

网络安全知识手册

苏州大学数据资源与信息化建设管理处

前言

随着 5G 网络的全面覆盖，互联网科技飞速发展，智能手机和电脑成为人们传播信息、互相交流、学习知识、休闲娱乐的工具。然而，互联网为我们的生活、学习和工作带来便利的同时也带来了风险和危害。在互联网世界里，每个人都是“半透明”的状态，时刻都可能遭遇计算机中毒、文档意外丢失、黑客异常攻击、网络行骗诈骗、个人信息泄露等威胁。

本手册针对常见的网络安全问题，提供了一些简便实用的措施和方法，帮助大家提升网络安全防范意识、提高网络安全防护技能、遵守国家网络安全法律和法规，共同维护、营造和谐的网络环境。

目录

一、案例.....	1
二、上网安全.....	6
1. 如何防范病毒或木马的攻击	
2. 如何防范账号和密码安全	
3. 如何安全使用电子邮件	
4. 如何防范钓鱼网站以及假冒网站	
5. 如何防范网络传销和诈骗	
6. 如何安全使用网上银行	
7. 如何安全网站炒股、购买基金	
8. 如何安全网上购物	
9. 如何防范虚假信息传播	
三、移动终端安全.....	13
1. 如何安全使用 wifi	
2. 如何安全使用智能手机	
3. 如何防范伪基站	
4. 如何防范骚扰电话、电话诈骗、垃圾短信	
5. 如何防范智能手机信息泄露。	
6. 如何保护手机支付安全	
7. 如何正确扫描二维码	
8. 如何防范虚假公众号	
9. 手机遗失的风险	
10. 处理旧手机时的注意事项	
四、个人信息安全.....	20
1. 什么是个人信息	
2. 个人信息泄露的途径和后果	
3. 如何防范个人信息泄露	
4. 发现个人信息泄露时怎么办	
五、计算机安全.....	23
1. 计算机中毒有哪些症状	
2. 在使用电脑过程中应该采取哪些网络安全防范措施	
3. 如何防范 U 盘、移动硬盘泄密	
4. 勒索软件的防范建议	
六、相关法律法规.....	25

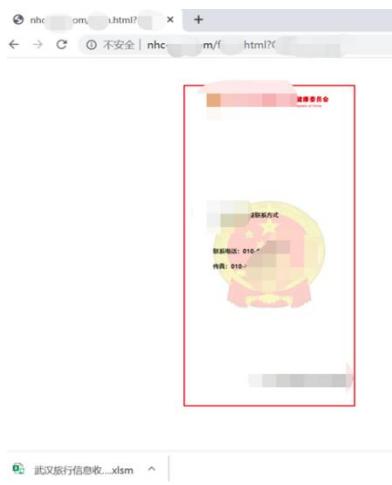
一、案例

1. 疫情期间，境外多个国家和地区对中国发动网络攻击

从2020年1月下旬开始，有一个黑客团伙用防疫和中医药相关的文件作诱饵，通过他们伪造的QQ邮箱界面盗取用户邮箱账号和密码。文件中没有夹带木马病毒，杀毒软件也不会发现。一旦点击，用户账户信息就会完全暴露在黑客面前。黑客们攻击的目标都是政府部门职员，安全风险大大增加。



2020年2月，印度APT组织“白象”（Patchwork、摩诃草）使用了一个伪装成我国卫生主管部门的域名，并借助新型肺炎为话题，伪造疫情相关文件，对我国医疗工作领域发动APT攻击。该组织于2020年1月注册仿冒域名“nhc****.com”，访问部分链接会直接下载名为“武汉旅行信息收集申请表.xlsx”、“卫生部指令.docx”的恶意文档，打开后将下载具备信息窃取、远程控制功能的木马后门。





2020年5月，有国外机构披露，疑似与越南有联系的黑客组织APT32（海莲花OceanLotus）在过去的数月中，持续对我国重要卫生医疗机构发起网络攻击，以获取和新型冠状病毒相关的重要信息情报。该黑客组织用名为“冠状病毒实时更新：中国正在追踪来自湖北的旅行者.docx”、“湖南省家禽H5N1亚型高致病性禽流感疫情情况.docx”样本信息文件作诱饵，使用户执行木马程序，最终达到控制系统、窃取情报的目的。本轮攻击还使用了自利用手法绕过了部分杀毒软件的查杀。

2. 多地高校数万学生隐私遭泄漏

2020年4月，河南财经政法大学、西北工业大学明德学院、重庆大学城市科技学院等高校的数千名学生发现，自己的个人所得税App上有陌生公司的就职记录。税务人员称，很可能是学生信息被企业冒用，以达到偷税的目的。郑州西亚斯学院多名学生反映，学校近两万学生个人信息被泄露，以表格的形式在微信、QQ等社交平台上流传。对此，该校官方微博在回应学生时称，已向公安机关报备，正在调查之中。5月31日，有人在班级微信群中发来两份“返校学生名单”，该名单涉及近两万名学生，信息具体到名字、身份证号、年龄、专业及宿舍门牌号，等等。事件发生后，多名学生反映收到骚扰电话。

3. 微博5.38亿账号信息在暗网出售

2020年3月，5.38亿条微博用户信息在暗网出售，其中1.72亿条有账户基本信息，包括：用户名、关注数、地理位置、最后一次微博发布时间等微博公开信息，售价1388美元。有新京报记者在Telegram上向灰产人士购买了价值约12元人民币的积分，获得了201条微博用户信息，其中不少信息包括用户身份证号、手机号、密码、生日等私密信息。对于灰产人士提供的微博定向查询手机号服务，记者测试查询了3个已绑定手机的微博账号，结果有2个微博账号被查询到了正确的关联手机号码，其中1个还给出了微博绑定的QQ等更详细的信息。

4. 网络交友+投资=诈骗！

近期，社交软件流行网络，不少市民纷纷下载使用，但是不法分子也盯上了此类软件，通过搭建虚假投资平台，在交友骗取信任后以“稳赚不赔”“操作简单”等为卖点博人眼球，诱导群众充值投资，实施网络诈骗。

1月12日，连云港市民李先生报警称，其通过某社交软件收到好友申请，后对方以投资理财向其发送二维码并让其扫码下载“兴业证券”APP进行投资，被骗13万余元。

2月11日，苏州市民张先生报警称，其在某软件上认识对方，对方在聊天中发送网址链接并让其下载“香港交易所”的APP，张某按照对方指示进行投资，被骗53万余元。

2月12日，淮安市民贾女士报警称，其在“SOUL”APP上，好友以追求其为由让其下载“恒泰财经”APP进行投资理财，被骗21万余元。

5. 扫描二维码要小心

一天，小陈在网上冲浪时看到一个“扫码免费送XX视频会员”的广告，当他用QQ扫描二维码后，跳转到一个提示“您的身份已过期，请重新登录并领取”的页面，小陈没多想就输入自己的QQ账号密码并登录。

不久后，他发现自己的QQ显示在他人手机上登录，而QQ余额里的2万多钱也没了。原来，小陈扫码进入的是一个植入木马程序的假登录页面，不法分子在获取小陈输入的账号密码后，可随意登录甚至修改密码，还有可能将假海报自动群发给好友，导致更多好友遭遇。

6. 手机数据被远程删除

1月12日，某网友在网上发布信息爆料，在与客服沟通领取“拼多多”红包后发现，其使用的vivo手机操作系统提示，“检测到‘拼多多’已删除照片或视频”，该网友表示，随后发现自己提供给客服的截图证据被删除，仅在已删除图片中可找到。

该名网友再次与拼多多客服沟通，质疑其侵害用户隐私。但拼多多客服不认为App有此行为，而是用户自己“误操作”或者“清除缓存”导致。该名网友遂又与vivo客服沟通，vivo客服声称手机操作系统不会对图片和视频进行操作，如用户授予了App存储权限，则App是可以利用此权限执行相应操作的。



此事被曝光后，立即受到网民和媒体强烈关注，迅速登上了微博热搜榜。1月12日晚上19点拼多多发布了《关于个别用户反馈“vivo手机提示拼多多删除照片”的说明》，声明会删除客服聊天页面拍摄且编辑的照片原图。这则说明也表明了，App在获取“存储”权限后，确实具备读增删改图片等的能力。

关于个别用户反馈“vivo手机提示拼多多删除照片”的说明

近日，我们收到个别用户反馈“vivo手机提示拼多多App删除照片”，团队十分重视并第一时间核查，初步原因说明如下：

1，在拼多多App内的客服聊天页面，点击“+”选择“拍摄”并完成拍照后，如果立刻点击发送，这一图片会被保存至系统相册；如果在发送之前，进行剪裁、美化等编辑动作，App会保存一张拍完的图片到系统相册，起到类似于“缓存”的作用，待编辑完成并发送后，App会删除编辑之前的图片，保留编辑后发送的图片。这导致了vivo系统认为有删除图片的操作。

7. 警惕手机病毒

2020年5月以来，朝阳警方陆续接到受害用户报案称，自己的手机上不止一个APP账号被盗。朝阳警方迅速展开侦查，通过对受害用户的询问及相关案情的梳理、分析，民警锁定了一个可疑的抽奖链接。

被盗号用户均反映，他们在某知名网络交友APP上，曾点开过网友发来的“某交友软件5周年抽奖”的链接。随后几天他们发现，手机上多款APP的密码被人篡改，原密码无法登陆。

经民警核实，该款网络交友APP的运营商称，从未举办过5周年抽奖活动。民警进一步调查发现，“5周年抽奖”链接实为不法人员设计的虚假网站链接，暗含木马病毒。网友点开该链接会导致手机中毒，不法分子即可盗取中毒手机上各类APP的账号信息等，并通过拦截手机短信、获取短信验证码进行密码修改，后通过出售账号、密码牟利。

二、上网安全

1. 如何防范病毒或木马的攻击

什么是木马？什么是病毒？

“木马”这个名字来源于古希腊传说特洛伊木马。在古希腊传说中，希腊联军围困特洛伊久攻不下，于是把一批勇士埋伏在一匹巨大的木马腹内，放在城外后，佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。到了夜间，埋伏在木马中的勇士跳出来，打开了城门，希腊将士一拥而入攻下了城池。



和故事中的“木马”一样，计算机病毒中的“木马”也是通过伪装成正常的程序吸引用户下载、执行，随后进入到电脑中的，通过特定的程序（木马程序）来控制另一台计算机。通常它有两个可执行程序：一个是控制端，另一个是被控制端。木马攻击者通过客户端与受害者的计算机服务建立远程连接，控制受害者计算机，盗取信息。

与木马程序不同，病毒具有传播性，以感染为目的，破坏计算机系统，占用硬盘空间，内存等物理设备导致计算机瘫痪。但现今单纯的病毒木马蠕虫等都很少了，绝大部分恶意软件都是混合型的。

安全建议：

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；
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；
3. 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；

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，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口令，及时删除或禁用过期账号；
9. 定期备份，当遭到病毒严重破坏后能迅速修复。

2. 如何防范账号和密码安全

在信息化时代，各类交流平台以及各种工具平台都是通过账号密码进行验证和登录。账户安全的重要性不言而喻，它的范围之广，关系到每一个人，包括个人手机 APP 账户、电脑网站账户、银行卡账户密码等各类账号信息。如果这些信息被泄露或者是被不法分子利用，将会造成不可挽回的损失。



账号密码安全风险主要有以下几方面：

1. 账号密码强度弱，被暴力破解；
2. 账号密码存储不当泄露；
3. 多个系统使用相同的账号密码，其中某个系统被拖库；
4. 在来历不明的网站，或者公共场所登录了账号密码，被恶意程序窃取。

安全建议：

1. 不要使用与隐私相关的信息作为密码，如姓名拼音、出生日期和手机号；避免使用有规律的字母或数字组合；根据账号的重要性，设置不同的密码，切忌“一套密码走天下”；
2. 对于极其重要的账户，可以通过动态密码、指纹验证、短信验证等相结合的多因子验证来提升账户的安全性；
3. 对于重要系统，要定期更换密码；
4. 账号密码在未经加密的情况下不要存储在互联网上或以纸质形式记录，这些存储方式同样容易导致密码泄露；
5. 不在公共场合随意输入自己的账号密码。

3. 如何安全使用电子邮件

电子邮件常见几种攻击形式有窃听攻击、钓鱼邮件、附件病毒。

窃听攻击

窃听攻击是指黑客在局域网里通过抓包的方式，窃取邮件的信息。比如当你在外通过被黑客破解了的无线路由器连接网络，如果黑客在无线路由器上安装了间谍软件，或者嗅探工具，去对无线网络里面的数据进行抓包，而此时通过该网络发的邮件没有加密，那么你的邮件就很可能被黑客在局域网里面通过抓包的方式，窃取了这封邮件的信息。

安全建议：

为了防止针对邮件的窃听攻击，我们不要通过不可控的网络传输敏感的邮件；收发邮件的时候，要确保传输通道是加密的，对附件实施加密，通过微信、短信或者打电话等其他的不同的传输渠道告知密码，确保传输信息的安全。

钓鱼邮件

钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。

安全建议：

遇到这种索要敏感信息的邮件，要保持警惕、保持冷静，提高警惕。如果不确认的话，第一时间主动联系发件人，确认他有没有发过这封邮件，提高个人的安全意识。尽量避免直接点击邮件中的网络链接。

链接、附件病毒

很多人看到邮件中有附件时，会习惯性的点开查看。但是电子邮件链接、附件中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，造成文件丢失损坏甚至系统瘫痪。

安全建议：

确保自己的邮件客户端禁止访问可执行的文件；加强个人安全意识，遇到可疑的链接、附件不要轻易点开。

4. 如何防范钓鱼网站以及假冒网站

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。

安全建议：

1. 留意网站配色、内容、链接等细微之处；
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. 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. 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，尤其是短网站；
5. 仔细辨别网址，比如工商银行网址 icbc. com. cn 被混淆为 Icbc. com. cn；
www. microsoft. com 被混淆为 ww-w. rncrosoft. com；
6. 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。

5. 如何防范网络传销和诈骗

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、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。

安全建议：

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。

6. 如何安全使用网上银行

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，很多用户或企业使用的密码都是弱密码，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，诱骗用户输入相关密码，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。

安全建议：

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。

7. 如何安全网站炒股、购买基金

网上炒股面临的安全风险主要体现在以下几个方面：一是网络钓鱼，不法分子制作仿冒证券公司网站，诱导人们登录后窃取用户账号和密码；二是盗买盗卖，攻击者利用电脑“木马病毒”窃取他人的证券交易账号和密码后，低价抛售他人股票，自己低价买入后再高价卖出，赚取差价。

安全建议：

1. 保护交易密码和通讯密码；
2. 尽量不要在多人共用的计算机（如网吧等）上进行股票交易，并注意在离开电脑时锁屏；
3. 注意核实时证券公司的网站地址，下载官方提供的证券交易软件，不轻信小广告；
4. 及时修改个人账户的初始密码，设置安全密码，发现交易有异常情况时，要及时修改密码，并通过截图、拍照等保留证据，第一时间向专业机构或证券公司求助。

8. 如何安全网上购物

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。

安全建议：

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；
8. 如果发现受骗，应及时联系银行报告欺诈交易，监控银行卡交易或冻结、止付银行卡账户；对已发生损失或情况严重的，应及时向当地公安机关报告并配合调查举证。

9. 如何防范虚假信息传播

互联网时代下，网络已经成为人们获取信息、资讯的重要渠道。与传统媒体相比，网络媒体时效性更高、信息资源更丰富，使受众从中可以获取更多、更新、更全面的新闻信息。也正是因为网络媒体的这种优势，使得信息在网络中很容易被发布，更容易出现虚假信息。虚假信息一旦踏入互联网这一快速通道，不仅会造成网络自媒体公信力的下降，还会对虚假信息中当事人产生影响，甚至一部分用户也因此蒙受了一定的损失。

安全建议：

1. 选择正规的信息获取渠道；
2. 提升自身的信息辨别能力。一方面提升自身的知识面，与相关领域的专家进行交流，另一方面扩大信息获取渠道，进行相关信息的对比。
3. 不造谣、不信谣、不传谣，发现疑似谣言信息及时举报。

三、移动终端安全



1. 如何安全使用 wifi

(1) 免费 Wi-Fi 或公共 Wi-Fi

在餐厅、商场、火车站、机场等公众场所，通常都部署了免费的 Wi-Fi 热点，然而，攻击者可能会创建一个有迷惑性的 Wi-Fi 热点，一旦连接到这些恶意热点，可能会导致信息泄露、流量劫持等风险。

免费 Wi-Fi 加密方式通常较弱，一旦被破解，会导致所有接入者有被攻击者攻击的风险。

一些广告公司会在公共场所部署“Wi-Fi 探针”，当用户手机开启 Wi-Fi 功能时，探针盒子可以自动识别到手机的 MAC 地址、RSSI 值等信息，从而掌握用户的行为轨迹。如果将这些信息与大数据进行匹配，可能会关联到用户的设备 ID 和手机号码，再据此进行有针对性的营销推广。

安全建议

在公众场所链接 Wi-Fi 前，应留意周围的提示，接入官方提供的网络；在同一地区，警惕有相同或相似名字的 WiFi，很有可能有黑客搭建钓鱼 WiFi；在处理重要信息或进行移动支付时，不要使用公用网络，最好使用工具（比如：手机）自带的 4G/5G 网络。

在公共场所，尽量不要自行搭建个人热点，不要使用“Wi-Fi 分享器”等设备；如确有需要，在架设无线路由器前必须进行安全检查，Wi-Fi 应使用 WPA/WPA2 的加密方式、设置复杂密码、保证密码定期更改。

在不需要使用 Wi-Fi 和蓝牙时，将手机的 Wi-Fi、蓝牙功能关闭；使用手机安全软件，根据数据库中保存的记录，对潜在的推销电话进行拦截。

(2) 家庭 Wi-Fi

一些 Wi-Fi 密码共享类 APP 会在安装后自动上传所有已经连接过的 Wi-Fi 密码，其中很可能包含一些家庭、工作单位的密码。一旦攻击者使用这类工具，可以轻而易举地连接到家庭或单位的办公网络。

安全建议

避免使用 Wi-Fi 密码共享类 APP；如果需要使用，建议首先关闭自动上传密码功能。

尽量区分自用 Wi-Fi 和客人 Wi-Fi，避免来客有意无意地获取隐私信息。

2. 如何安全使用智能手机

智能手机在使用时必然要联网，否则无法体现其“智能”之处。当其联网时，和所处的网络有很大关系，也和手机本身的设置有关系，更和使用的人有关系。

安全建议

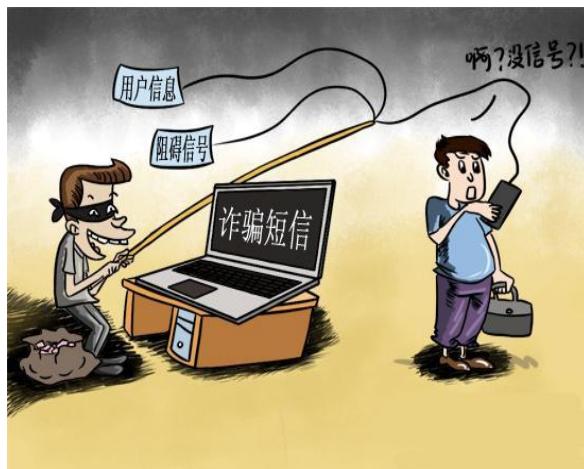
1. 为手机设置访问密码是保护手机

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；
4. 在QQ、微信等应用程序中关闭地理定位功能；
5. 仅在需要时开启蓝牙；
6. 经常为手机数据做备份；安装安全防护软件，并经常对手机系统进行扫描；
7. 到权威网站或应用市场下载手机应用软件，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。



3. 如何防范伪基站



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。

安全建议

1. 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. 如何防范骚扰电话、电话诈骗、垃圾短信

广告、骚扰电话和短信几乎每天都能见面，尤其当个人信息被泄露时，这类电话、短信会尤其的多，但并不是所有电话、短信都可以被忽略。

安全建议

1. 克服“贪利”思想，不要轻信，谨防上当；
2. 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；
3. 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；
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. 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。



5. 如何防范智能手机信息泄露。

智能手机泄露个人信息的 4 种方式：

- 1、恶意软件：在手机中预设软件，或通过远程植入软件，实时窃取用户信息：在盗取用户手机后，人工安装窃听软件或病毒软件。
- 2、病毒和木马：通过广告，邮件，APP 应用软件或二维码等途径传播手机病毒和木马，暗中破坏或窃取手机用户信息。
- 3、截获设备：通过专门的设备截获手机的通话和收发信息的内容。
- 4、恶意 WiFi：通过未加密的恶意 WiFi 连接，以设伏方式获取用户手机中的信息。

安全建议

- 1、通过正规渠道购买手机，选择正规手机售后维修店去维修，避免不法分子趁机安装窃听软件。
- 2、为智能手机安装一些正规下载的专业防火墙和防病毒软件，定期查杀病毒并进行软件升级。
- 3、不要随意点击身份可疑的广告，短信，二维码，不要轻易下载和安装网上搜索到的来历不明的 app 应用软件。
- 4、不要轻易连接免费和不设密码的 WiFi，使用要看清 WiFi 热点名称。
- 5、关闭手机中一些可能泄露用户隐私信息的服务，比如用户位置定位。
- 6、不要轻易将智能手机交给他人保管和使用，在手机失而复得或维修后应进行必要的专业检测。
- 7、长期不上网应关闭手机的无线连接功能及蓝牙，USB 接口等。
- 8、将私密数据加密保存，不轻易发送私密信息或以加密方式发送。
- 9、一旦发现手机流量异常或可疑应用上传隐私数据，应及时求助于正规售后服务商。
- 10、不把手机当密码记录本，不把身份证号，地址，银行卡号等敏感信息存在手机里，一旦手机丢失或中病毒，面临泄露风险。

6. 如何保护手机支付安全

手机支付和手机有关，也有二维码等媒介有关，所以当手机本身的设置以及手机本身所处的环境有问题时，会产生手机支付安全问题；当二维码有问题时，也能产生手机支付安全问题。



安全建议

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插件，减少手机中的本地分享，对程序执行权限加以限制；
2. 谨慎下载手机应用，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. 登录手机支付应用、网上商城时，勿选择“记住密码”选项；
4. 禁用 WiFi 自动连接到网络功能，尽量不使用公共 WiFi 来进行手机支付；
5. 如有必要，降低“小额免密”的支付额度；
6. 勿见二维码就刷。

7. 如何正确扫描二维码



如今，在餐厅，地铁，商场，甚至街边小广告上，二维码已无处不在。可是，由扫二维码带来的风险也日益显现。由于很多人的支付宝账号就是手机号，恶意二维码的始作俑者通过其他辅助手段就能很容易划走顾客支付宝内的钱。

安全建议

手机用户不要轻易扫描来源不明的二维码，如需扫描，可通过手机安全软件进行扫码，识别带毒二维码，保护移动支付宝及其他支付工具。

8. 如何防范虚假公众号

在互联网技术迅速发展给公众带来巨大便利的同时，也隐含着对公众不利的危险因素，公众普遍缺乏有效甄别网络平台海量信息的能力，并且相应的行业规范和法律规范未能及时跟上技术的发展，这也给不法分子以可乘之机。

安全建议

1、对于网络用户而言，应当慎重加入公众号，尤其要警惕那些没有规范途径的或者自己非常陌生的公众号，提高对个人信息尤其是敏感信息的保护意识，防患于未然。

2、对于网络平台运营者而言，其是有效规避、防范真假公众号的核心，因此应当强化管理意识并提高管理水平，及时发现并封禁违法违规的公众号，及时通知并配合公安机关开展相应的调查和处理；对于因为网络平台运营者的过错而导致相应损害发生的，网络用户有权向其主张承担相应的民事法律责任。

3、对于监管机构而言，应尽快建立监测、研判、预警、处置和追踪的网络安全问题联合处置机制，为包括公众号运营在内的网络环境提供完善的监管机制。并依法及时对违反网络安全运营职责的平台予以处理，使其能够在规避防范问题公众号时真正发挥核心功能。



9. 手机遗失的风险

手机遗失，并不仅仅是丢失了一部手机。

智能手机中安装了各种应用，这些应用不仅涉及到个人隐私，更涉及到资金的安全。当手机没有设置开机口令或仅设置了弱口令时，则手机内容将被一览无遗。

安全建议

- 1.为手机设置开机密码；
- 2.安装手机安全软件；
- 3.备份联系人和短信；
- 4.取消单独绑定手机的账号和密码；
- 5.修改家人手机号的备注名称。

当确定手机确实是遗失了而无法找回时：

- 1.致电手机运营商挂失手机号码；
- 2.挂失银行卡；
- 3.手机绑定支付宝的，拨打 95188 挂失；
- 4.微信用户登录 <http://110.qq.com/>冻结微信账号；
- 5.修改各相关应用软件的登录密码；
- 6.向常住户口所在地派出所申报丢失补领身份证；
- 7.补办手机卡。



10. 处理旧手机时的注意事项



现在手机的更新非常频繁，有的人一年就更新手机，最多两三年也会更新手机。买了新手机的你当然非常高兴，但是，千万不要忘记要好好处理淘汰的旧手机。处理旧手机的关键是防止手机信息泄露。

旧手机信息是怎么泄露的？

1、普通删除或恢复出厂设置并不能抹去数据，系统在执行文件删除时，仅是被做了一个“删除”的标记，但储存的数据本身依然存在，只是处于一个可覆盖的状态，照片，短信，通讯录，视频等都可以恢复。

2、如未进行新的数据操作，最上层信息很容易被恢复。因为硬盘上的数据可反复被覆盖，数据恢复一般只能读取覆盖在最上层的信息。

安全建议

- 1、将手机恢复出厂设置或格式化，再存入一些无关紧要的内容，将手机的存储空间占满；
- 2、不要将手机作为一般的生活垃圾扔掉，可卖给相对正规的厂家。

四、个人信息安全

1. 什么是个人信息

以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的各种信息。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。例如身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

2. 个人信息泄露的途径和后果

目前，个人信息的泄露主要有以下途径：

- 利用互联网搜索引擎搜索个人信息，汇集成册，并按照一定的价格出售给需要购买的人；
- 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；
- 借“问卷调查”之名，窃取群众个人信息。有人宣称只要在“调查问卷表”上填写信息，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；



7. 超市、商场通过向群众邮寄免费资料、申办会员卡时掌握到的群众信息，通过个别
人向外泄露。

8. 手机的定位功能如果被不法分子利用，就会对手机持有者进行跟踪，并窃取有关个
人的一些信息。

9. 用户分享网盘上的内容时不设置提取码或者密码，则里面的内容有可能会被网上的
爬虫抓取到并索引，文件就会变成公开访问并可以被任何人下载。

10. 家用监控摄像头可能导致用户监控视频被泄露，甚至会出现智能摄像头被恶意控制
的风险。

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。
2. 直接实施抢劫、敲诈勒索等严重暴力犯罪活动。
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，对群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、信息曝光等行为滋扰民众生活。

3. 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. 电子邮件发送时要加密，并注意不要错发；
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. 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。
12. 关闭不必要的软件定位功能，在社交平台发布信息时尽可能的避免发布位置信息；
13. 使用网盘分享文件时使用加密分享方式、并设定有效时间段，不要分享个人隐私信息，定期整理网盘内文件，尽可能避免将隐私信息存储在网盘上；
14. 使用家用监控时要选择正规产品，注册账户时使用高强度密码，避免摄像头正对隐私区域，不随意分享监控拍摄画面，不使用时应及时关闭电源。

4. 发现个人信息泄露时怎么办

公民发现泄露个人身份、侵犯个人隐私的网络信息，或者受到商业性电子信息侵扰，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止，必要时可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。

公民还可依据《侵权责任法》、《消费者权益保护法》以及《个人信息保护法》等，通过法律手段进一步维护自己的合法权益，如要求侵权人赔礼道歉、消除影响、回复名誉、赔偿损失等。

五、计算机安全

1. 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。



2. 在使用电脑过程中应该采取哪些网络安全防范措施



1. 安装防火墙和防病毒软件，并经常升级，及时更新木马库，给操作系统和其他软件打补丁；
2. 对计算机系统的各个账号要设置口令，及时删除或禁用过期账号；
3. 不要打开来历不明的网站、邮件链接或附件，不要执行从网上下载后未经杀毒处理的软件，不要打开聊天软件上收到的不明文件。
4. 打开任何移动存储器前用杀毒软件进行检查；
5. 定期备份，以便在遭到病毒、木马或恶意软件等的破坏后能迅速修复。

3. 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. U 盘、移动硬盘介入电脑前，先进行病毒扫描；
4. 定期备份并加密重要数据；
5. 不要将办公与个人的可移动存储介质混用。

4. 勒索软件的防范建议

1. 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的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；

2. 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；

3. 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；

4. 封堵端口：关闭无用的计算机服务/端口，开启 Windows 防火墙；

5. 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。



六、相关法律法规

1、《中华人民共和国网络安全法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

2、《国家网络空间安全战略》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

3、《中华人民共和国密码法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2019-10/27/c_1573711980953641.htm

4、《中华人民共和国电子签名法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2004-08/28/c_126468489.htm

5、《全国人民代表大会常务委员会关于加强网络信息保护的决定》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2012-12/29/c_133353262.htm

6、《全国人民代表大会常务委员会关于维护互联网安全的决定》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2000-12/29/c_133158942.htm

7、《互联网域名管理办法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2017-09/28/c_1121737753.htm

8、《网络安全审查办法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

9、《网络信息内容生态治理规定》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

10、《儿童个人信息网络保护规定》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

11、《互联网信息服务管理办法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2000-09/30/c_126193701.htm

12、《公共互联网网络安全威胁监测与处置办法》

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2017-09/14/c_1121660498.htm

13、《个人信息和重要数据出境安全评估办法》（征求意见稿）

来源：中共中央网络安全与信息化委员会办公室

http://www.cac.gov.cn/2017-04/11/c_1120785691.htm

14、《中华人民共和国个人信息保护法》（草案）

来源：中国人大网

<http://www.npc.gov.cn/flcaw/flca/ff80808175265dd401754405c03f154c/attachment.pdf>

15、《数据安全管理条例》（征求意见稿）

来源：中华人民共和国司法部网站

http://www.chinalaw.gov.cn/government_public/content/2019-05/28/657_235862.html

苏州大学数据资源与信息化建设管理处



天赐庄校区：东校区教育超市北



0512-65880000



its.suda.edu.cn

独墅湖校区：一期 304 号楼 5 楼

阳澄湖校区：行政楼 401