

网络安全

科

普

资

料

内江师范学院共青团

## 网络安全的通用定义:

网络安全是指保护网络系统中的软件、硬件及信息资源,使之免受偶然或恶意的破坏篡改和泄露,保证网络系统的正常运行、网络服务不中断。

## 网络安全现状：

随着[计算机技术](http://baike.so.com/doc/1312255.html)的飞速发展，信息网络已经成为社会发展的重要保证。有很多是敏感信息，甚至是国家机密。所以难免会吸引来自世界各地的各种人为攻击（例如信息泄漏、信息窃取、数据篡改、数据删添、[计算机病毒](http://baike.so.com/doc/336385.html)等）。同时，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

## 网络不安全的主要因素：

### 1、计算机病毒

在计算机网络中，由于要尽可能的实现资源共享，所以接收信息的结点一般有多个。由于没有办法保证每个结点的安全性，所以极易感染计算机病毒。而病毒一旦侵入计算机，后果将不堪设想。病毒会在网络内以极快的速度进行再生和传染，很多波及到整个网络，使得各个网络阶段都受到感染。如果没有很好的应急措施，那么在短时间内就会造成网络的瘫痪。如近几年的“冲击波”、“震荡波”、“熊猫烧香”给我们的正常工作已经造成过严重威胁。
2、人为的无意失误

网络系统要正常运行，就需要专门的管理人员对网络系统进行管理。那么，在管理的过程中，出现一些不当措施的情况，也是时有发生的。一旦系统管理人员操作不当，就会使得网络管理出现漏洞，有时会造成设备的损坏，保密信息在这个过程中很有可能遭到人为泄露。这种情况在现实中还是并不少见的，而这些失误大多都是人为因素造成的。
3、人为的恶意攻击

这是计算机网络所面临的最大威胁，以各种方式有选择地破坏信息的有效性和完整性。还有就是网络侦查，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。
4、网络软件的缺陷和漏洞

网络软件不可能是百分之百的无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。
5、物理安全问题

物理安全是指在物理介质层次上对存贮和传输的信息安全保护。如通信光缆、电缆、电话线、局域网等有可能遭到破坏，引起计算机网络的瘫痪。

## 2016年最新网络骗局：

### 案例一：远程协助——骗!

　　案例介绍：今年6月14日，陈某在一家淘宝网店购买一台42寸标价2003元的电视机，但因操作失误多付了2003元。因退款心切，在客服的要求下，陈某加了对方QQ，让对方远程操控自己的电脑“帮助退款”，结果被对方分7次转走6万余元。

　　提示：千万不要让陌生人远程操作你的电脑。因为一旦启动远程操控，任何人都可以在异地通过网络控制你的电脑。另外，淘宝交易需要加QQ沟通的，往往是诈骗。

### 案例二：“支付宝”发邮件称需升级?——骗!

案例介绍：小美在淘宝开了一家汽车用品店。今年2月底，一个“买家”来店里拍了一套汽车坐垫后发了一张截图，显示“本次支付失败”，并提示“由于卖家账号异常，已发邮件给卖家”。

　　小美打开邮箱，果然有一封主题为“来自支付宝的安全提醒”的未读邮件。小美没有多想就点击邮件里的链接，按提示一步步进行了“升级”，期间几次输入支付宝账号和密码。隔天，小美发现账户里的8000多元余额被人以支付红包的形式盗空。

　　提示：要警惕收到的陌生邮件、文档、链接，不要轻易点击，防止木马病毒。如遇疑难问题，一定要找官方客服了解咨询，或拨打110求助。

### 案例十：QQ上谈钱——骗!

案例介绍：今年1月，小飞在家上网时，QQ上一个同学发来信息，说朋友要还自己钱，但自己卡掉了，想先把钱转小飞卡上，然后再由小飞转给他。小飞答应了，对方又说汇钱需要银行卡号、身份证及联系电话，小飞又全部告诉了对方。过了几分钟，小飞手机收到一个验证码，对方称只要告诉他这个验证码，钱就能到账了，小飞没细想就告诉了他。直到收到银行短信通知，小飞才发现自己卡里被消费了2200元。

提示：无论是给你打钱还是向你借钱，如在网上提出钱财交易请求，即便有视频画面也不要轻信，务必先打电话确认;同时要牢记，手机上收到的验证码，千万不能随意泄漏。

## 网络安全防范与常识

### 1、电子邮件欺诈

广大网民如收到有如下特点的邮件就要提高警惕，不要轻易打 开和听信：(一)是伪造发件人信息；(二)是问候语或开场白往往模仿被假冒单位的口吻和语气，如“亲爱的用户”；(三)是邮件内容多为传递紧迫的信息，如以帐户状态将影响到正常使用或宣称正在通过网站更新帐号资料信息等；(四)是索取个人信息，要求用户提供密码、帐号等信息。还有一类邮件是以超低价或海关查没品等为诱饵诱骗消费者。

### 2、防范“假冒的银行”

由于侵入银行系统难度较大，不法分子将黑手直接伸向网银用户。通常，不法分子通过“网络钓鱼方式，通过邮件发布虚假信息，骗取客户银行卡卡号、密码，窃取客户资金。因此，我们要有一定的防范意识和良好的习惯，避免上当受骗。 一是核对网址，看是否与真正网址一致； 二是选妥和保管好密码，不要选诸如身份证号码、出生日期、电话号码等作为密码，建议用字母、数字混合密码，尽量避免在不同系统使用同一密码； 三是做好交易记录，对网上银行、网上证券等平台办理的转账和支付等业务做好记录，定期查看“历史交易明细”和打印业务对账单，如发现异常交易或差错，立即与有关单位联系； 四是管好数字证书，避免在公用的计算机上使用网上交易系统； 五是对异常动态提高警惕，如不小心在陌生的网址上输入了账户和密码，并遇到类似“系统维护”之类提示时，应立即拨打有关客服热线进行确认，万一资料被盗，应立即修改相关交易密码或进行银行卡、证券交易卡挂失； 六是通过正确的程序登录支付网关，通过正式公布的网站进入，不要通过搜索引擎找到的网址或其他不明网站的链接进入。

### 3、虚假电子商务信息的情况

广大网民应掌握以下诈骗信息特点，不要上当： 一是虚假购物、拍卖网站看上去都比较“正规”，有公司名称、地址、联系电话、联系人、电子邮箱等，有的还留有互联网信息服务备案编号和信用资质等； 二是交易方式单一，消费者只能通过银行汇款的方式购买，且收款人均为个人，而非公司，订货方法一律采用先付款后发货的方式； 三是诈取消费者款项的手法如出一辙，当消费者汇出第一笔款后，骗子会来电以各种理由要求汇款人再汇余款、风险金、押金或税款之类的费用，否则不会发货，也不退款，一些消费者迫于第一笔款已汇出，抱着侥幸心理继续再汇； 四是在进行网络交易前，要对交易网站和交易对方的资质进行全面了解。

### 四、其他网络安全防范措施：

一是安装防火墙和防病毒软件，并经常升级； 二是注意经常给系统打补丁，堵塞软件漏洞； 三是禁止浏览器运行JavaScript和ActiveX代码； 四是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； 五是提高自我保护意识，注意妥善保管自己的私人信息，如本人证件号码、帐号、密码等，不向他人透露；尽量避免在网吧等公共场所使用网上电子商务服务。

## 如何专业维护网络安全：

1、基础设施管理
（1）确保网络通信传输畅通及配线的合理有序；
（2）掌控主干设备的配置情况及配置参数变更情况，备份各个设备的配置文档；
（3）[实时监控](https://www.baidu.com/s?wd=%E5%AE%9E%E6%97%B6%E7%9B%91%E6%8E%A7&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLPvcsuyfzPjuWPAR3n1610ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWmvP1cLnHD3)整个局域网的运转和网络通信流量情况，发现问题后和有关机构及时联系，定制、发布网络基础设施使用管理办法并监督执行情况。
2、[操作系统](https://www.baidu.com/s?wd=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLPvcsuyfzPjuWPAR3n1610ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWmvP1cLnHD3)管理
（1）在网络[操作系统](https://www.baidu.com/s?wd=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLPvcsuyfzPjuWPAR3n1610ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWmvP1cLnHD3)配置完成并投入正常运行后，[网络管理员](https://www.baidu.com/s?wd=%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLPvcsuyfzPjuWPAR3n1610ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWmvP1cLnHD3)首先应该实时监督系统的运转情况，及时发现故障征兆并进行处理。

（2）网络管理员应为关键的网络操作系统服务器建立热备份系统，做好防灾准备。
3、应用系统管理
（1） 确保各种网络应用服务运行的不间断性和工作性能的良好性，出现故障时应将故障造成的损失和影响控制在最小范围内。
（2） 对于用户访问频率高、系统负荷的网络应用服务，必要时网络管理员还应该采取分担的技术措施。
4、用户服务和管理

用户的开户和撤销；用户计费管理;用户组的配置和管理; 用户可用服务和资源的的权限管理和配额管理；包括用户桌面连网电脑的技术支持服务和用户技术培训服务的用户端支持服务。
5、安全保密管理

对于普通级别的网络，主要是配置管理好[系统防火墙](https://www.baidu.com/s?wd=%E7%B3%BB%E7%BB%9F%E9%98%B2%E7%81%AB%E5%A2%99&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLPvcsuyfzPjuWPAR3n1610ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWmvP1cLnHD3)。对安全保密级别需要高的网络，除了应该采取上述措施外，还应该配备网络安全漏洞扫描系统，并对关键的网络服务器采取容灾的技术手段。
6、信息存储备份管理

采取一切可能的技术手段和管理措施，保护网络中的信息安全。同时将备份数据保存在安全地点更是很重要。
7、机房管理
（1） 掌控机房数据通信电缆布线情况及供电线路安排，在增减设备时确保布线合理及负载的合理配置，管理维护方便；
（3） 管理网络机房的温度、湿度和通风状况，保持机房整洁有序，提供适合的工作环境；确保室内各种设备的正常运转；
8、个人

最关键的是及时安装更新补丁；应用可及时升级的杀毒软件（含防火墙和web监控）；对系统进行必要的优化。