# 最新网络安全的教案 网络安全教案(优质13篇)

来源：网络 作者：逝水流年 更新时间：2024-07-31

*作为一名默默奉献的教育工作者，通常需要用到教案来辅助教学，借助教案可以让教学工作更科学化。大家想知道怎么样才能写一篇比较优质的教案吗？下面是小编带来的优秀教案范文，希望大家能够喜欢!网络安全的教案篇一一、在使用电脑过程中应该采取哪些网络安全...*

作为一名默默奉献的教育工作者，通常需要用到教案来辅助教学，借助教案可以让教学工作更科学化。大家想知道怎么样才能写一篇比较优质的教案吗？下面是小编带来的优秀教案范文，希望大家能够喜欢!

**网络安全的教案篇一**

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。

四、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。

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。

**网络安全的教案篇二**

1、如何文明上网、健康上网；

2、如何防范不良信息、不健康网站和网络骗子；

3、如何防止沉迷网络游戏；

1、如何健康上网、交友。

2、全国青少年网络文明公约。

1、正确认识网络游戏及带来的危害。

2、如何辩别网络行骗的手段及防范方法。

讲授、提问 教具

（一）设计电脑网络知识问答题，准备多媒体课件。

（二）情景设计：报纸摘抄，一个中学生的网聊日记，学生心理陈述等

（三）学生搜集网络的利弊资料

在教学中我大致按“电脑网络知多少——网络的利弊谈——不健康上网方式的危害——文明上网、绿色上网、远离网吧”四个环节预设我的教学过程。

看来多数同学把上网作为了一种娱乐的方式，上网时感到轻松、刺激和兴奋。除了娱乐的功能，大家对电脑网络还了解多少？老师准备了几道题，看谁能最先说出答案。

屏幕显示：电脑网络知识问答题

1、我国开始正式接入internet的时间为\_\_\_\_\_\_\_\_\_\_\_。（答案：b）

a。1986年 b。1994年 c。1995年 d。1996

2、计算机网络最突出的优点是\_\_\_\_\_\_\_\_。（答案：a）

a、软件。硬件和数据资源共享 b。运算速度快 c。可以相互通讯 d。内存容量大

3、计算机是如何进行数据转换的？

4、你知道国际象棋特级大师与电脑之间的“人机大战”吗？

5、请说出计算机的十个用途？

（这两组问题的对比，使学生从心理上认识到自己对电脑的了解片面，对于电脑网络的娱乐功能，了如指掌，但一些关于电脑的产生、发展历史以及在其他领域的实用功能，他们却知之甚少甚至一无所知，对于电脑网络，并不像自己认为的那样了解。）

分别出示两张照片（屏幕显示图片）并介绍说

2、2024年12月，北京海军总医院的神经外科专家田增民教授，通过互联网的连接，操控一个远程脑外科手术机器人，成功地为1300公里外延安一名脑出血患者进行了手术。

（经过介绍，学生们对电脑网络有了新的认识：电脑网络是现代高科技发展的产物，在生产、卫生、教育、科技、国防等领域有着广泛的应用，它使人的能力更大程度上得到拓展和延伸，展现出无限的可能性。）

此时，学生认识到电脑是工具而不是玩具，使用电脑网络应多注重它的实用的功能，而不仅仅是娱乐的功能。

（三）结论：电脑是工具而非玩具

（一）字幕显示：中国青少年网络行为调查，网络究竟带给我们什么？

（二）小讨论：网络利弊谈

学生边讨论，老师适当点拨分别总结出网络的利与弊。

1、网络的弊：

1）容易网络痴迷而难以自拔，成为无辜的受害者。

2）容易造成现实感缺乏而生活在虚拟的世界里。

3）容易扭曲自尊做虚拟世界里的“英雄”。

4）容易造成现实感缺乏而使正常的人际沟通受阻。

5）耽误时间，影响学习

6）浪费钱财，没钱上网还可能引发偷盗或抢劫。

2、网络的利：

1）开阔视野，丰富知识，足不出户博览世界知识宝库。

2）拓展我们的生活空间，让我们足不出户了解天下大事。

3）帮助我们缩短时间和空间的距离，让我们足不出户就可以传递信息。

4）娱乐的场所，给人刺激和轻松的感觉

5）网上聊天很畅快淋漓，无拘无束

（学生利用自己搜集来的资料，采用辩论的形式，激发学生的`积极性，加深了对网络的认识）

（三）结论：网络是把双刃剑，要学会趋利避害

网络有有害的一面，下面所列的几种上网方式，你认为是有利还是有弊呢？

1、情景设计

1）报纸摘抄：网络对学生的危害《血的教训》《通宵上网累晕头，坐睡铁轨被轧死》

2）学生日记摘抄——网聊十几个小时不下线

“我的身影时常出现在网络的虚幻世界里，我依恋上qq，有时能在qq上挂线十几个小时而不会下线，就像是人在吸毒一样，上瘾后没完没了，看来上网和吸毒可以画等号。我感觉qq就像人们所说的“网络毒品？！”而我已经深深的中毒了，我成了网络中无数网虫的一员了，说到网虫我对它的理解是：一个人在网上吸食了“网络毒品”，以后逐渐上瘾，再以后死在了网络上。网络这把双刃剑把我“杀”死了，只是它“杀人”不见血。”

3）学生心理陈述——回归

4）影像资料

你看了有何感想呢？

（通过教师引导，学生讨论，加深了学生对不健康、不安全上网方式的认识和危害的了解，不但会影响学生正常的生活和学习，甚至会导致堕落和犯罪。）

教师适时引导学生说：“看来网络确实是有利也有害，不健康、不安全的上网方式给我们带来了很大的危害。那么我们如何趋利弊害，健康上网呢？”

（一）上网安全规则八条

第一条：切勿到网吧娱乐，远离不良网络游戏。特别提示：网络是一柄双刃剑，稍不留意它就会刺向你。

第二条：切不可将网络游戏当作一种精神寄托而沉溺其中。尤其是在现实生活中受挫的青少年，不能只依靠网络来缓解压力和焦虑。应该在成年人或朋友的帮助下，勇敢地面对现实生活。

第三条：控制上网时间。一般以30分钟为宜，不超过一小时。在不影响自己正常生活、学习的情况下安全使用网络。

第四条：在网上，不要给出能确定自己真实身份的信息，包括：家庭地址、学校名称、家庭电话号码、密码、父母身份、家庭经济状况等信息。如需要给出，一定要征询父母意见。

第五条：由于网络的虚拟性，在网上读到任何信息都可能是不真实的。任何人在网上都可以匿名或改变性别等，一个给你写信的“12岁女孩”，可能是一个40岁的先生。

第六条：当你单独在家时，不允许网友来访。未经父母同意，不向网上发送自己的照片。不要自己单独与网友会面，如果认为非常有必要会面，则到公共场所，并且需要父母的陪同。

第七条：经常与父母沟通，让父母了解自己在网上的聊天内容或所作所为，如果父母实在对计算机或互连网不感兴趣，也要让自己的可靠的朋友了解，并能经常交流使用互连网的经验。

第八条：如果遇到带有脏话、攻击性、淫秽、威胁、暴力等使你感到不舒服的信件或信息，请不要理睬或反驳，但要马上告诉父母或通知服务商。

（二）倡议—别把自己困在网中央

——珍爱生命，珍惜时间！健康上网，安全上网！绿色上网，远离网吧！

好的板书是一节课最精华的体现。在这堂课中，我根据课堂内容，设计了这个板书，力求突出重点，做到简明，概括。让学生获得更鲜明的印象和有关知识。

网络：天使 魔鬼

一、网络是学习的工具而不是玩具

二、网络是柄双刃剑，要趋利避害。

三、不健康上网方式的危害

四、文明上网，绿色上网，远离网吧

五、别把自己困在网中央

**网络安全的教案篇三**

共建网络安全、共享网络文明

20xx年11月29日。

在化工系内广泛宣传关于网络安全的事项

本次网络安全宣传活动采取多种形式开展：

（一）组织召开网络安全主题教育的团课

通过召开主题教育团课，结合身边典型案例，使学生了解网络安全的重要性以及日常网络生活需要遵守的准则，特别是加强对沉溺于网络学生的教育。

（二）在微信平台上进行网络安全宣传

利用化工系微信平台，对开展网络安全教育活动的方案、计划等相关资料以及宣传活动所取得的成果进行发布。

（三）开展网络安全知识竞赛

为调动师生的积极性，组织师生开展网络安全知识竞赛，竞赛内容紧扣本次活动主题。

（四）开展\"网络安全精彩一课\"教育活动。

举办网络安全宣传讲座，组织师生观看网络安全视频。

通过本次网络安全宣传的活动，使同学们深刻了解到了网络安全的重要性以及怎样防范网络诈骗的发生，从而让同学们更好的利用网络资源来武装自己，提升自己，成就自己！

**网络安全的教案篇四**

1、网络为我们提供了丰富的信息资源，创造了精彩的\'娱乐时空。成为学生学习知识、交流思想、休闲娱乐的重要平台，增强了与外界的沟通和交流，但网络犹如一把双刃剑，其中一些不良内容也极易对学生造成伤害。主要表现在：许多孩子上网浏览色情、暴力等不健康的内容，沉迷于内容低级、庸俗的网上聊天和网络游戏等。网络“无时差、零距离”的特点使得不良内容以前所未有的速度在全球扩散，网络不良内容甚至还会造成学生生理上的伤害。加强网络安全教育尤为紧迫。

2、据佛山日报3月8日报导：在顺德某小学，课间嬉戏时，因为模仿网络游戏，一小学生刺死同班好友。

班会目的：让同学们清楚地认识到网络上存在的各种不安全的隐患，学会在虚拟的网络世界中保护自己的利益；理智地对待各种诱惑，抵制不良思想的侵蚀；尤其注意不能沉迷网络游戏，用血淋淋的事实敲响警钟。

1、对网络中遇到的问题，大家发表见解。

2、看案例和资料，谈感受。

3、班主任进行总结。

甲、乙合：各位同学大家好！这节班会课的主题是《网络安全教育》。

主持人甲：相信同学们对网络都比较了解，但对于网络安全问题又有多少认识呢？不如我们先听李钊提几个有关网络安全的问题吧！

主持人乙：下面的问题都是同学们在上网的过程中遇到的，你们是如何处理，又是为什么呢？请同学们畅所欲言。

（1）你上网有节制吗？时间是怎么安排的？一般是做什么事情？

（2）你有没有保护好自己的上网密码，个人资料？

（4）你会接收不认识的人发过来的文件等资料吗？为什么？

（5）对于暗示、挑衅、威胁等不良信息，你会如何处理？

（6）对发布不良信息的网站、不健康的聊天室以及不健康的页面，你会采取怎样的态度？

（7）有人以赠送钱物或见面等为理由，提出赴约或登门拜访时，你会怎样做？

主持人甲：看来同学们对网络安全的认识是比较全面的，都能理智的控制自己不受不良

思想的侵蚀。

据称，目前中国网络的负面影响主要有以下3个方面：其一、国内外敌对势力在互联网上刊载大量反动性、煽动性、暴力和低级庸俗的内容。对未成年人身心健康造成严重的不良影响。其二、很多犯罪分子利用网站、网吧提供的平台，针对未成年人自控力较弱的特点，利用上网聊天的机会寻找目标实施诈骗、抢劫等犯罪活动，给未成年人的人身安全直接造成威胁。

（8）你曾经去过网吧上网吗？甚至是玩游戏？

（10）如果你的身边有沉迷网络游戏的同学或亲戚朋友，你能说说他们的表现吗？

主持人甲：沉迷网络甚至网络游戏不仅影响我们的学习和心理健康，还可能会让我们走进一个歧途。模仿游戏中的语言或动作，造成惨剧。

主持人甲：3月7日，顺德容桂一所小学的学生在课间嬉戏时模仿网络游戏中的场景进行打斗。同班好友小彭和小龚各自饰演一款当下流行的网络游戏中的敌对角色，“战斗”进行中，小龚不慎用弹簧刀刺死了小彭。

同学自由发表看法：为什么会出现这样的惨剧，你从中想到什么？你会怎样要求自己？

主持人乙：这起惨剧的发生，当然不是偶然的。它的背后，是数量庞大的青少年网络游戏大军。根据最新统计的结果，目前中国约有2024万网游少年中，其中的260万人是网游成瘾者。此前，上海市青少年网络成瘾调查结果显示，该市青少年网络成瘾总发生率为14.2%。“网络成瘾”已成为导致这批青少年家庭矛盾加剧和参与违法犯罪的诱因。

网络成瘾症：可造成人体植物神经紊乱，体内激素水平失衡，免疫功能降低，引发心血管疾病、胃肠神经官能病、紧张性头疼、焦虑、忧郁等，甚至可导致死亡。

网络为我们提供了丰富的信息资源，创造了精彩的娱乐时空。成为学生学习知识、交流思想、休闲娱乐的重要平台，增强了与外界的沟通和交流，但网络犹如一把双刃剑，其中一些不良内容也极易对学生造成伤害，存在很大的安全隐患。这节班会课，我们通过从上网的时间安排，到在网上选择性地浏览信息，对虚拟网络中各种情况采取的自我保护措施，最后到对网络游戏的正确认识做了交流和讨论，目的就是让同学们清楚地认识到网络安全的重要性，学会理智的对待各种诱惑，从而更好的利用网络促进我们学习的进步。

班会结束！

**网络安全的教案篇五**

二、新课教学

（一）网络安全知识小调查

师：下面的问题都是同学们在上网的过程中遇到的，你们是如何处理的呢？

1、你上网有节制吗？时间是怎么安排的？一般是做什么事情？

2、你有没有保护好自己的上网密码，个人资料？

4、你会接收不认识的人发过来的文件等资料吗？为什么？

5、对于暗示、挑衅、威胁等不良信息，你会如何处理？

6、对发布不良信息的网站、不健康的聊天室以及不健康的页面，你会采取怎样的态度？

7、你曾经去过网吧上网吗？都做些什么？

9、如果你的身边有沉迷网络游戏的同学或亲戚朋友，你能说说他们的表现吗？

师：看来同学们对网络安全的认识是比较全面的，都能理智的控制自己不受不良思想的侵蚀。据称，目前中国网络的负面影响主要有以下3个方面：

其一、国内外敌对势力在互联网上刊载大量反动性、煽动性、黄色、暴力和低级庸俗的内容，对未成年人身心健康造成严重的不良影响。

其二，很多犯罪分子利用网站、网吧提供的平台，针对未成年人自控力较弱的特点，利用上网聊天的机会寻找目标实施诈骗、抢劫等犯罪活动，给未成年人的人身安全直接造成威胁。

其三，沉迷网络甚至网络游戏不仅影响未成年人的学习和心理健康，还可能会让未成年人走进一个歧途：模仿游戏中的语言或动作，造成惨剧。

（二）看案例和资料，谈感受

案例一：顺德容桂一所小学的学生在课间嬉戏时模仿网络游戏中的场景进行打斗。同班好友小彭和小龚各自饰演一款当下流行的网络游戏中的敌对角色，“战斗”进行中，小龚不慎用弹簧刀刺死了小彭。

案例三：新疆生产建设兵团农三师53团初中三年级的小伟，原是个品学兼优的好学生，自从在网吧迷恋上了一种叫“传奇”网络游戏后，成绩一落千丈。一边是父母想让他上重点中学的期望，一边是网络游戏的诱惑，让他一直处在矛盾中，小伟认为是网吧影响了自己的学习成绩，于是用匕首将网吧老板陈鹃捅死。

案例四：简阳市平泉镇和平村流浪少年赵刚被杀，头颅被人砸烂，尸体上还有几处刀伤，其死状惨不忍睹。而令人瞠目的却是：杀害少年的凶手竟是3名嗜好上网玩“杀人游戏”的中专生，他们杀人的目的只是为了验证自己“胆量有多大”。

思考：为什么会出现这些惨剧，你从中想到什么？你会怎样要求自己？

师：这些惨剧的发生，当然不是偶然的。它的背后，是数量庞大的青少年网络游戏大军。根据最新统计的结果，目前中国约有万网游少年中，其中的260万人是网游成瘾者。此前，上海市青少年网络成瘾调查结果显示，该市青少年网络成瘾总发生率为14.2%。“网络成瘾”已成为导致这批青少年家庭矛盾加剧和参与违法犯罪的诱因。网络成瘾症：可造成人体植物神经紊乱，体内激素水平失衡，免疫功能降低，引发心血管疾病、胃肠神经官能病、紧张性头疼、焦虑、忧郁等，甚至可导致死亡。

（三）如何正确对待网络

师：刚才我们讲的都是过度沉迷网络造成的危害，但是，网络还是有许多的用途，它为我们搭建了自主学习的宽广平台，它使我们获取更多的信息知识，“足不出户”“尽览天下风云”；它为我们提供参与社交活动的广阔空间，它丰富了我们的生活，摆脱了“两点一线”读书生活的单调。所以，我们要学会正确的运用网络。那么，如何才算正确上网呢？（学生讨论）

师总结：

1、树立正确上网目的，制订上网计划，合理安排时间，注意上网安全。上网之前先决定好上网时间以及上网目的。甚至可以邀请父母和自己一起上网，在网上与朋友交谈或发送email时要保持礼貌和良好的态度。不要随意在网上透露自己的信息。更不可以随意约会网友。对于不明的邮件，一律删除，看到不良内容和网站，要自觉离开。

2、远离聊天室、游戏、bbs，及不良网站。上网的时候尽量远离聊天室、bbs、不良网站，下载的时候尽量借助下载工具，如网络快车、网络蚂蚁、网络传输带等下载软件，提高下载速度。如果在网上阅读花的时间过多，可以重新尝试阅读书本及报刊，一来可以保护视力，二来可以控制上网时间。如果还改变不了的话，可以先把文章下载，等有空的时候再拿出来看，尽量不要影响正常的学习和休息。

3、养成良好的学习和生活习惯。从自身做起，有针对性地从小事入手，逐渐培养和锻炼自己的意志力，尽量丰富课余生活，多参加体育锻炼，多和同学、朋友交流，多参加班级和学校里的集体活动。

三、总结

网络给我们平静如水的生活增添了清新亮丽的色彩，使我们开阔了眼界、增长了知识，给了我们释放情感的机会，但沉迷网络，其危害也是不可低估的，因此，我们务必要把握好自己，千万不要在这虚拟的世界里迷失了自己。最后，让我们一起来大声朗读《全国青少年网络文明公约》：要善于网上学习，不浏览不良信息；要诚实友好交流，不侮辱欺诈他人；要增强自护意识，不随意约会网友；要维护网络安全，不破坏网络秩序；要有益身心健康，不沉溺虚拟时空。

拓展资料：

网络安全概念

网络安全，通常指计算机网络的安全，实际上也可以指计算机通信网络的安全。计算机通信网络是将若干台具有独立功能的计算机通过通信设备及传输媒体互连起来，在通信软件的支持下，实现计算机间的信息传输与交换的系统。而计算机网络是指以共享资源为目的，利用通信手段把地域上相对分散的若干独立的计算机系统、终端设备和数据设备连接起来，并在协议的控制下进行数据交换的系统。计算机网络的根本目的在于资源共享，通信网络是实现网络资源共享的途径，因此，计算机网络是安全的，相应的计算机通信网络也必须是安全的，应该能为网络用户实现信息交换与资源共享。下文中，网络安全既指计算机网络安全，又指计算机通信网络安全。

安全的基本含义：客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。可以把网络安全定义为：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能。要使网络能正常地实现资源共享功能，首先要保证网络的硬件、软件能正常运行，然后要保证数据信息交换的安全。从前面两节可以看到，由于资源共享的滥用，导致了网络的安全问题。因此网络安全的技术途径就是要实行有限制的共享。

相对概念

从用户（个人或企业）的角度来讲，其希望：

（1）在网络上传输的个人信息（如银行账号和上网登录口令等）不被他人发现，这就是用户对网络上传输的信息具有保密性的要求。

（2）在网络上传输的信息没有被他人篡改，这就是用户对网络上传输的信息具有完整性的要求。

（3）在网络上发送的信息源是真实的，不是假冒的，这就是用户对通信各方提出的身份认证的要求。

（4）信息发送者对发送过的信息或完成的某种操作是承认的，这就是用户对信息发送者提出的不可否认的要求。

从网络运行和管理者的角度来讲，其希望本地信息网正常运行，正常提供服务，不受网外攻击，未出现计算机病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁。从安全保密部门的角度来讲，其希望对非法的、有害的、涉及国家安全或商业机密的信息进行过滤和防堵，避免通过网络泄露关于国家安全或商业机密的信息，避免对社会造成危害，对企业造成经济损失。从社会教育和意识形态的角度来讲，应避免不健康内容的传播，正确引导积极向上的网络文化。

狭义解释

网络安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。它包括硬件系统的安全、可靠运行，操作系统和应用软件的安全，数据库系统的.安全，电磁信息泄露的防护等。狭义的网络安全，侧重于网络传输的安全。

广义解释

网络传输的安全与传输的信息内容有密切的关系。信息内容的安全即信息安全，包括信息的保密性、真实性和完整性。

广义的网络安全是指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。

其中的信息安全需求，是指通信网络给人们提供信息查询、网络服务时，保证服务对象的信息不受监听、窃取和篡改等威胁，以满足人们最基本的安全需要（如隐秘性、可用性等）的特性。网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全，可见，这与其所保护的对象有关。

由于网络是信息传递的载体，因此信息安全与网络安全具有内在的联系，凡是网上的信息必然与网络安全息息相关。信息安全的含义不仅包括网上信息的安全，而且包括网下信息的安全。现在谈论的网络安全，主要是是指面向网络的信息安全，或者是网上信息的安全。

主要问题

安全隐患

1．internet是一个开放的、无控制机构的网络，黑客（hacker）经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

2．internet的数据传输是基于tcp/ip通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

3．internet上的通信业务多数使用unix操作系统来支持，unix操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

4．在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄露等，在应用层支持的服务协议中是凭着君子协定来维系的。

5．电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息会存在着很大的危险。

6．计算机病毒通过internet的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名ftp文件传送、也可以通过邮件和邮件的附加文件传播。

攻击形式

主要有四种方式中断、截获、修改和伪造。

中断是以可用性作为攻击目标，它毁坏系统资源，使网络不可用。

截获是以保密性作为攻击目标，非授权用户通过某种手段获得对系统资源的访问。

修改是以完整性作为攻击目标，非授权用户不仅获得访问而且对数据进行修改。

伪造是以完整性作为攻击目标，非授权用户将伪造的数据插入到正常传输的数据中。

解决方案

1．入侵检测系统部署

入侵检测能力是衡量一个防御体系是否完整有效的重要因素，强大完整的入侵检测体系可以弥补防火墙相对静态防御的不足。对来自外部网和校园网内部的各种行为进行实时检测，及时发现各种可能的攻击企图，并采取相应的措施。具体来讲，就是将入侵检测引擎接入中心交换机上。入侵检测系统集入侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件，作为网络管理员事后分析的依据；如果情况严重，系统可以发出实时报警，使得学校管理员能够及时采取应对措施。

2．漏洞扫描系统

采用最先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。

3．网络版杀毒产品部署

在该网络防病毒方案中，我们最终要达到一个目的就是：要在整个局域网内杜绝病毒的感染、传播和发作，为了实现这一点，我们应该在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能。

网络信息分类

网络通信具有全程全网联合作业的特点。就通信而言，它由五大部分组成：传输和交换、网络标准、协议和编码、通信终端、通信信源、人员。这五大部分都会遭到严重的威胁和攻击，都会成为对网络和信息的攻击点。而在网络中，保障信息安全是网络安全的核心。网络中的信息可以分成用户信息和网络信息两大类。

用户信息

在网络中，用户信息主要指面向用户的话音、数据、图像、文字和各类媒体库的信息，它大致有以下几种：

一般性的公开信息：如正常的大众传媒信息、公开性的宣传信息、大众娱乐信息、广告性信息和其他可以公开的信息。

个人隐私信息：如纯属个人隐私的民用信息，应保障用户的合法权益。

知识产权保护的信息：如按国际上签订的《建立世界知识产权组织公约》第二条规定的保护范围，应受到相关法律保护。

商业信息：包括电子商务、电子金融、证券和税务等信息。这种信息包含大量的财和物，是犯罪分子攻击的重要目标，应采取必要措施进行安全防范。

不良信息：主要包括涉及政治、文化和伦理道德领域的不良信息，还包括称为“信息垃圾”的无聊或无用信息，应采取一定措施过滤或清除这种信息，并依法打击犯罪分子和犯罪集团。

攻击性信息：它涉及各种人为的恶意攻击信息，如国内外的“黑客”攻击、内部和外部人员的攻击、计算机犯罪和计算机病毒信息。这种针对性的攻击信息危害很大，应当重点进行安全防范。

保密信息：按照国家有关规定，确定信息的不同密级，如秘密级、机密级和绝密级。这种信息涉及政治、经济、军事、文化、外交等各方面的秘密信息，是信息安全的重点，必须采取有效措施给予特殊的保护。

网络信息

在网络中，网络信息与用户信息不同，它是面向网络运行的信息。网络信息是网络内部的专用信息。它仅向通信维护和管理人员提供有限的维护、控制、检测和操作层面的信息资料，其核心部分仍不允许随意访问。特别应当指出，当前对网络的威胁和攻击不仅是为了获取重要的用户机密信息，得到最大的利益，还把攻击的矛头直接指向网络本身。除对网络硬件攻击外，还会对网络信息进行攻击，严重时能使网络陷于瘫痪，甚至危及国家安全。网络信息主要包括以下几种：

通信程序信息：由于程序的复杂性和编程的多样性，而且常以人们不易读懂的形式存在，所以在通信程序中很容易预留下隐藏的缺陷、病毒，隐蔽通道和植入各种攻击信息。

操作系统信息：在复杂的大型通信设备中，常采用专门的操作系统作为其硬件和软件应用程序之间的接口程序模块。它是通信系统的核心控制软件。由于某些操作系统的安全性不完备，会招致潜在的入侵，如非法访问、访问控制的混乱、不完全的中介和操作系统缺陷等。

数据库信息：在数据库中，既有敏感数据又有非敏感数据，既要考虑安全性又要兼顾开放性和资源共享。所以，数据库的安全性，不仅要保护数据的机密性，重要的是必须确保数据的完整性和可用性，即保护数据在物理上、逻辑上的完整性和元素的完整性，并在任何情况下，包括灾害性事故后，都能提供有效的访问。

通信协议信息：协议是两个或多个通信参与者（包括人、进程或实体）为完成某种功能而采取的一系列有序步骤，使得通信参与者协调一致地完成通信联系，实现互连的共同约定。通信协议具有预先设计、相互约定、无歧义和完备的特点。在各类网络中已经制定了许多相关的协议。如在保密通信中，仅仅进行加密并不能保证信息的机密性，只有正确地进行加密，同时保证协议的安全才能实现信息的保密。然而，协议的不够完备，会给攻击者以可乘之机，造成严重的恶果。

电信网的信令信息：在网络中，信令信息的破坏可导致网络的大面积瘫痪。为信令网的可靠性和可用性，全网应采取必要的冗余措施，以及有效的调度、管理和再组织措施，以保证信令信息的完整性，防止人为或非人为的篡改和破坏，防止对信令信息的主动攻击和病毒攻击。

数字同步网的定时信息：我国的数字同步网采用分布式多地区基准钟（lpr）控制的全同步网。lpr系统由铷钟加装两部全球定位系统（gps）组成，或由综合定时供给系统bits加上gps组成。在北京、武汉、兰州三地设立全国的一级标准时钟（prc），采用铯钟组定时作为备用基准，gps作为主用基准。为防止gps在非常时期失效或基准精度下降，应加强集中检测、监控、维护和管理，确保数字同步网的安全运行。

网络管理信息：网络管理系统是涉及网络维护、运营和管理信息的综合管理系统。它集高度自动化的信息收集、传输、处理和存储于一体，集性能管理、故障管理、配置管理、计费管理和安全管理于一身，对于最大限度地利用网络资源、确保网络的安全具有重要意义。安全管理主要包括系统安全管理、安全服务管理、安全机制管理、安全事件处理管理、安全审计管理和安全恢复管理等内容。

**网络安全的教案篇六**

1、使学生了解什么是网络信息安全,让学生了解维护信息系统安全的.一般措施。

2、掌握网络存在哪些信息安全威胁，会带来怎么样的后果，应如何有效保护自己的信息。

3、培养学生安全地使用网络信息技术,增强学生的信息安全意识.

解威胁信息的常见因素。

学会病毒防护和信息安全防护的基本措施

1、学会病毒防护和信息安全防护的基本措施

2、日常生活中信息技术的安全使用。

1、情境导入：初识计算机病毒、电脑黑客造成的严重后果。

播放计算机病毒、黑客进行破坏、犯罪的相关新闻视频资料。

使得学生认识道病毒的破坏作用，意识到信息技术安全问题的严峻性。

2、引出课题《信息安全》

3、提出问题，学生回答，教师指点：

通过刚才的演示，大家想想下面几个问题：

某天，朋友在他的机器上看到你计算机中的一些文件夹，这说明了什么？

某天，朋友告诉你，他知道你的上网帐号和密码，你信吗？

你在网络上收到信息，说只要你邮寄多少钱到某一账户，就可得到大奖，你如何看待？

某天，当你用qq聊天时，某个陌生人给你发来一个网址，你会打开吗？

因特网是一个信息的海洋，对于这里的所有信息，所有的“网中人”，你都会相信吗？

结合学生对于计算机的日常应用，讨论后，学生对病毒、黑客、垃圾邮件、网络共享、计算机犯罪有了初步认识。每一个学生都强化了一种意识，信息安全问题关系到的我们每个人。

4、掌握威胁信息安全的“最大元凶”计算机病毒(小组讨论方式)

(1)定义：

计算机病毒是一种人为编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

(2)特性：具有潜伏性、传染性、隐蔽性和破坏性。

(3)传播途径：有很多种传播途径，主要通过网络和磁盘进行传播。

5、做好信息安全的防护工作教师对于如何树立正确的网络行为进行归纳：

安装正版的杀毒软件和防火墙，不定期对其升级，对系统全面查杀病毒；

对计算机系统打补丁，对重要数据不定期的进行备份；

不制造、使用和传播计算机病毒和黑客攻击软件；

遵守国家相关法律法规，不做违法的事。

6、将学生分为7个小组，每组6人，对于以上的学习讲讲自己的心得体会，并谈谈对于自己应该如何树立正确的网络文明行为。

7、课堂总结

这节课我们学习了网络存在的信息安全的威胁的几种类型，希望通过这节课的学习，同学提高自己的信息安全意识，正确的使用网络给我们提供的便利的同时，时刻注意信息安全的重要。

8、课后作业：

学习《全国青少年网络文明公约》。

查询安全上网的方法。

**网络安全的教案篇七**

(一)网络钓鱼

网络钓鱼是指不法分子通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件或短信、即时通讯信息等，引诱收信人给出敏感信息(如用户名、口令、帐号id或信用卡详细信息)，然后利用这些信息假冒受害者进行欺诈性金融交易，从而获得经济利益。受害者经常遭受显著的经济损失或全部个人信息被窃取并用于犯罪的目的。

(二)木马病毒

特洛伊木马是一种基于远程控制的黑客工具，它通常会伪装成程序包、压缩文件、图片、视频等形式，通过网页、邮件等渠道引诱用户下载安装，如果用户打开了此类木马程序，用户的电脑或手机等电子设备便会被编写木马程序的不法分子所控制，从而造成信息文件被修改或窃取、电子账户资金被盗用等危害。

(三)社交陷阱社交陷阱是指有些不法分子利用社会工程学手段获取持卡人个人信息，并通过一些重要信息盗用持卡人账户资金的网络诈骗方式。

(四)伪基站

“伪基站”一般由主机和笔记本电脑组成，不法分子通过“伪基站”能搜取设备周围一定范围内的手机卡信息，并通过伪装成运营商的基站，冒充任意的手机号码强行向用户手机发送诈骗、广告推销等短信息。

(五)信息泄露

目前某些中小网站的安全防护能力较弱，容易遭到黑客攻击，不少注册用户的用户名和密码便因此泄露。而如果用户的支付账户设置了相同的用户名和密码，则极易发生盗用。

安全工具相当于给你的账户或者资金上了一道道锁。如果能合理使用网络安全支付工具，能够大大降低网络支付风险，使你的支付更加安全，更有保障。

目前，市场上主流的网络安全支付工具主要有下面几类：

一是数字证书。电脑或手机上安装数字证书后，即使账户支付密码被盗，也需要在已经安装了数字证书的机器上才能支付，保障资金安全。

二是短信验证码。短信验证码是用户在支付时，银行或第三方支付通过客户绑定的手机，下发短信给客户的一次性随机动态密码。

三是动态口令。无需与电脑连接的安全支付工具，采用定时变换的一次性随机密码与客户设置的密码相结合。

四是usbkey。连接在电脑usb接口上使用的一种安全支付工具，支付时需要插入电脑，才能进行支付。

用户可以根据自己的实际情况以及银行或支付机构的建议，选择适合自己的网络安全支付工具。

(一)保管好账号、密码和usbkey(或称ukey、网盾、u盾等)

1、不要相信任何套取账号、usbkey和密码的行为，也不要轻易向他人透露您的证件号码、账号、密码等。

2、密码应尽量设置为数字、英文大小写字母的组合，不要用生日、姓名等容易被猜测的内容做密码。

3、如果泄露了usbkey密码，应尽快办理补发或更换业务。

(二)认清网站网址

网上购物时请到正规、知名的网上商户进行网上支付，交易时请确认地址栏里的网址是否正确。

(三)确保计算机系统安全

1、从银行官方网站下载安装网上银行、手机银行安全控件和客户端软件。

2、设置windows登录密码，windowsxp以上系统请打开系统自带的防火墙，关闭远程登录功能。

3、定期下载并安装最新的操作系统和浏览器安全补丁。

4、安装防病毒软件和防火墙软件，并及时升级更新。

(四)提升安全意识

1、使用经国家权威机构认证的网银证书，建议同时开通usbkey和短信口令功能。

2、开通短信口令时，务必确认接收短信的手机号码为本人手机号码。

3、不要轻信手机接收到的中奖、贷款等短信、电话和非银行官方网站上的任何信息。

4、不要轻信假公安、假警官、假法官、假检察官等以“安全账户”名义要求转账的电话欺诈。

5、避免在公共场所或他人计算机上登录和使用网上银行。退出网上银行或暂时离开电脑时，一定要将usbkey拔出。

6、操作网银时建议不要浏览别的网站，有些网站的恶意代码可能会获取您电脑上的信息。

7、建议对不同的电子支付方式分别设置合理的交易限额，每次交易都请仔细核对交易内容，确认无误后再进行操作。在交易未完成时不要中途离开交易终端，交易完成后应点击退出。

8、定期检查核对网上银行交易记录。可以通过定制银行短信提醒服务和对账邮件，及时获得银行登录、余额变动、账户设置变更等信息提醒。

网络安全重在防范，一旦发现被骗，要在第一时间联系银行、支付机构，采取相应应急措施，同时向当地警方报警。

(一)已经在钓鱼网站输入了密码怎么办?

1、如果您还能登录您的账户：请立刻修改您的支付密码和登录密码。同时，进入交易明细查询查看是否有可疑交易。如有，须立刻致电银行或支付机构的客服电话。

2、如果您还输入了银行卡信息：请立刻致电银行申请临时冻结账户或电话挂失(此时您的银行账户只能入账不能出账)。

3、如果您已经不能登录：请立刻致电银行或者支付机构的客服电话，申请对您的账户进行暂时监管。

4、使用最新版的杀毒软件对电脑进行全面扫描，确保钓鱼网站没有挂木马。如果发现有，请在确认电脑安全后再次修改登录与支付密码。

(二)发现账户资金被盗怎么办?

1、要在第一时间修改账户密码，同时转出余额资金。

2、进入交易管理，查找可疑交易，保留对非授权的资金交易。

3、如果被盗的是银行卡账户的话，请立刻致电银行申请临时冻结账户或电话挂失(此时您的银行账户只能入账不能出账)。

6月1日起，《中华人民共和国网络安全法》正式施行，它不仅明确了政府各部门的职责权限，强化了网络运营者的主体责任，还对我们每一个人都提出了明确的要求。

**网络安全的教案篇八**

提高网络安全意识，合理利用网络资源

1、提升大学生三种网络相关的能力：分辨网络安全隐患的能力、正确使用网络资源的能力、合理使用网络的自控能力。

2、树立一种网络观念：网络是大学生的学习资源，而不仅仅是娱乐工具。引导大学生将网络成为自己的学习工具，做网络的主人，使丰富的网络资源为己所用，提高自我竞争力。

新学期伊始，我所带的大一学生已经成为大二学生，他们已经基本适应了大学生活，在专业学习、校园生活、社会实践等方面都进展有序。为了方便自我学习和生活，很多同学在大二学年都配置了电脑，在宿舍也开通了网络，网络在为同学们的网上课程学习、课外娱乐活动、大学生校内网交流、网上购物、网络资源使用等提供了极大的便利，但我们也同时看到，网络使用是一把双刃剑，很多同学在网络交友、网络购物、网络游戏等中误入歧途，有的交友不慎感情受伤甚至人身受到伤害、有的沉迷游戏荒废学业不得不退学、有的网络购物不慎被骗遭受经济损失的等等，可以说，网络在给我们大学生呈现一幅美好画面的同时，背后也波涛汹涌遍布暗礁。大二学生有的还没有足够的警惕心和较高的辨别能力，很容易在网络中迷失自我，陷入危机，有必要通过主题班会的宣讲，提高同学们分辨网络安全隐患的能力、正确使用网络资源的能力、合理使用网络的自控能力，真正做到网络服务于同学们的成长成才。

待定

待定

全体同学

1、对同学们网络使用情况的摸底调查。

2、收集有关网络安全的文字、视频资料及网络不安全的`案例。

3、请班级同学编排有关于网络安全的小品。

4、对各班委相关工作进行分配。

1、班级组织委员组织同学们准时到场并进行签到。

2、请同学们欣赏小品，通过小品明确本次班会主题，主持人宣布班会正式开始。

3、现场调查一下同学们网络的使用用途以及在使用过程中遇到的问题。

4、展示有关于网络使用安全的图片和视频资料，请同学们讲讲观后感受。

5、结合案列，详细介绍大学生在网络使用过程中可能遇到的各种安全隐患如网络交友不慎、网络购物不当、网络游戏成瘾、网络言语不实等可能导致的一系列后果等，让同学们对网络安全能形成全面清晰深刻的认识，提高对网络安全的辨别能力。

6、结合大学生的学习和生活，展现网络优越的一面如免费网络课程资源、学校图书馆网上资源、大学生就业资源网站等，形成正确使用网络资源的能力。

7、请相关学生现身说法，介绍网络安全教育经验，主持人指出网络只是丰富我们学习和生活的一种途径，不能过度依赖和沉湎于网络中，鼓励同学们在现实生活中多加锻炼，提高对网络使用的自控力，真正做到让网络成为大学生学习的助推器，生活中的好帮手。

8、辅导员进行总结，请同学们再次认识到网络的利与弊，重视网络使用中的安全隐患，将网络成为自己的学习工具，做网络的主人，使丰富的网络资源为己所用，提高自我竞争力。

1、同学们在使用网络资源的时候，一定要提高警惕，学会分辨网络各类隐患。

2、面对网络资源的庞杂纷繁，要学会如何合理利用的能力更加重要，班级可以成立网络中心小组，帮助同学们鉴别真伪、去除糟粕，提高网络安全系数。

3、每一个同学都应该好好把握大二时光，加强专业学习，使网络资源服务同学们的自我成长。

**网络安全的教案篇九**

1、通过生活中发生的被拐骗案例、引起同学们对防拐骗防诱拐的重视。

2、通过本次班会活动，使同学们了解一些基本的防拐骗防诱拐知识和被拐骗后的自我解救方法。

讲授法、讲事例组织学生讨论

一节课

1、让同学们收集有关被拐骗方面的新闻。

2、了解一些基本的防拐骗防诱拐知识。

３、了解一些被拐骗后的自我解救方法。

（一）导入

1、学生自由发言，陈述所搜集到的被拐骗被诱拐的事例。

2、呈现主题。

（二）被拐骗被诱拐的事例

1）柴伟是郑州市民，一个月前他16岁的儿子在郑州火车站附近突然走失，经过多方打听，柴伟得知儿子被人贩子卖到了山西黑窑场做了苦工。在寻找孩子的过程中，他结识了另外五家和他一样丢失孩子的家长，几位家长开始联合在山西黑窑场寻找孩子。在将近两个月的寻找过程中，他们只找到了一家丢失的孩子，却解救了另外50多名素不相识的童工。这三个孩子，都是刚从山西被解救出来的。

2）今年3月的一天，18岁的北京女孩小静（化名）在太原被网友骗了财物。怕被父母骂，她想打工挣回家路费。这个时候，她认识了吕梁男子郭兰军。郭兰军花言巧语将其骗到了他的老家———吕梁山区一个山村，并强迫小静做了他的.媳妇。从此，小静开始了她噩梦般的135天。近日，记者从北京警方获悉，9月19日，小静被北京警方解救。她安全了，但至今那些非人的生活仍在梦里折磨她。小静的生活因此发生了很多变化。她希望她的经历能够警醒那些上网聊天的女孩，不要轻信网友。

活动过程：

系列活动一：“防拐防骗”安全演练

1、年级组发动家长参与到活动中来，专门请平时不怎么来接送幼儿的家长来幼儿园充当“骗子”，利用诱人的美食，新颖的玩具去“诱拐”孩子们。

小结：从活动中我们可以看到有些孩子经不起诱惑，乖乖地跟着“骗子”走，这说明部分幼儿的自我保护意识是比较淡薄的。

2、老师们利用照片和录像等形式记录下活动的过程，然后根据活动的具体情况，各班再有针对性地开展防拐防骗的教育活动，如：“一个人在家有人敲门了怎么办”、“出门旅游或逛超市时与大人走散了怎么办”、“路上有陌生人跟着你怎么办”、及“怎样拨打报警电话”等日常生活中的安全问题及应对方案。

系列活动二：举行“防拐防骗”家长座谈会

活动结束后，班级老师与所有的幼儿家长进行了交流和总结。通过这次的演练活动，帮助幼儿了解和掌握一些和陌生人相处的方法，让孩子知道如何应变可能遇到的危险。知道仅仅告诉幼儿“不接受陌生人的糖果或不要和陌生人说话”是远远不够的，还必须向孩子描述可能遇到的情况，然后指导孩子如何去做。家长们更要提高警惕防范，在大忙季节更要关注孩子，让孩子随时在自己的视线之内；入园时要将孩子送到班级老师的手里才能离园，家长委托别人接孩子，不仅要带好接送卡，还要事先给班级教师打电话预先告知。

反思：

这次“防拐防骗”的安全系列活动，不管是对教师、家长还是对幼儿都是一次特殊的经历，更起到了警醒和呼吁的作用。安全教育需要幼儿园、家庭共同努力，在引导孩子们增强自我保护意识的同时，教师及家长也应提高防范意识，将安全教育融入到日常生活中，不断强化自我安全保护意识和辨别是非的\'能力，培养幼儿在紧急情况下的自救能力和处理问题能力，确保自己的人身安全。

**网络安全的教案篇十**

1、让学生认识到网络有积极的`一面，也有消极的一面。

2、让学生加强对不良网上内容的抵抗力。

3、正确对待互联网，做健康阳光青年。

教学重点:让学生对互联网有一个正确的态度，正确利用网络。

教学难点:提高网络自制力，让学生有节制的上网。

教学方法:讲授法，讨论法，演讲法。

教学时间:1课时

导入语:据中国青少年网络协会提供的数据，目前，城市上网小学生比例为xx%，初中生为xx%，高中生为xx%。我国网瘾青少年约占青少年网民总数的xx%，而13岁至17岁的中学生群体成为“网瘾重灾区”。网络这把“双刃剑”?正在无情地吞噬着青少年的身心健康，因迷恋上网而逃学、离家出走、抢劫甚至猝死在网吧、走向犯罪道路的现象屡屡发生。

一、认识网瘾，拒绝网瘾

1.网瘾是什么?

“网瘾”?可谓互联网成瘾综合征。即对现实生活冷漠，而对虚拟的网络游戏、情爱、信息等沉溺、痴迷。它是一种行为过程，也是行为发展的终结。心理学认为?网瘾是一种精神病;而心理老师认为?网瘾?是正常人出现的心理问题(特例除外)。网瘾具体可分为网络交际瘾、网络色情瘾、网络游戏瘾、网络信息瘾和网络赌博瘾等类型。

2、网瘾的危害

青少年患上网瘾后，开始只是精神依赖，以后便发展为躯体依赖，长时间的沉迷于网络可导致情绪低落、视力下降、肩背肌肉劳损、睡眠节奏紊乱、食欲不振、消化不良、免疫功能下降。停止上网则出现失眠、头痛、注重力不集中、消化不良、恶心厌食、体重下降。由于上网时间过长，大脑高度兴奋，导致一系列复杂的生理变化，尤其是植物神经功能紊乱，机体免疫功能降低，由此诱发心血管疾病、焦虑症、抑郁症等。青少年正处在身体发育的关键时期，这些问题的出现都会对他们的身体健康和成长发育产生极大的影响。网络成瘾的青少年最为直接的危害是影响了正常的学习，使他们不能集中精力听课，不能按时完成作业，成绩下滑，丧失学习的信心和兴趣，甚至会发展到逃课、辍学。网络中各种不健康的内容，也可造成青少年自我过分放纵，使法律及道德看念淡薄，人生观、价值看扭曲。患有网瘾青的青少年，为了能上网，他们不惜用掉自己的学费、生活费，不惜丧失自己的人格和自尊向人乞讨，在外借钱，在家欺骗父母，甚至会发展到偷窃、抢劫，最后走上违法犯罪的道路。

二、及早预防，树立正确的网络意识

染上网瘾的孩子多半是自制能力差，内心得不到理解，对学习表示厌倦的孩子。对于他们，我们必须让他们改掉陋习，不要注重成绩，更重要的是素质教育，理解和支持与鼓励他们，使他们变得阳光，开朗，自信，这才是前提。

1、帮助孩子认清网络的虚拟性和隐蔽性。

2、限制上网时间和上网内容

孩子每天上网时间2个小时比较好，可以帮助孩子制定一个日程表，多做一些运动，不要守在电脑前面，对身体也不好。还有孩子上网的内容一定要监控好，我们可以安装一些软件来定时截图，或者查看浏览器浏览历史等，及时了解孩子使用网络的状况，把孩子浏览的内容引导至新闻，学习等方面。如果年龄小的孩子，最好家长一起陪同上网。

3、与孩子交流和沟通

经常与孩子交流，聊聊天，让孩子倾诉自己的烦恼，敞开自己的心扉，尤其是内向的孩子，更应该获得父母的理解，不要让他们把网络当作唯一交流，发泄情绪的对象。不要是孩子内心感到寂寞，要学会倾听孩子。

4、防止孩子去网吧上网

5、一旦染上网瘾，必须及时制止

当孩子已经成迷于网络而无法自拔时，我们就需要联合老师，关注孩子的动态，避免继续去网吧，讲明其危害，帮他们树立正确的人生观，价值观。这个也需要动员全社会的力量，需要政府保证未成年人所享有的权利。但是我们作为父母更需要给孩子关怀，让他们心中有爱，注重孩子的道德教育，让他们明白自己人生价值的取向。

**网络安全的教案篇十一**

（一）网络安全知识小调查

师：下面的问题都是同学们在上网的过程中遇到的，你们是如何处理的呢？

1、你上网有节制吗？时间是怎么安排的？一般是做什么事情？

2、你有没有保护好自己的上网密码，个人资料？

4、你会接收不认识的人发过来的文件等资料吗？为什么？

5、对于暗示、挑衅、威胁等不良信息，你会如何处理？

6、对发布不良信息的网站、不健康的聊天室以及不健康的页面，你会采取怎样的态度？

7、你曾经去过网吧上网吗？都做些什么？

9、如果你的身边有沉迷网络游戏的同学或亲戚朋友，你能说说他们的表现吗？

师：看来同学们对网络安全的认识是比较全面的，都能理智的控制自己不受不良思想的侵蚀。据称，目前中国网络的负面影响主要有以下3个方面：

其一、国内外敌对势力在互联网上刊载大量反动性、煽动性、黄色、暴力和低级庸俗的内容，对未成年人身心健康造成严重的不良影响。

其二，很多犯罪分子利用网站、网吧提供的平台，针对未成年人自控力较弱的特点，利用上网聊天的机会寻找目标实施诈骗、抢劫等犯罪活动，给未成年人的人身安全直接造成威胁。

其三，沉迷网络甚至网络游戏不仅影响未成年人的学习和心理健康，还可能会让未成年人走进一个歧途：模仿游戏中的语言或动作，造成惨剧。

（二）看案例和资料，谈感受

案例一：顺德容桂一所小学的学生在课间嬉戏时模仿网络游戏中的场景进行打斗。同班好友小彭和小龚各自饰演一款当下流行的网络游戏中的敌对角色，“战斗”进行中，小龚不慎用弹簧刀刺死了小彭。

案例三：新疆生产建设兵团农三师53团初中三年级的小伟，原是个品学兼优的好学生，自从在网吧迷恋上了一种叫“传奇”网络游戏后，成绩一落千丈。一边是父母想让他上重点中学的期望，一边是网络游戏的诱惑，让他一直处在矛盾中，小伟认为是网吧影响了自己的学习成绩，于是用匕首将网吧老板陈鹃捅死。

案例四：简阳市平泉镇和平村流浪少年赵刚被杀，头颅被人砸烂，尸体上还有几处刀伤，其死状惨不忍睹。而令人瞠目的却是：杀害少年的凶手竟是3名嗜好上网玩“杀人游戏”的中专生，他们杀人的目的只是为了验证自己“胆量有多大”。

思考：为什么会出现这些惨剧，你从中想到什么？你会怎样要求自己？

师：这些惨剧的发生，当然不是偶然的。它的背后，是数量庞大的青少年网络游戏大军。根据最新统计的结果，目前中国约有2024万网游少年中，其中的260万人是网游成瘾者。此前，上海市青少年网络成瘾调查结果显示，该市青少年网络成瘾总发生率为14.2%。“网络成瘾”已成为导致这批青少年家庭矛盾加剧和参与违法犯罪的诱因。网络成瘾症：可造成人体植物神经紊乱，体内激素水平失衡，免疫功能降低，引发心血管疾病、胃肠神经官能病、紧张性头疼、焦虑、忧郁等，甚至可导致死亡。

（三）如何正确对待网络

师：刚才我们讲的都是过度沉迷网络造成的危害，但是，网络还是有许多的用途，它为我们搭建了自主学习的宽广平台，它使我们获取更多的信息知识，“足不出户”“尽览天下风云”；它为我们提供参与社交活动的广阔空间，它丰富了我们的生活，摆脱了“两点一线”读书生活的单调。所以，我们要学会正确的运用网络。那么，如何才算正确上网呢？（学生讨论）

师总结：

1、树立正确上网目的，制订上网计划，合理安排时间，注意上网安全。上网之前先决定好上网时间以及上网目的。甚至可以邀请父母和自己一起上网，在网上与朋友交谈或发送email时要保持礼貌和良好的态度。不要随意在网上透露自己的信息。更不可以随意约会网友。对于不明的邮件，一律删除，看到不良内容和网站，要自觉离开。

2、远离聊天室、游戏、bbs，及不良网站。上网的时候尽量远离聊天室、bbs、不良网站，下载的时候尽量借助下载工具，如网络快车、网络蚂蚁、网络传输带等下载软件，提高下载速度。如果在网上阅读花的时间过多，可以重新尝试阅读书本及报刊，一来可以保护视力，二来可以控制上网时间。如果还改变不了的话，可以先把文章下载，等有空的时候再拿出来看，尽量不要影响正常的学习和休息。

3、养成良好的学习和生活习惯。从自身做起，有针对性地从小事入手，逐渐培养和锻炼自己的意志力，尽量丰富课余生活，多参加体育锻炼，多和同学、朋友交流，多参加班级和学校里的集体活动。

网络给我们平静如水的生活增添了清新亮丽的色彩，使我们开阔了眼界、增长了知识，给了我们释放情感的机会，但沉迷网络，其危害也是不可低估的，因此，我们务必要把握好自己，千万不要在这虚拟的世界里迷失了自己。最后，让我们一起来大声朗读《全国青少年网络文明公约》：要善于网上学习，不浏览不良信息；要诚实友好交流，不侮辱欺诈他人；要增强自护意识，不随意约会网友；要维护网络安全，不破坏网络秩序；要有益身心健康，不沉溺虚拟时空。

网络安全，通常指计算机网络的安全，实际上也可以指计算机通信网络的安全。计算机通信网络是将若干台具有独立功能的计算机通过通信设备及传输媒体互连起来，在通信软件的支持下，实现计算机间的信息传输与交换的系统。而计算机网络是指以共享资源为目的，利用通信手段把地域上相对分散的若干独立的计算机系统、终端设备和数据设备连接起来，并在协议的控制下进行数据交换的系统。计算机网络的根本目的在于资源共享，通信网络是实现网络资源共享的途径，因此，计算机网络是安全的，相应的计算机通信网络也必须是安全的，应该能为网络用户实现信息交换与资源共享。下文中，网络安全既指计算机网络安全，又指计算机通信网络安全。

安全的基本含义：客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。可以把网络安全定义为：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能。要使网络能正常地实现资源共享功能，首先要保证网络的硬件、软件能正常运行，然后要保证数据信息交换的安全。从前面两节可以看到，由于资源共享的滥用，导致了网络的安全问题。因此网络安全的技术途径就是要实行有限制的共享。

相对概念

从用户（个人或企业）的角度来讲，其希望：

（1）在网络上传输的个人信息（如银行账号和上网登录口令等）不被他人发现，这就是用户对网络上传输的信息具有保密性的要求。

（2）在网络上传输的信息没有被他人篡改，这就是用户对网络上传输的信息具有完整性的要求。

（3）在网络上发送的信息源是真实的，不是假冒的，这就是用户对通信各方提出的身份认证的要求。

（4）信息发送者对发送过的信息或完成的某种操作是承认的，这就是用户对信息发送者提出的不可否认的要求。

从网络运行和管理者的角度来讲，其希望本地信息网正常运行，正常提供服务，不受网外攻击，未出现计算机病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁。从安全保密部门的角度来讲，其希望对非法的、有害的、涉及国家安全或商业机密的信息进行过滤和防堵，避免通过网络泄露关于国家安全或商业机密的信息，避免对社会造成危害，对企业造成经济损失。从社会教育和意识形态的角度来讲，应避免不健康内容的传播，正确引导积极向上的网络文化。

狭义解释

网络安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。它包括硬件系统的安全、可靠运行，操作系统和应用软件的安全，数据库系统的.安全，电磁信息泄露的防护等。狭义的网络安全，侧重于网络传输的安全。

广义解释

网络传输的安全与传输的信息内容有密切的关系。信息内容的安全即信息安全，包括信息的保密性、真实性和完整性。

广义的网络安全是指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。

其中的信息安全需求，是指通信网络给人们提供信息查询、网络服务时，保证服务对象的信息不受监听、窃取和篡改等威胁，以满足人们最基本的安全需要（如隐秘性、可用性等）的特性。网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全，可见，这与其所保护的对象有关。

由于网络是信息传递的载体，因此信息安全与网络安全具有内在的联系，凡是网上的信息必然与网络安全息息相关。信息安全的含义不仅包括网上信息的安全，而且包括网下信息的安全。现在谈论的网络安全，主要是是指面向网络的信息安全，或者是网上信息的安全。

安全隐患

1．internet是一个开放的、无控制机构的网络，黑客（hacker）经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

2．internet的数据传输是基于tcp/ip通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

3．internet上的通信业务多数使用unix操作系统来支持，unix操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

4．在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄露等，在应用层支持的服务协议中是凭着君子协定来维系的。

5．电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息会存在着很大的危险。

6．计算机病毒通过internet的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名ftp文件传送、也可以通过邮件和邮件的附加文件传播。

攻击形式

主要有四种方式中断、截获、修改和伪造。

中断是以可用性作为攻击目标，它毁坏系统资源，使网络不可用。

截获是以保密性作为攻击目标，非授权用户通过某种手段获得对系统资源的访问。

修改是以完整性作为攻击目标，非授权用户不仅获得访问而且对数据进行修改。

伪造是以完整性作为攻击目标，非授权用户将伪造的数据插入到正常传输的数据中。

解决方案

1．入侵检测系统部署

入侵检测能力是衡量一个防御体系是否完整有效的重要因素，强大完整的入侵检测体系可以弥补防火墙相对静态防御的不足。对来自外部网和校园网内部的各种行为进行实时检测，及时发现各种可能的攻击企图，并采取相应的措施。具体来讲，就是将入侵检测引擎接入中心交换机上。入侵检测系统集入侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件，作为网络管理员事后分析的依据；如果情况严重，系统可以发出实时报警，使得学校管理员能够及时采取应对措施。

2．漏洞扫描系统

采用最先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。

3．网络版杀毒产品部署

在该网络防病毒方案中，我们最终要达到一个目的就是：要在整个局域网内杜绝病毒的感染、传播和发作，为了实现这一点，我们应该在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能。

网络通信具有全程全网联合作业的特点。就通信而言，它由五大部分组成：传输和交换、网络标准、协议和编码、通信终端、通信信源、人员。这五大部分都会遭到严重的威胁和攻击，都会成为对网络和信息的攻击点。而在网络中，保障信息安全是网络安全的核心。网络中的信息可以分成用户信息和网络信息两大类。

用户信息

在网络中，用户信息主要指面向用户的话音、数据、图像、文字和各类媒体库的信息，它大致有以下几种：

一般性的公开信息：如正常的大众传媒信息、公开性的宣传信息、大众娱乐信息、广告性信息和其他可以公开的信息。

个人隐私信息：如纯属个人隐私的民用信息，应保障用户的合法权益。

知识产权保护的信息：如按国际上签订的《建立世界知识产权组织公约》第二条规定的保护范围，应受到相关法律保护。

商业信息：包括电子商务、电子金融、证券和税务等信息。这种信息包含大量的财和物，是犯罪分子攻击的重要目标，应采取必要措施进行安全防范。

不良信息：主要包括涉及政治、文化和伦理道德领域的不良信息，还包括称为“信息垃圾”的无聊或无用信息，应采取一定措施过滤或清除这种信息，并依法打击犯罪分子和犯罪集团。

攻击性信息：它涉及各种人为的恶意攻击信息，如国内外的“黑客”攻击、内部和外部人员的攻击、计算机犯罪和计算机病毒信息。这种针对性的攻击信息危害很大，应当重点进行安全防范。

保密信息：按照国家有关规定，确定信息的不同密级，如秘密级、机密级和绝密级。这种信息涉及政治、经济、军事、文化、外交等各方面的秘密信息，是信息安全的重点，必须采取有效措施给予特殊的保护。

网络信息

在网络中，网络信息与用户信息不同，它是面向网络运行的信息。网络信息是网络内部的专用信息。它仅向通信维护和管理人员提供有限的维护、控制、检测和操作层面的信息资料，其核心部分仍不允许随意访问。特别应当指出，当前对网络的威胁和攻击不仅是为了获取重要的用户机密信息，得到最大的利益，还把攻击的矛头直接指向网络本身。除对网络硬件攻击外，还会对网络信息进行攻击，严重时能使网络陷于瘫痪，甚至危及国家安全。网络信息主要包括以下几种：

通信程序信息：由于程序的复杂性和编程的多样性，而且常以人们不易读懂的形式存在，所以在通信程序中很容易预留下隐藏的缺陷、病毒，隐蔽通道和植入各种攻击信息。

操作系统信息：在复杂的大型通信设备中，常采用专门的操作系统作为其硬件和软件应用程序之间的接口程序模块。它是通信系统的核心控制软件。由于某些操作系统的安全性不完备，会招致潜在的入侵，如非法访问、访问控制的混乱、不完全的中介和操作系统缺陷等。

数据库信息：在数据库中，既有敏感数据又有非敏感数据，既要考虑安全性又要兼顾开放性和资源共享。所以，数据库的安全性，不仅要保护数据的机密性，重要的是必须确保数据的完整性和可用性，即保护数据在物理上、逻辑上的完整性和元素的完整性，并在任何情况下，包括灾害性事故后，都能提供有效的访问。

通信协议信息：协议是两个或多个通信参与者（包括人、进程或实体）为完成某种功能而采取的一系列有序步骤，使得通信参与者协调一致地完成通信联系，实现互连的共同约定。通信协议具有预先设计、相互约定、无歧义和完备的特点。在各类网络中已经制定了许多相关的协议。如在保密通信中，仅仅进行加密并不能保证信息的机密性，只有正确地进行加密，同时保证协议的安全才能实现信息的保密。然而，协议的不够完备，会给攻击者以可乘之机，造成严重的恶果。

电信网的信令信息：在网络中，信令信息的破坏可导致网络的大面积瘫痪。为信令网的可靠性和可用性，全网应采取必要的冗余措施，以及有效的调度、管理和再组织措施，以保证信令信息的完整性，防止人为或非人为的篡改和破坏，防止对信令信息的主动攻击和病毒攻击。

数字同步网的定时信息：我国的数字同步网采用分布式多地区基准钟（lpr）控制的全同步网。lpr系统由铷钟加装两部全球定位系统（gps）组成，或由综合定时供给系统bits加上gps组成。在北京、武汉、兰州三地设立全国的一级标准时钟（prc），采用铯钟组定时作为备用基准，gps作为主用基准。为防止gps在非常时期失效或基准精度下降，应加强集中检测、监控、维护和管理，确保数字同步网的安全运行。

网络管理信息：网络管理系统是涉及网络维护、运营和管理信息的综合管理系统。它集高度自动化的信息收集、传输、处理和存储于一体，集性能管理、故障管理、配置管理、计费管理和安全管理于一身，对于最大限度地利用网络资源、确保网络的安全具有重要意义。安全管理主要包括系统安全管理、安全服务管理、安全机制管理、安全事件处理管理、安全审计管理和安全恢复管理等内容。

**网络安全的教案篇十二**

1、了解学生的网络安全意识和水平

2、让学生从整体上把握网络概念,有个大概的了解

课前引言：信息时代的到来,越来越多的人平常的学习、工作和生活已经离不开计算机网络,随之出现的是各类网络安全问题。一些人用网络工作、学习,但总是有一些人出于赚钱、显示自己的计算机水平,对网络进行破坏,使平常的工作等受到很大的影响。通过本课程学习,希望同学们能对网络安全有个总体上的认识,在例如木\*\*检测、黑客技术、计算机网络病毒、漏洞检查和防范等方面有个较为细致的掌握,通过理论和实际操作结合,包括一些常用的安全软件的使用等,使同学们在老师的指导下由浅入深系统地学习网络安全的相关知识。

1、本课程没有合适的教材,希望大家能勤做笔记,结合网上教案,认真做好听课及复习工作。

2、除了上课认真听讲,这门课更依靠大家的自觉性,通过各类途径查看并学习相关资料,多动手动脑勤做笔记,以便以后解决类似问题。

3、适时开展一些交流讨论会,分享一段时间来大家的所得。

1、学生分组讨论的形式了解学生能网络安全的理解、兴趣及掌握程度。

分两组同学分别就木马及最近网络上流行的“熊猫烧香”病毒进行10分钟左右的讨论,然后每组选一个代表进行发言。老师根据情况作一个小结。

2、老师通过小结使大家对木马以及“熊猫烧香”这种病毒有个较为准确的理解。

木马：“木马”程序是目前比较流行的病毒文件,与一般的病毒不同,它不会自我繁殖,也并不“刻意”地去感染其他文件,它通过将自身伪装吸引用户下载执行,向施种木马者提供打开被种者电脑的门户,使施种者可以任意毁坏、窃取被种者的文件,甚至远程操控被种者的电脑。

网络安全的概念：信息安全指对信息的机密性、完整性和可获性的保护,即面向数据的安全。互联网出现以后,信息安全除了上述概念以外,其内涵又扩展到面向用户的安全。综合而言,网络安全包括物理安全威胁、操作系统的安全缺陷、网络协议的安全缺陷、应用软件的实现缺陷、用户使用的缺陷和恶意程序等6个方面的威胁。

安全漏洞从理论上说,安全漏洞就是软件中存在的意外功能分枝,通过安全漏洞,可以让软件做软件设计人员意想不到的事情。

1、实例：“支付宝”支付宝控件原本的设计功能是加密通信,保护用户的通信安全,但是由于存在安全漏洞,也可以被利用来执行任何功能,譬如运行一个盗取银行帐号的木马。木马要想在用户的计算机上运行,一个主要的手段就是利用安全漏洞。而目前被利用最多的,就是各种各样的ie控件漏洞。2024年2月8日支付宝升级了控件,修复了上述漏洞,只要安装了有漏洞的控件,不管你用不用支付宝,是否登陆支付宝,都会受到漏洞的威胁。因为任何网页都可以通过放置特殊的代码来调用这个控件。但是用支付宝服务本身反而并不会有危险——因为支付宝网站本身并不会包含这种恶意代码。

2、怎么防止中木马和病毒

目前所有杀毒软件主要的工作原理都是基于特征识别。什么叫特征识别呢?通俗来说,就是掌握一份坏人的花名册,根据花名册去找。如果这个病毒或者木马刚刚被写出来,还没有“案底”,不在花名册上,杀毒软件就识别不出来。某些杀毒软件虽然也有些不依赖于花名册的高级识别功能,但是这种功能并不百分之百可靠。更何况,现在的病毒木马作者,在写完程序后,都会先用杀毒软件测试一下,确认不会被检测出来才放出去。那么杀毒软件岂不是没用了么?不是。各种杀毒软件能帮你解决大多数的麻烦,但不能指望它百分之百可靠。

黑客是只有极少数人能够进入的行业,每一名黑客都有一段残酷的青春,绝大部分人对计算机汇编语言产生兴趣的年代都在中学或者大学一二年级,随后,他们必须花费大量的时间进行基础学习,从而迈进黑客进阶之路,绝大部分的人难以逾越这个挑战而选择放弃。黑客也是一个只有年轻人才能从事的行业,中国黑客中那些自称老人的`老一辈黑客年龄不过30岁,而新生一代也许还不到20岁。

“特洛伊木马程序”技术是黑客常用的攻击手段。它通过在你的电脑系统隐藏一个会在windows启动时运行的程序,采用服务器/客户机的运行方式,从而达到在上网时控制你电脑的目的。黑客利用它窃取你的口令、浏览你的驱动器、修改你的文件、登录注册表等等。

此外黑客也常利用系统的漏洞进行一些破坏性攻击。这些在以后的教学中会慢慢和大家一起学习。

本次课主要通过身边的实例让同学们对网络安全有个整体上的了解,以后的教学中将对黑客、木马、安全漏洞、计算机病毒等作进一步的学习,希望大家能好好配合、为以后的工作学习打下良好的基础！

**网络安全的教案篇十三**

1.培养学生正确上网，文明上网的习惯。

2.教育学生自觉拒绝网络不良信息。

3.倡导文明上网，争做一个文明的网上公民。

网络的危害及如何远离网吧

多媒体课件

一、导入

1.同学们，你们喜欢玩电脑吗？上过网的请举手；“你们平时上网都做些什么？”（学生回答）

2.师述：看来，同学们利用网络做了许许多多的事情。通过网络我们能查资料，玩游戏，聊天，看天气预报，看新闻，看小说，发邮件，听音乐，看电影，购物等。给我们的工作和生活带来了便利,网络世界是精彩的，它丰富了我们的生活。但是如果不会科学、安全、合理的上网,同样会也给我们带来了危害。这就是我们今天要学习的内容-----小学生网络安全教育（板书课题）。

二、教学过程

（一）警钟长鸣

同学们，你们平时都在什么地方上网？你每周的上网时间大约是几小时呢？（请同学们说一说）适度的上网对我们来说是可以的。如果经常长时间的上网，好不好呢？那么长时间的上网会对我们未成年人有哪些影响呢？我们一起看一看真实的案例。

（二）网络的危害

1.请同学们在小组内进行交流讨论，并请小组长记录下来。

2.学生发言。

3.老师补充并总结。

（1）危害身心健康

（2）导致学习成绩下降

（3）弱化道德意识

（4）影响人际交往能力

（5）影响人生观、价值观

三、老师建议：

上网前定好上网目标和要完成的任务；

2.根据任务，合理安排上网时间长度。

3上网前最好经过家长的同意。

4.上网时间最多不要超过2小时。

5.一定要上健康的网页，如中国儿童资源网，六一儿童网，腾讯儿童，里面有很多丰富的内容。

（一）什么叫“网瘾”？（板书）

你知道什么叫网瘾吗？

“网瘾”可谓互联网成瘾综合征（简称iad）。即对现实生活冷漠，而对虚拟的网络游戏、情爱、信息等沉溺、痴迷。

（二）如何判断上网成瘾呢？

主要表现为，一到电脑前就废寝忘食；常上网发泄痛苦、焦虑等。以上症状是上网综合征的初期表现。更有甚者表现为上网时身体会颤抖，手指头经常出现不由自主敲打键盘的动作，再发展下去则会导致舌头与两颊僵硬甚至失去自制力，出现幻觉。

防止网瘾最重要的一条就是严格控制上网时间，每天以不超过两小时为宜。儿童青少年处于发育时期，更应严格节制。

（三）未成年人上网指导

同学们，我们知道了“网瘾”及网瘾的危害，大家说说你今后应该怎样对待上网呢？

1.请同学们在小组内进行交流讨论，并请小组长记录下来后派代表发言。

2.老师补充并总结。

（1）遵守网络规则，保护自身安全。

（2）学会目标管理和时间管理，提高上网效率。

（3）积极应对生活挫折，不在网络中逃避。

（4）要诚实友好交流?，不侮辱欺诈他人。?

四、小结

同学们已经做出了自己的承诺，我相信同学们从现在起一定能做到“远离网吧，安全文明上网，。”希望大家课下把学习到的网络安全知识广泛宣传，人人争做安全小卫士。

本文档由028GTXX.CN范文网提供，海量范文请访问 https://www.028gtxx.cn