共建网络安全 共享网络文明

国家网络安全宣传周
China Cybersecurity Week

网络安全知识手册

网络安全知识手册编写组

2014年11月

CONTENTS 目录

一. 计算机安全

二. 上网安全

三 . 移动终端安全

四 . 个人信息安全

五 . 法律知识

六 . 安全事件处置


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. 安装防火墙和防病毒软件，并经常升级；
2. 注意经常给系统打补丁，堵塞软件漏洞；
3. 不要上一些不太了解的网站，不要执行从网上下载后未经杀毒处理的软件，不要打开 MSN 或者 QQ 上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 如何设置 windows 操作系统开机密码

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。

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. 利用病毒防护软件对所有下载资源及时进行恶意代码扫描。

五 为什么要定期进行补丁升级

编写程序不可能十全十美，所以软件也免不了会出现 BUG，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，升级到最新的安全补丁，可以有效地防止非法入侵。

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 计算机日常使用中遇到的异常情况有哪些

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、可执行程序文件大小改变等异常现象。

十 Cookies 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 GET 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；
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. 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，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。

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. 适当设置找回密码的提示问题；
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

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。

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。

十 如何保护网上炒股安全

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。

保护网上炒股安全，应采取如下措施：

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。

十二 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。

十二 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。

十三 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。

十四 如何准确访问和识别党政机关、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。

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。

网站标识分为党政机关和事业单位两类。

十七 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“95516”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。

十八 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。

十九 当公民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

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。网络安全事件处置相关机构联系方式，参见第六部分“安全事件处置”。


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。

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；

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。

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

今年以来出现了一种利用“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。

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. 出差之前备份好宝贵数据；
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；二是用户信息安全意识不足，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。

手机支付毕竟是一个新事物，尤其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. 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，装订成册，对外出售；
4. 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；
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。

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，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。如 2011 年，北京发生一起案件，由于分手后发生口角，闫某前男友将其个人私密照片在网上曝光，给闫某造成极大困扰。

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。

（一）违反《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》的单位或者个人会被给予什么处罚

对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布。构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任。

（二）网上的哪些行为会被认定为《刑法》第二百四十六条第一款规定的“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。

（三）利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第一款规定的“情节严重”

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。

（四）利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第二款规定的“严重危害社会秩序和国家利益”

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。

（五）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。

（六）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。

（七）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。

（八）非法经营认定的数额标准是多少

1. 个人非法经营数额在五万元以上，或者违法所得数额在两万元以上的；

2. 单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

（九）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。

（十）国家对经营性和非经营性互联网信息服务分别采取什么管理制度

国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。

未取得许可或者未履行备案手续的，不得从事互联网信息服务。

（十一）互联网新闻信息及新闻信息服务包括哪些

新闻信息是指时政类新闻信息，包括有关政治、经济、军事、外交等社会公共事务的报道、评论，以及有关社会突发事件的报道、评论。互联网新闻信息服务包括通过互联网登载新闻信息、提供时政类电子公告服务和向公众发送时政类通讯信息。

（十二）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》，就上述问题作出如下规定：

第二条 在中华人民共和国境内从事即时通信工具公众信息服务，适用本规定。

本规定所称即时通信工具，是指基于互联网面向终端使用者提供即时信息交流服务的应用。本规定所称公众信息服务，是指通过即时通信工具的公众账号及其他形式向公众发布信息的活动。

第三条 国家互联网信息办公室负责统筹协调指导即时通信工具公众信息服务发展管理工作，省级互联网信息内容主管部门负责本行政区域的相关工作。

互联网行业组织应当积极发挥作用，加强行业自律，推动行业信用评价体系建设，促进行业健康有序发展。

第四条 即时通信工具服务提供者应当取得法律法规规定的相关资质。即时通信工具服务提供者从事公众信息服务活动，应当取得互联网新闻信息服务资质。

第五条 即时通信工具服务提供者应当落实安全管理责任，建立健全各项制度，配备与服务规模相适应的专业人员，保护用户信息及公民个人隐私，自觉接受社会监督，及时处理公众举报的违法和不良信息。

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”。

第七条 即时通信工具服务使用者为从事公众信息服务活动开设公众账号，应当经即时通信工具服务提供者审核，由即时通信工具服务提供者向互联网信息内容主管部门分类备案。

新闻单位、新闻网站开设的公众账号可以发布、转载时政类新闻，取得互联网新闻信息服务资质的非新闻单位开设的公众账号可以转载时政类新闻。其他公众账号未经批准不得发布、转载时政类新闻。

即时通信工具服务提供者应当对可以发布或转载时政类新闻的公众账号加注标识。

鼓励各级党政机关、企事业单位和各人民团体开设公众账号，服务经济社会发展，满足公众需求。

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。

（十三）现行《刑法》中，专门规定了哪两个关于计算机犯罪的罪名

第二百八十五条【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

（十四）利用计算机或计算机网络实施的犯罪行为在《刑法》中如何定罪

利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。该条规定的犯罪侵害客体比较广泛，包括公司财产或国家秘密的拥有权等。

（十五）禁止从事哪些危害计算机信息网络安全的活动

《计算机信息网络国际联网安全保护管理办法》第六条规定，任何单位和个人不得从事下列危害计算机信息网络安全的活动：（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；（四）故意制作、传播计算机病毒等破坏性程序的；（五）其他危害计算机信息网络安全的。

（十六）利用信息网络侵害人身权益案件适用哪些法律规定

2014 年 6 月 23 日最高人民法院审判委员会第 1621 次会议通过了《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》，就上述问题明确作出如下规定：

第二条 利用信息网络侵害人身权益提起的诉讼，由侵权行为地或者被告住所地人民法院管辖。

侵权行为实施地包括实施被诉侵权行为的计算机等终端设备所在地，侵权结果发生地包括被侵权人住所地。

第三条 原告依据侵权责任法第三十六条第二款、第三款的规定起诉网络用户或者网络服务提供者的，人民法院应予受理。

原告仅起诉网络用户，网络用户请求追加涉嫌侵权的网络服务提供者为共同被告或者第三人的，人民法院应予准许。

原告仅起诉网络服务提供者，网络服务提供者请求追加可以确定的网络用户为共同被告或者第三人的，人民法院应予准许。

第四条 原告起诉网络服务提供者，网络服务提供者以涉嫌侵权的信息系网络用户发布为由抗辩的，人民法院可以根据原告的请求及案件的具体情况，责令网络服务提供者向人民法院提供能够确定涉嫌侵权的网络用户的姓名（名称）、联系方式、网络地址等信息。

网络服务提供者无正当理由拒不提供的，人民法院可以依据民事诉讼法第一百一十四条的规定对网络服务提供者采取处罚等措施。

原告根据网络服务提供者提供的信息请求追加网络用户为被告的，人民法院应予准许。

第五条 依据侵权责任法第三十六条第二款的规定，被侵权人以书面形式或者网络服务提供者公示的方式向网络服务提供者发出的通知，包含下

列内容的，人民法院应当认定有效：

（一）通知人的姓名（名称）和联系方式；

（二）要求采取必要措施的网络地址或者足以准确定位侵权内容的相关信息；

（三）通知人要求删除相关信息的理由。

被侵权人发送的通知未满足上述条件，网络服务提供者主张免除责任的，人民法院应予支持。

第六条 人民法院适用侵权责任法第三十六条第二款的规定，认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据网络服务的性质、有效通知的形式和准确程度，网络信息侵害权益的类型和程度等因素综合判断。

第七条 其发布的信息被采取删除、屏蔽、断开链接等措施的网络用户，主张网络服务提供者承担违约责任或者侵权责任，网络服务提供者以收到通知为由抗辩的，人民法院应予支持。

被采取删除、屏蔽、断开链接等措施的网络用户，请求网络服务提供者提供通知内容的，人民法院应予支持。

第八条 因通知人的通知导致网络服务提供者错误采取删除、屏蔽、断开链接等措施，被采取措施的网络用户请求通知人承担侵权责任的，人民法院应予支持。

被错误采取措施的网络用户请求网络服务提供者采取相应恢复措施的，人民法院应予支持，但受技术条件限制无法恢复的除外。

第九条 人民法院依据侵权责任法第三十六条第三款认定网络服务提供者是否“知道”，应当综合考虑下列因素：

（一）网络服务提供者是否以人工或者自动方式对侵权网络信息以推荐、排名、选择、编辑、整理、修改等方式作出处理；

（二）网络服务提供者应当具备的管理信息的能力，以及所提供服务的性质、方式及其引发侵权的可能性大小；

（三）该网络信息侵害人身权益的类型及明显程度；

（四）该网络信息的社会影响程度或者一定时间内的浏览量；

（五）网络服务提供者采取预防侵权措施的技术可能性及其是否采取了相应的合理措施；

（六）网络服务提供者是否针对同一网络用户的重复侵权行为或者同一侵权信息采取了相应的合理措施；

（七）与本案相关的其他因素。

第十条 人民法院认定网络用户或者网络服务提供者转载网络信息行为的过错及其程度，应当综合以下因素：

（一）转载主体所承担的与其性质、影响范围相适应的注意义务；

（二）所转载信息侵害他人人身权益的明显程度；

（三）对所转载信息是否作出实质性修改，是否添加或者修改文章标题，导致其与内容严重不符以及误导公众的可能性。

第十一条 网络用户或者网络服务提供者采取诽谤、诋毁等手段，损害公众对经营主体的信赖，降低其产品或者服务的社会评价，经营主体请求网络用户或者网络服务提供者承担侵权责任的，人民法院应依法予以支持。

第十二条 网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。但下列情形除外：

（一）经自然人书面同意且在约定范围内公开；

（二）为促进社会公共利益且在必要范围内；

（三）学校、科研机构等基于公共利益为学术研究或者统计的目的，经自然人书面同意，且公开的方式不足以识别特定自然人；

（四）自然人自行在网络上公开的信息或者其他已合法公开的个人信息；

（五）以合法渠道获取的个人信息；

（六）法律或者行政法规另有规定。

网络用户或者网络服务提供者以违反社会公共利益、社会公德的方式公开前款第四项、第五项规定的个人信息，或者公开该信息侵害权利人值得保护的重大利益，权利人请求网络用户或者网络服务提供者承担侵权责任的，人民法院应予支持。

国家机关行使职权公开个人信息的，不适用本条规定。

第十三条 网络用户或者网络服务提供者，根据国家机关依职权制作的文书和公开实施的职权行为等信息来源所发布的信息，有下列情形之一、侵害他人人身权益、被侵权人请求侵权人承担侵权责任的，人民法院应予支持：

（一）网络用户或者网络服务提供者发布的信息与前述信息来源内容不符；

（二）网络用户或者网络服务提供者以添加侮辱性内容、诽谤性信息、

不当标题，或者通过增删信息、调整结构、改变顺序等方式致人误解；

（三）前述信息来源已被公开更正，但网络用户拒绝更正或者网络服务提供者不予更正；

（四）前述信息来源已被公开更正，网络用户或者网络服务提供者仍然发布更正之前的信息。

第十四条 被侵权人与构成侵权的网络用户或者网络服务提供者达成一方支付报酬，另一方提供删除、屏蔽、断开链接等服务的协议，人民法院应认定为无效。

擅自篡改、删除、屏蔽特定网络信息或者以断开链接的方式阻止他人获取网络信息，发布该信息的网络用户或者网络服务提供者请求侵权人承担侵权责任的，人民法院应予支持。接受他人委托实施该行为的，委托人与受托人承担连带责任。

第十五条 雇佣、组织、教唆或者帮助他人发布、转发网络信息侵害他人人身权益，被侵权人请求行为人承担连带责任的，人民法院应予支持。

第十六条 人民法院判决侵权人承担赔礼道歉、消除影响或者恢复名誉等责任形式的，应当与侵权的具体方式和所造成的影响范围相当。侵权人拒不履行的，人民法院可以采取在网络上发布公告或者公布裁判文书等合理的方式执行，由此产生的费用由侵权人承担。

第十七条 网络用户或者网络服务提供者侵害他人人身权益，造成财产损失或者严重精神损害，被侵权人依据侵权责任法第二十条和第二十二条的规定请求其承担赔偿责任的，人民法院应予支持。

第十八条 被侵权人为制止侵权行为所支付的合理开支，可以认定为侵权责任法第二十条规定的财产损失。合理开支包括被侵权人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情，可以将符合国家有关部门规定的律师费用计算在赔偿范围内。

被侵权人因人身权益受侵害造成的财产损失或者侵权人因此获得的利益无法确定的，人民法院可以根据具体案情在 50 万元以下的范围内确定赔偿数额。

精神损害的赔偿数额，依据《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》第十条的规定予以确定。

可以向哪些专业机构求援

类别	机构名称	网址
服务机构	国家互联网应急中心	http://www.cert.org.cn/
	国家计算机病毒应急处理中心	http://www.antivirus-china.org.cn/
	中国信息安全测评中心	http://www.itsec.gov.cn/
	中国国家信息安全漏洞库	http://www.cnnvd.org.cn/
违法和不良信息举报	中国互联网违法和不良信息举报中心	http://net.china.com.cn/
	中国互联网协会反垃圾信息中心	http://www.12321.org.cn/
	网络违法犯罪举报网站	http://www.cyberpolice.cn/wfjb/
	网络不良与垃圾信息举报受理中心	http://www.12321.cn/
	UNT 统一信任网络	http://www.trustutn.org/
	网络社会诚信网	http://www.zx110.org/

特别鸣谢

中央编办电子政务中心
上海市经济和信息化委员会
黑龙江省工业和信息化委员会
新华网
国家网络安全宣传周专家评审委员会
工业和信息化部电子科学技术情报研究所