所登录的网址与官方公布的网址是否相符；

3. 登录官方发布的相关网站辨识真伪；

4. 安装防护软件，及时更新系统补丁；

5. 当收到邮件、短信、电话等要求到指定的网页修改密码，或通知中奖并要求在领取奖金前先支付税金、邮费等时，务必提高警惕。

十三、如何准确访问和识别党政极端、事业单位网站

按照党政机关、事业单位网站与其实体名称对应、网络身份与实体机构相符的

原则，国家专门设立“.政务”和“.公益”中文域名，由工业和信息化部授权中央编办电子政务中心负责注册管理；

1. 通过中文域名访问党政机关、事业单位网站“.政务”和“.公益”域名是党政机关和事业单位的专用中文域名，其注册、解析均由机构编制部门进行严格审核和管理。通过在浏览器地址栏输入“.政务”和“.公益”中文域名，可准确访问党政机关和事业单位网站。如何准确访问和识别党政机关、事业单位网站，详见政务和公益机构域名注册管理中心（http://www.chinagov.cn）；

2. 通过查看网站标识识别党政机关和事业单位网站

网站标识是经机构编制部门核准后统一颁发的电子标识，该标识显示在网站所有页面底部中间显著位置。点击该标识，即可查看到经机构编制部门审核确认的该网站主办单位的名称、机构类型、地址、职能，以及网站名称、域名和标识发放单位、发放时间等信息，以确认该网站是否为党政机关或事业单位网站。

十四、如何防范网络非法集资诈骗

非法集资特点如下：

一是未经有关部门依法批准，包括没有批准权限的部门批准的集资，以及有批准权限超越权限批准的集资；

二是承诺在一定期限内给出资人还本付息，还本付息的形式除货币形式为主外，还包括实物形式或其他形式；

三是向社会不特定对象及社会公众筹集资金，集资对象多为下岗职工、退休人员、农民等低收入阶层，承受经济损失的能力较低；

四是以合法形式掩盖其非法集资的性质。

防范非法集资注意事项：

1. 加强法律知识学习，增强法律观念；

2. 要时刻紧绷防范思想，不要被各种经济诱惑蒙骗，摒弃“发横财”和“暴富”等不劳而获的思想；

3. 在投资前详细做足调查，对集资者的底细了解清楚；

4. 若要投资股票、基金等金融证券，应通过合法的证券公司申购和交易，不轻

信非法从事证券业务的人员和机构，以及小广告、网络信息、手机短信、推介会等方式；

5. 社会公众不要轻信非法集资犯罪嫌疑人的任何承诺，以免造成无法挽回的巨大经济损失。

十五、使用 ATM 机时需要注意哪些问题

1. 使用自助银行服务终端时，留意周围是否有可疑的人，操作时应避免他人干扰，用一只手挡住密码键盘，防止他人偷窥密码；

2. 遭遇吞卡、未吐钞等情况，应拨打发卡银行的全国统一客服热线，及时与发卡银行取得联系；

3. 不要拨打机具旁粘贴的电话号码，不要随意丢弃打印单据；

4. 刷卡门禁不需要输入密码。

十六、受骗后该如何减少自身的损失

1. 及时致电发卡银行客服热线或直接向银行柜面报告欺诈交易，监控银行卡交易或冻结、止付银行卡账户；如被骗钱

款后能准确记住诈骗的银行卡账号，可通过拨打银联中心客服电话的人工服务台，查清该诈骗账号的开户银行和开户地点（可精确至地市级）；

2. 对已发生损失或情况严重的，应及时向当地公安机关报案；

3. 配合公安机关及发卡银行做好调查、举证工作。

十七、网络服务提供者和其他企事业单位在业务活动中收集、使用公民个人电子信息，应当遵循什么原则

应当遵循合法、正当、必要的原则，明示收集和使用信息的目的、方式和范围，并经被收集者同意；不得违反法律、法规的规定以及双方的约定收集和使用公民个人电子信息。

十八、当发现网上有泄露个人身份、侵犯个人隐私的网络信息时该怎么办

发现泄露个人身份、侵犯个人隐私的网络信息，或者受到商业性电子信息侵扰，公民有权要求网络服务提供者删除有关信息或采取其他必要措施予以制止，必

要时可向相关的网络安全事件处置机构进行举报或求援。

移动终端安全篇

一、如何安全地使用 Wi-Fi

目前 Wi-Fi 陷阱有两种：

（一）是“设套”，主要是在宾馆、饭店、咖啡厅等公共场所搭建免费 Wi-Fi，骗取用户使用，并记录其在网上进行的所有操作记录；

（二）是“进攻”，主要针对一些在家里组建 Wi-Fi 的用户，即使用户设置了 Wi-Fi 密码，如果密码强度不高的话，黑客也可通过暴力破解的方式破解家庭 Wi-Fi，进而可能对用户机器进行远程控制。

安全地使用 Wi-Fi，要做到以下几方面:

1. 勿见到免费 Wi-Fi 就用，要用可靠的 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，应特别注意与公共场所内已开放的 Wi-Fi 名称类似的信号很可能是钓鱼陷阱，尽量不

要在公共场所进行网银操作；

3、修改家中无线路由器默认用户名和密码；启用 WPA / WEP 加密方式；修改默认 SSID 号，关闭 SSID 广播；必要时可启用 MAC 地址过滤；无人使用时，关闭路由器电源。

二、如何安全地使用智能手机

1. 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；

2. 不要轻易打开陌生人通过手机发送的链接和文件；

3. 为手机设置锁屏密码，并将手机随身携带；

三、如何防范病毒和木马对手机的攻击

1. 为手机安装安全防护软件，开启实时监控功能，并定期升级病毒库；

2. 警惕收到的陌生图片、文件和链接，不要轻易打开在 QQ、微信、短信、邮件中的链接；

3. 到权威网站下载手机应用。

四、如何防范“伪基站”的危害

近年来出现了一种利用“伪基站”设备作案的新型违法犯罪活动。“伪基站”设备是一种主要由主机和笔记本电脑组成的高科技仪器，能够搜取以其为中心、一定半径范围内的手机卡信息，并任意冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。犯罪嫌疑人通常将“伪基站”放在车内，在路上缓慢行驶或将车停放在特定区域，从事短信诈骗、广告推销等违法犯罪活动。

“伪基站”短信诈骗主要有两种形式：

一是“广种薄收式”，嫌疑人在银行、商场等人流密集地以各种汇款名目向一定半径范围内的群 众手机发送诈骗短信；

二是“定向选择式”，嫌疑人筛选出手机号后，以该号码的名义向其亲朋好友、同 事等熟人发送短信，实施定向诈骗。

用户防范“伪基站”诈骗短信可从如下方面着手：

1. 当用户发现手机无信号或信号极弱时仍然能收到推销、中奖、银行相关短信，则用户所在区域很可能被 “伪基站”覆盖，不要相信短信的任何内容，不要轻信收到的中奖、推销信息，不轻信意外之财；

2. 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，不向任何陌生账号转账；

3. 安装手机安全防护软件，以便对收到的垃圾短信进行精准拦截。

4. 在 QQ、微信等应用程序中关闭地理定位功能，并仅在需要时开启蓝牙；

5. 经常为手机数据做备份；

6. 安装安全防护软件，并经常对手机系统进行扫描；

7. 到权威网站下载手机应用软件，并在安装时谨慎选择相关权限；

8. 不要试图破解自己的手机，以保证应用程序的安全性。

五、如何防范骚扰电话、电话诈骗、垃圾短信

用户使用手机时遭遇的垃圾短信、骚扰电话、电信诈骗主要有以下 4 种形式：

一是冒充国家机关工作人员 实施诈骗；

二是冒充电信等有关职能部门工作人员，以电信欠费、送话费等为由实施诈骗；

三是冒充被害 人的亲属、朋友，编造生急病、发生车祸等意外急需用钱，从而实施诈骗；

四是冒充银行工作人员，假称 被害人银联卡在某地刷卡消费，诱使被害人转账实施诈骗。

在使用手机时，防范骚扰电话、电话诈骗、垃 圾短信的主要措施如下：

1. 克服“贪利”思想，不要轻信，谨防上当；

2. 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；

3.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；

4. 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；

5. 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；

6. 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问；

7. 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。

六、出差在外，如何确保移动终端的隐私安全

1. 出差之前备份好重要数据；

2. 不要登录不安全的无线网络；

3. 在上网浏览时不要选择“记住用户名和密码” ；

4. 使用互联网浏览器后，应清空历史记录和缓存内容；

5. 使用公用电脑时，当心击键记录程序和跟踪软件。

七、如何防范智能手机信息泄露

1. 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；

2. 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；

3. 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；

4. 下载软件或游戏时，应详细阅读授权内容，防止将木马带到手机中；

5. 经常为手机做数据同步备份；

6. 勿见码就刷。

八、如何保护手机支付安全

目前移动支付上存在的信息安全问题主要集中在以下两个方面：

一是手机丢失或被盗，即不法分子盗取受害者手机后，利用手机的移动支付功能，窃取受害者的财物；

二是用户信息全意识不足，轻信钓鱼网站，当不法分子要求自己告知对方敏感信息时无警惕之心，从而导致财物被盗。手机支付方便快捷，但是通过移动互联网进行交易，安全防范工作一定要做足，不然智能手机也会“引狼入室”。

保护智能手机支付安全的措施如下：

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。

个人信息安全篇

一、容易被忽视的个人信息有哪些

个人信息是指与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的数据。一般包括姓名、职业、职务、年龄、血型、婚姻状况、宗教信仰、学历、专业资格、工作经历、家庭住址、电话号码(手机用户的手机号码)、身份证号码、信用卡号码、指纹、病史、电子邮件、网上登录账号和密码等等。覆盖了自然人的心理、生理、智力，以及个体、社会、经济、文化、家庭等各个方面。个人信息可以分为个人一般信息和个人敏感信息。个人一般信息是指正常公开的普通信息，例如姓名、性别、年龄、爱好等。个人敏感信息是指一旦遭泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

二、个人信息泄露的途径及后果

目前，个人信息的泄露主要有以下途径:

1. 利用互联网搜索引擎搜索收集个人信息，私自出售给他人；

2. 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；

3. 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，私下出售；

4. 借各种“问卷调查”之名，以奖品为诱惑，窃取被调查者的个人信息，包括详细联系方式、收入情况、信用卡情况等；

5. 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；

6. 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；

7. 超市、商场开展正常邮寄免费资料、申办会员卡活动时掌握到的个人信

息，被个别人向外泄露。

目前，针对个人信息的犯罪已经形成了一条灰色的产业链，在这个链条中，有专门从事个人信息收集的泄密源团体，他们之中包括一些有合法权限的内部用户主动通过 QQ、互联网、邮件、移动存储等各类渠道泄露信息。还包括一些黑客，通过攻击行为获得企业或个人的数据库信息；有专门向泄密源团体购买数据的个人信息中间商团体，他们根据各种非法需求向泄密源购买数据，作为中间商向有需求者推销数据，作为中间商买卖、共享和传播各种数据库；还有专门从中间商团体购买个人信息，并实施各种犯罪的使用人团体，他们是实际利用个人信息侵害个人利益的群体。据不完全统计，这些人在获得个人信息后，会利用个人信息从事五类违法犯罪活动：

1. 电信诈骗、网络诈骗等新型、非接触式犯罪。如 2012 年底，北京、上海、深圳等城市相继发生大量电话诈骗学生家长案件。犯罪分子利用非法获取的公民家庭成员信息，向学生家长打电话谎称其

在校子女遭绑架或突然生病，要求紧急汇款解救或医治，以此实施诈骗。

2. 直接实施抢劫、敲诈勒索等严重暴力犯罪活动。如 2012 年初，广州发生犯罪分子根据个人信息资料，冒充快递员，直接上门抢劫，造成户主一死两伤的恶性案件。

3. 实施非法商业竞争。不法分子以信息咨询、商务咨询为掩护，利用非法获取的公民个人信息，收买客户、打压竞争对手。

4. 非法干扰民事诉讼。不法分子利用购买的公民个人信息，介入婚姻纠纷、财产继承、债务纠纷等民事诉讼，对民众正常生活造成极大困扰。

5. 滋扰民众。不法分子获得公民个人信息后，通过网络人肉搜索、信息曝光等行为，恶意曝光个人隐私，滋扰民众生活。

三、如何防范个人信息泄露

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. 敏感个人信息需加密保存；

3. 不使用 U 盘存储交互个人敏感信

息；

4. 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. 只将个人信息转移给合法的接收者；

6. 个人敏感信息需带出公司时要防止被盗、丢失；

7. 电子邮件内容涉及个人信息发送时要加密，并注意切勿错发；

8. 邮包寄送时选择可信赖的邮寄公司，并要求回执；

9. 避免传真错误发送；

10. 废弃纸质资料要用碎纸机销毁；

11. 废弃的光盘、U 盘、电脑等要消磁或彻底破坏。

图书与信息中心网络信息服务主页：
http://net.njau.edu.cn
微信号：njau-library

服务电话：
84396018（教学区网络、校园信息应用）
84395733（宿舍区网络）
现场受理地址：理科楼南一楼网络信息服务大厅