走进网络 贴近安全

——网络安全科普手册

目录/contents

工 作 篇

工作篇——办公环境

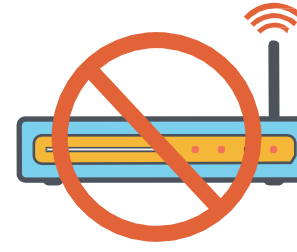
遵守办公场所的管理制度，非工作设备不要接入到办公网络。

1、非工作设备接入办公网络后，可以访问共享资源，如机密或重要文件等，一旦被恶意修改、拷贝、删除，会形成巨大损失；2、非工作设备可能携带病毒、木马等，接入局域网后传 播给内网的其他电脑，造成恶劣影响；3、非工作设备若下载文件或者在线游戏、在线视频等，挤占网速，影响正常工作秩序等。

工作篇——办公环境

不擅自增加网络设备及节点，如交换机、无线路由器等。

1、极易被非工作设备接入办公网络；2、若网络设备存在漏洞或者后门，极易被利用，从而形成内网入侵；3、无线网络设备若配置和管理不到位，会成为很大的风险点，容易被利用，例如近期刚曝出 WiFi KRACK 攻击。



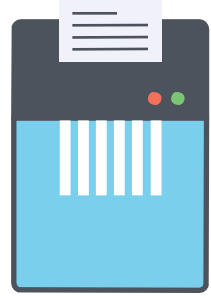
无线路由器

打印、传真完毕应立即取走文件。

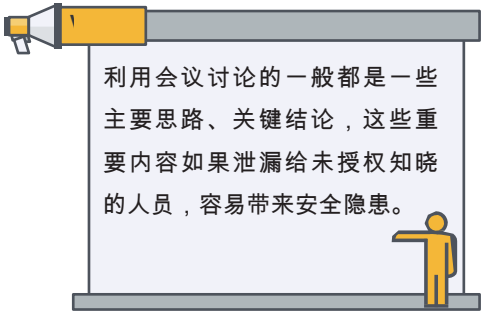
如果打印或传真的机密文件没有被及时取走，可能会造成机密信息泄漏，有着巨大的安全隐患。

工作篇——办公环境

纸质文件妥善保管，切忌随意放置或丢弃含有敏感信息的纸质文件，废弃文件用碎纸机粉碎。

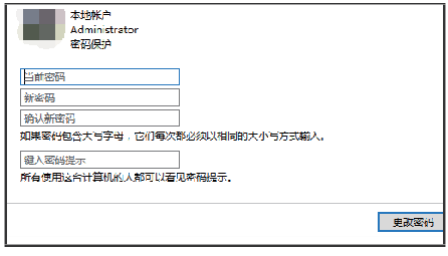


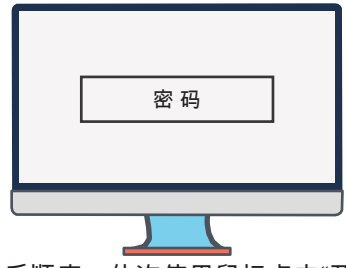
会议期间，禁止未授权的拍照、录音及录像，会后不要遗留重要文件，及时清理白板等。



工作篇——办公设备

电脑一定要设置开机密码。





Windows 系统密码设置方式： 按照先后顺序，依次使用鼠标点击“开始”菜单中的“控制面板”下的“用户 账户”，选择账户后点击“创建密码”，输入两遍密码后按“创建密码”按钮 即可。

打开操作系统的自动更新。

Windows 系统自动更新设置： 按照先后顺序，依次使用鼠标点击“开始”菜单中的“控制面板”下的“系统 和安全”，选择单击“Windows 更新”下的启用或关闭自动更新，在弹出的 更改设置对话框，选择重要更新下拉菜单中的“自动安装更新（推荐）”。

安装防火墙和防病毒软件，并定期升级 所安装的软件也应尽快升级到最新版本

工作篇——办公设备

编写程序不可能十全十美，所以软件也免不了会出现 BUG 或漏洞，而软件版本更新是专门用于修复这些 BUG 或漏洞的。因为原来发布的软件存在缺陷，发现之后通过 软件升级的方式使其完善，可以有效地防止非法入侵。

- 不要打开来历不明的网页、电子邮件链接或附件，不要随意接受陌生人的文件。
- 下载软件时尽量到官方网站或大型软件下载网站，在安装软件或打开来历不明的文件前先杀毒。

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瘫痪。

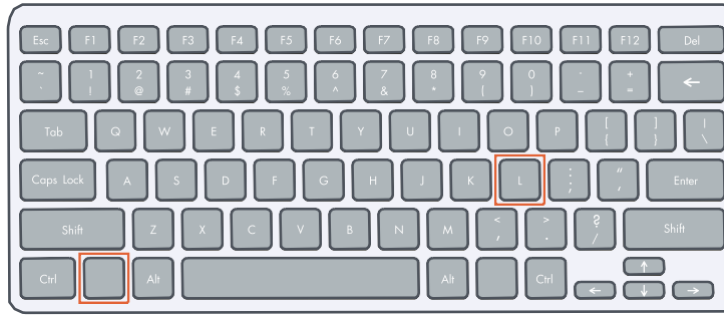
电脑插入移动存储设备时，如移动硬盘、U 盘等，首先进行病毒扫描。

工作篇——办公设备

移动存储设备也是信息存储介质，所存的信息很容易带有各种病毒，如果将带有病毒的移动存储设备接入电脑，很容易将病毒传播到电脑中。

临时离开电脑时，一定要将屏幕锁定，避免在离开期间电脑被 人恶意利用。

电脑锁屏操作： 首先设置系统密码，见前文“Windows 系统密码设置方式”。 当离开电脑前，同时按下键盘上的 Win 键 +L 键即可完成立刻锁屏 操作。（如下图）



当电脑、U 盘等办公设备损坏时，由单位管理员进行处 置，不要私自丢弃处理。

工作篇——文件数据

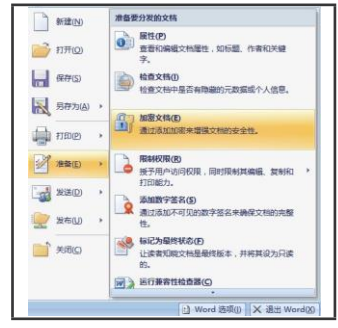
工作沟通工具建议使用钉钉，并强烈推荐使用第三方加密工具——密盾对聊天内容和文件传输进行加密。

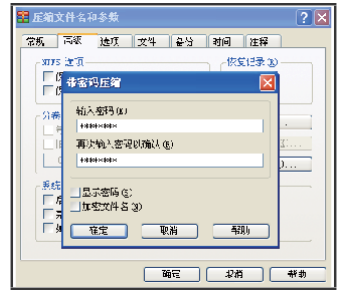
安全密盾

做好重要资料文件的备份，以备当文件遭到严重破坏时，能迅速修复数据，降低损失。对重要、敏感的文件进行加密，避免文件被直接利用。

1、office 文件加密：按照 先后顺序，依次使用鼠标 点击左上角 office 图标， 弹出菜单中的“准备”下 的“加密文档”，然后输 入密码即可。

2、压缩文件加密：右键点击要压缩加密的文件，选择“添加到压缩文件”，在“高级”标签页中勾选“设置密码”，然后输入密码开始压缩。





电脑中的文件可用加密软件进行加密，例如 Windows 系统自带的 BitLocker 或者开源软件 TrueCrypt 等。

工作篇——文件数据

Windows BitLocker 设置： 按照先后顺序，依次使用鼠标点击“开始”菜单中的“控制面 板”下的“BitLocker 驱动器加密”，选择需要加密的数据盘，在 弹出的设置对话框中，勾选“使用密码解锁驱动器”，输入密码 后等待系统完成加密即可。（如下图）

普通文件删除，记得清空回收站。 敏感文件删除，可以使用安全删除软件进行数据擦除， 如“文件粉碎机”等，若没有安全删除软件时，可采用 数据反复覆盖的方式，避免敏感文件被恢复。

1、U 盘、移动硬盘删除数据：反复往 U 盘、移动硬盘中拷 贝和删除非敏感文件。 2、数码相机删除数据：在删除隐私照片之后继续多拍几 张照片来覆盖数据。

工作篇——账号密码

不要将账号密码写在纸上，并贴到显眼位置。

账号备忘录

账户平台	账户名	邮箱	密码
~~百度~~	~~anheng~~	~~anhengxinxi@XX.com~~	~~123456~~
~~腾讯~~	~~anheng~~	~~anhengxinxi@XX.com~~	~~123456~~
~~网易~~	~~anheng~~	~~anhengxinxi@XX.com~~	~~123456~~
~~阿里~~	~~anheng~~	~~anhengxinxi@XX.com~~	~~123456~~

不同平台使用不同的密码，且设置得尽量复杂。

1、组合法：使用方便记忆的组合方式编排密码。例如用单位名称、单位地址、平台缩写、时间等等，中间穿插特殊字符的方式进行组合。

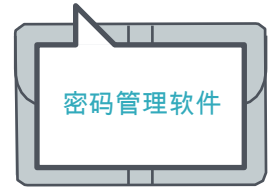
2、短语法：找到一个生僻但易记的短语或句子（可以摘自歌曲、书本或电影），然后创建它的缩写形式，其中包括大写字母和标点符号等。

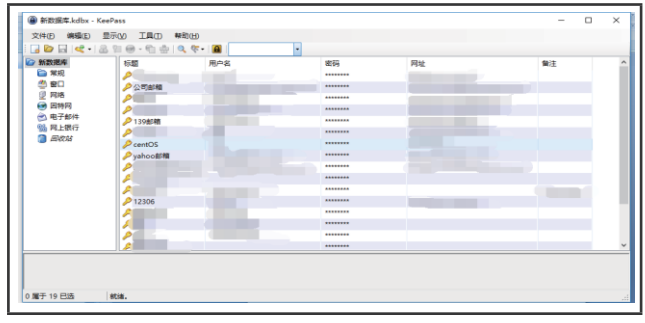
3、替换法：用数字或符号来替换选定的字母，从而提高密码的复杂性。

4、键盘法：使用 Z 字型或者多条短线连接键盘上的字符，并结合数字和特殊字符形成密码。

工作篇——账号密码

可以使用密码管理软件进行账号密码管理，如 keepass、1password 等。





不要使用“记住密码”和“自动登录”功能。

生 活 篇

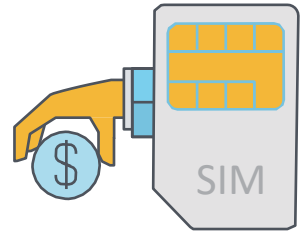
生活篇——移动设备

移动设备下载应用软件，尽量去系统自带的官方应用商店或应 用的官方网站下载，安装应用时，谨慎授予应用所需的权限。

1、目前手机、平板电脑的 APP 应 用市场多如牛毛，各市场对上架的 APP 审核力度不一，且一些对安 全性重视不够的应用市场容易被黑 客入侵，导致正常的 APP 被替换 为恶意 APP。 2、应用经常会向用户索要超出其 功能范围之外的权限，若全部授权，会带来隐私泄露的风险。

SIM 卡设置 PIN 码，当手机重启或更换手机后必须输入 PIN 码 才能正常使用这个号码。

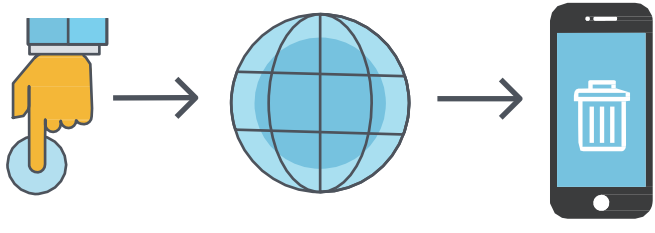
手机丢失后，如果不及时挂失 SIM 卡，可轻易将 SIM 卡换到另一部手 机里收取验证信息，通常只需要证 件号码、银行卡和短信验证，就可 以注册银行快捷支付，不法分子很 容易盗取银行卡内的资金。



生活篇——移动设备

手机或 SD 卡上不要存储敏感信息，如身份证照片、银行卡照片、工作文档等。

安装防盗软件，一旦丢失，可以通过远程指令，清空手机内的文件和数据。



手机丢失后，应立即做的事情：

1、挂失手机号码；
2、致电冻结银行网银；
3、挂失支付帐号，重置支付密码；
4、尽快更改重要 APP 密码。

生活篇——社交账号

开通实名认证，并绑定手机号： 不同社交账号设置不同密码，尽量由大小写字母、数字和其他字 符混合组成，并定期修改密码，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。有多重验证登录保护的 平台，尽量开启登录保护。

1、我国法律法规要求实名制上网，若不进行实名认证，社交网络服务的功能会受到相应限制。
2、实名之后，若社交网络账号被盗，找回过程会相对容易。

在公共电脑或公共设备上登录社交账号时，警惕输入账号密码时被人偷看；为防账号被病毒、木马的键盘记录，可先输入部分账户名和部分密码，然后再输入剩下的账户名和密码。

不要轻易相信社交网络上传言，任何消息都以权威发布为准，做到不信谣，不传谣。

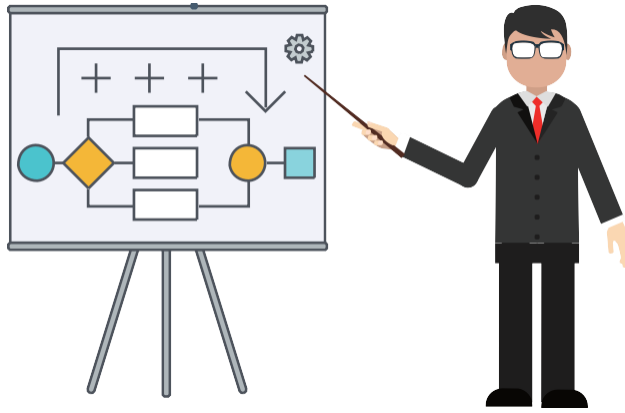
当收到与个人信息和金钱相关（如中奖、集资等）的信息时要提高警 惕。

生活篇——网络交易

网络交易的威胁主要表现在三个方面。

一、钓鱼网站： 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。

二、病毒木马： 病毒、木马等恶意代码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。



生活篇——网络交易

三、密码破解： 很多人使用的密码都是“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。

1、核实网站真伪，尽量到知名、权威的网站购物，仔细甄别，严加防范。

2、尽量选择比较安全的第三方支付平台担保交易，切忌直接与卖家私下交易。

3、注意商家的信誉、评价和联系方式。

4、不贪小便宜，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。

5、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。

6、使用移动支付时，最好绑定II类或III类的小额银行账户，以防账户被盗带来较大的资金损失。

7、删除有绑定银行卡的 APP 时，谨记先解绑银行卡。

生活篇——预防诈骗

网络诈骗手段等多种多样，已经成为一条完整的违法产业链，网络诈骗的不法分子结成团伙作案，各环节互不认识但分工协作、勾联紧密的利益链条。

骗术大揭秘之一：身份冒充

1、冒充公检法工作人员拨打电话，以身份信息被盗用、涉嫌洗钱、贩毒等理由，要求将钱转入到“安全账户”配合调查。

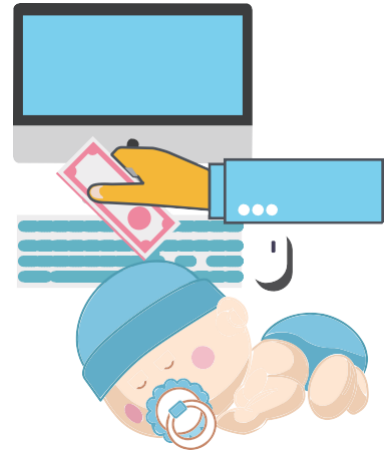
2、冒充公司领导，发出要求快速转帐汇款的指令等。

骗术大揭秘之二：金钱诱惑

1、重金求子，引诱上当后，以检查费、诚意金等理由行骗。

2、高薪招聘，要求到指定地点面试，随后要求交培训费、服装费，甚至陷入传销团伙。

3、网络兼职，以打字员、刷单员为名义，要求缴纳信息费等。



生活篇——预防诈骗

骗术大揭秘之三：有奖活动

1、发布集赞、转发有奖等虚假活动，要求提供姓名、电话、地址等信息，套取足够信息后要求缴纳保证金、个人所得税、快递费等。

2、以热播栏目节目组的名义发短信，称被选为幸运观众，有巨额奖品，后以个人所得税、快递费等借口要求转账汇款。

骗术大揭秘之四：消费退款

1、以系统卡单、故障、无货等理由，发来退款网址，此退款网 址是钓鱼网站，若按要求填入信息，则支付宝、银行卡的钱会被 快速转走。

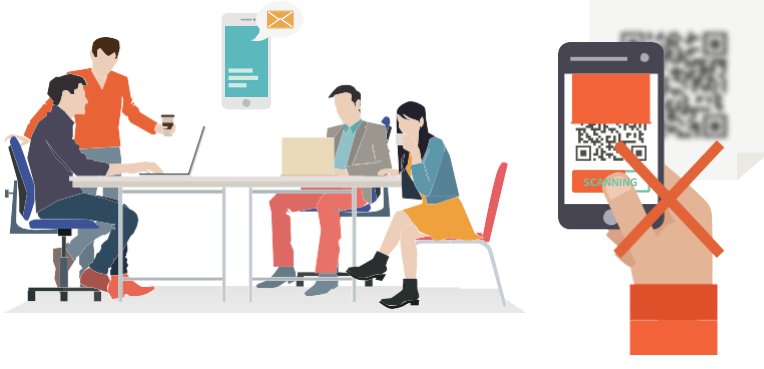
2、群发假冒银行卡消费短信，后以境外大额消费涉嫌洗钱为由，套取个人信息及银行卡信息，通过第三方支付的快捷支付进行消费。

3、以机票改签等，诱骗进行汇款操作。

生活篇——预防诈骗

骗术大揭秘之五：恶意代码

1、利用伪基站群发网银系统升级、积分兑换等虚假链接，一旦点击后，手机便被植入盗取银行账号、密码、短信验证码的木马，从而实施犯罪。 2、以互联网公司的名义群发短信，包含钓鱼网站链接，进而获 取账号密码等信息，转走账号中的资金。



骗术大揭秘之六：其他骗术

1、在公共场所设置与正规 WiFi 类似的山寨免密 WiFi，一旦连接 上，通过截取数据传输，轻松获取手机上各类 App 的账号密码以 及隐私。 2、骗子用受害者临时身份证办理补卡，同时用骚扰软件打电话 发短信轰炸受害者手机，以掩盖补卡业务提醒短信。然后用补办 的手机卡登录网银、第三方支付等平台，获取验证码盗取账户。 3、发布信用卡提额、低息贷款等广告，然后以验资、中介、手 续费等名义要求转账。 4、发布虚假色情服务广告，待有人联系后，称需要先付款保证 人身安全才能提供服务。

生活篇——预防诈骗

网络防骗“十”凡是

1、凡是自称公安机关、检察院、法院等单位要求汇款的；
2、凡是要求汇款到“安全账户”的；
3、凡是通知中奖、积分兑换要先交钱的；
4、凡是通知“亲朋好友”出急事要求汇款的；
5、凡是索要个人和银行卡信息及短信验证码的；
6、凡是说招聘又轻松、又高薪、还日结工作的；
7、凡是要求开通网银远程协助接受检查的；
8、凡是通知网购系统、订单错误需要进行操作的；
9、凡是自称领导要求突然汇款的；
10、凡是陌生网站要求输入银行卡信息的。

网络防骗“五”不要

1、不要轻信：中奖、红包、违法、洗钱等；
2、不要回拨：陌生信息提供的联系方式，不要致电联系；
3、不要点击：免费领奖、红包链接、视频相册等陌生链接统统不点；
4、不要透露：手机号、身份证号、银行卡号等一切隐私信息；
5、不要转账：不经核实的情况统统不要转账。

网络防骗“两”核实

1、核实可疑信息陌生可疑的短信、电话、QQ、微信、邮件、通知等等，只要拿不准情 况，都通过官方渠道进行核实；

2、核实转账请求他人要求借钱、打款、线上支付、充值等等，所有金钱往来，一定要当面 或电话联系到本人进行确认。

生活篇——个人信息

个人信息： 个人信息一般包括姓名、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，会对个人造成不良影响的 个人信息。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。

生活篇——个人信息

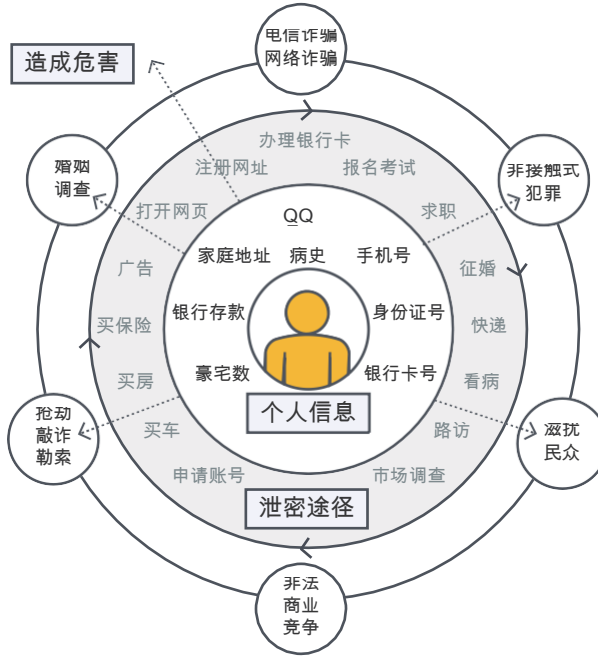
个人信息如何泄露的？ 1、正常的社会活动被泄露，如旅馆住宿、保险公司投保、租赁 公司、银行办证、电信、移动、联通、房地产、邮政部门等需要 身份证件实名登记的部门、场所，个别人员利用登记的便利条 件，收集客户个人信息，汇集成册，并按照一定的价格出售给需 要购买的人；2、利用各种活动引诱填写个人信息，如填写详细联系方式、 收 入情况、 信用卡情况等内容就能参加抽奖活动，可以获得不等奖 次的奖品；3、一些互联网公司由于安全防范措施不到位，其用户的个人信息被黑客窃取等。

个人信息能用来干什么？ 1、电信诈骗、网络诈骗等新型、非接触式犯罪。 如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， 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。 如以信息咨询、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。 如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。

5、滋扰民众。 通过网络人肉搜索、信息曝光等行为滋扰民众生活。

生活篇——个人信息



泄密原因

个人：疏忽管理，过量提供，随意丢弃 企业：贩卖牟利，随意保存，内部员工非法泄密，超授权使用，未及时销毁 犯罪份子：黑客攻击，恶意电话和短信，网站钓鱼，病毒和木马，社会工程 攻击

如何防范个人信息泄露？1、培养安全意识，做到不主动透露个人信息，不被利益诱惑泄 露个人信息；2、养成安全习惯，如密码设置、软件及时更新、软件授权、数 据备份、不随意连接 WiFi、勿见二维码码就刷等；3、善用法律维权，当发现个人信息泄露的确凿证据时，积极向 监管单位进行举报。

法律篇

法律篇——网络安全法

网络不是法外之地，有哪些需要了解的法律知识呢？

一、网上何种行为会被认定为寻衅滋事罪？ 利用信息网络辱骂、恐吓他人，情节恶劣、破坏社会秩序的，依 照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪 定罪处罚。 编造虚假信息，或者明知是编造的虚假信息，在信息网络上散 布，或者组织、指使人员在信息网络上散布， 起哄闹事， 造成公 共秩序严重混乱的，依照刑法第二百九十三条第一款第(四)项的 规定， 以寻衅滋事罪定罪处罚。

二、网上何种行为会被认定为敲诈勒索罪？ 以在信息网络上发布、删除等方式处理网络信息为由，威胁、要 挟他人，索取公私财物，数额较大，或者多次实施上述行为的， 依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

法律篇——网络安全法

三、网上的哪些行为会被认定为捏造事实诽谤他人？ 根据《刑法》第二百四十六条第一款规定，以下情况会被认定为 捏造事实诽谤他人： 1.捏造损害他人名誉的事实，在信息网络上散布，或者组织、指 使人员在信息网络上散布的； 2.将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的 事实，在信息网络上散布，或者组织、指使人员在信息网络上散 布的；

3.明知是捏造的损害他人名誉的事实， 在信息网络上散布， 情节 恶劣的，以“捏造事实诽谤他人”论。

情节严重的包括：

1. 同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的； 2.造成被害人或者其近亲属精神失常、自残、自杀等严重后果 的；

3. 两年内曾因诽谤受过行政处罚，又诽谤他人的；

4. 其他情节严重的情形。

严重危害社会秩序和国家利益的包括：

1. 引发群体性事件的；
2. 引发公共秩序混乱的；
3. 引发民族、宗教冲突的；
4. 诽谤多人，造成恶劣社会影响的；
5. 损害国家形象，严重危害国家利益的；
6. 造成恶劣国际影响的；
7. 其他严重危害社会秩序和国家利益的情形。

法律篇——网络安全法

四、网上何种行为会被认定为非法经营罪？ 违反国家规定，以营利为目的，通过信息网络有偿提供删除信息 服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等 服务，扰乱市场秩序，属于非法经营行为“情节严重”，依照刑 法第二百二十五条第(四)项的规定，以非法经营罪定罪处罚。

五、明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，会构成什么性质的犯罪？

以共同犯罪论处。

六、关于即时通信工具（如微信、腾讯 QQ 等）的公众信息服务有哪些管理规定？ 国家互联网信息办公室 2014 年 8 月 7 日发布《即时通信工具公众

信息服务发展管理暂行规定》，其中有以下几条： 第六条：即时通信工具服务提供者应当按照“后台实名、前台自 愿”的原则，要求即时通信工具服务使用者通过真实身份信息认 证后注册账号。即时通信工具服务使用者注册账号时，应当与即 时通信工具服务提供者签订协议，承诺遵守法律法规、社会主义 制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信 息真实性等“七条底线”。 第八条：即时通信工具服务使用者从事公众信息服务活动，应当 遵守相关法律法规。对违反协议约定的即时通信工具服务使用 者，即时通信工具服务提供者应当视情节采取警示、限制发布、 暂停更新直至关闭账号等措施，并保存有关记录，履行向有关主 管部门报告义务。