# 网络安全安全教案中班 网络安全教案(精选15篇)

来源：网络 作者：静谧旋律 更新时间：2024-06-24

*作为一名教师，通常需要准备好一份教案，编写教案助于积累教学经验，不断提高教学质量。怎样写教案才更能起到其作用呢？教案应该怎么制定呢？这里我给大家分享一些最新的教案范文，方便大家学习。网络安全安全教案中班篇一网络安全是指网络系统的硬件、软件及...*

作为一名教师，通常需要准备好一份教案，编写教案助于积累教学经验，不断提高教学质量。怎样写教案才更能起到其作用呢？教案应该怎么制定呢？这里我给大家分享一些最新的教案范文，方便大家学习。

**网络安全安全教案中班篇一**

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

一、基本概念

网络安全的具体含义会随着“角度”的变化而变化。比如：从用户(个人、企业等)的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

二、主要特性

网络安全应具有以下五个方面的特征：

保密性：信息不甚露给非授权用户、实体或过程，或供其利用的特性。

完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

可控性：对信息的传播及内容具有控制能力。

可审查性：出现的安全问题时提供依据与手段。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、拒绝服务和网络资源非常占用和非常控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非常的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网(intranet)、企业外部网(extranet)、全球互联网(internet)的企业级计算机处理和世界范围内的信息共享和业务处理。在处理能力提高的同时，连接能力也在不断的提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络安全、应用安全和网络管理的安全等。

因此计算机安全问题，应该像每家每户的防火防盗问题一样，做到防范于未然。甚至不会想到你自己也会成为目标的时候，威胁已经出现了，一旦发生，常常措手不及，造成极大的损失。

三、它与网络性能和功能的关联

通常，安全与性能和功能是一对矛盾的关联。如果某个关联不向外界提供任何服务(断开)，外界是不可能构成安全威胁的。但是，企业接入国际互连网络，提供网上商店和电子商务等服务，等于一个内部的网络建成了一个开放的网络环境，各种安全问题也随之产生。

构建网络安全，一方面由于要进行认证、加密、监听，分析、记录等工作，由此影响网络效率，并且降低客户应用的灵活性;另一方面也增加了管理费用。

但是，来自网络的安全威胁是实际存在的，特别是在网络上运行关键业务时，网络安全是首先要解决的问题。

选择适当的技术和产品，制订灵活的网络安全策略，在保证网络安全的情况下，提供灵活的网络服务通道。

采用适当的安全体设计和管理计划，能够有效降低网络安全对网络性能的影响并降低管理费用。

全方位的安全：

访问控制：通过对特定网段、服务建立的访问控制体系，绝大多数攻击阻止在到达攻击目标之前。

检查安全漏洞：通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效。

攻击监控：通过对特定网段、服务建立的攻击监控，可实时检测出绝大多数攻击，并采取相应的行动(如断开网络连接、记录攻击过程、跟踪攻击源等)。

加密通讯：主动的加密通讯，可使攻击者不能了解、修改敏感信息。

认证：良好的认证可防止攻击者假冒合法用户。

备份和恢复：良好的备份和恢复机制，可在攻击造成损失时，较快地恢复数据和系统服务。

多幂防御，攻击者在突破第一道防线后，延缓或阻断其到达攻击目标。

隐藏内部信息，使攻击者不能了解系统内的基本情况。

设立安全监控中心，为信息系统提供安全体系管理、监控，渠护及紧急情况服务。

四、网络安全分析

1.物理安全分析

网络的物理安全是整个网络系统安全的前提。在工程建设中，由于网络系统弱电工程，耐压值很低。因此，在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害;考虑布线系统与照明电线、动力电线、通信线路、暖渔管道及冷热空渔管道之间的距离;考虑布线系统和绝缘线及接地与焊接的安全;必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。总体来说物理安全的风险主要有，地震、渴灾、火灾等环境事故;电源故障;人为操作失误或错误;设备被盗、被毁;电磁干扰;线路截获;高可用性的硬件;双机多冗余的设计;机房环境及报警系统、安全意识等，因此要尽量避免网络的物理安全风险。

2.网络结构的安全分析

网络拓扑结构设计也直接影响到网络系统的安全性。假如在外部和内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也影响在同一网络上的许多其他系统。透过网络传播，还会影响到连上internet/intrant的其他的网络;影响所及，还可能涉及金融等安全敏感领域。因此，我们在设计时有必要对公开服务器(web、dns、email等)和外网及内部其它业务网络进行必要的隔离，避免网络结构信息外漏;同时还要对外网的服务清查加以过滤，只允许正常通信的数据包到达相应主机，其它的服务在到达主机之前都应该遭到拒绝。

3.系统的安全分析

所c系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。目前恐怕没有绝对安全的操作系统可以选择，无论是microsfot的windowsnt或者其它任何商用unix操作系统，其开发厂商必然有其back-door。因此，我们可以得出如下结论：没有完全安全的操作系统。不同的用户应从不同的方面对其网络作详细的分析，选择安全性能可能高的操作系统。因此不但要选用可靠的操作绻统和硬件平台，并对操作系统进行安全配置。而且，必须加强登录过程的认证(特别是在到达服务器主机之前的认证)，确保用户的合法性;其次应该严格限制登录者的操作权限，完成的操作限制在最佳的范围内。

4.应用系统的安全分析

应用系统的安全跟具体的应用有关，它涉及面广。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，它包括很多方面。应用系统的安全是动态的\'、不断变化的。

应用的安全涉及方面很多，以目前internet上应用最为广舻e-mail系统来说，其解决方案有sendmail、netscapemessagingserver、、lotusnotes、exchangeserver、suncims等不下二十多种。其安全手段涉及ldap、des、rsa等各种方式。应用系统是不断发幕且应用类型是不断增加的。在应用系统的安全性上，主要考虑到可能建立安全的系统平台，而且通过专业的安全工具不断发现漏洞，修补漏洞，提高系统的安全性。

信息的安全性涉及到机密信息泄漏、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。在某些网络系统中，涉及到很多机密信息，如果一些重要信息遭到窃取或破坏，它的经济、社会影响和政治影响都是很严重的。因此，对用户使用计算机必须进行身份认证，对于重要信息的通讯必须授权，传输必须加密。采用多幂次的访问控制与权限控制手段，实现对数据的安全保护;采用加密技术，保证网上传输的信息(包括管理员口令与帐户、上传信息等)的机密性与完整性。

5.管理的安全风险分析

管理是网络中安全最最重要的部分。责权不明，安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其它一些安全威胁时(如内部人员的违规操作等)，无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多幂次的记录，及时发现非法入侵行为。建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是制定健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络便成为了首要任务。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是校园网建设过程中重要的一环。

五、网络安全措施

1.安全技术手段物理措施：例如，保护网络关键设备(如交换机、大型计算机等)，制定严格的网络安全规章制度，采取防辐射、防火以及安装不间断电源(ups)等措施。

访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限，等等。

数据加密：加密是保护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。防止计算机网络病毒，安装网络防病毒系统。

网络隔离：网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网闸实现的。

隔离卡主要用于对单台机器的隔离，网闸主要用于对于整个网络的隔离。

其他措施：其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。近年来，围绕网络安全问题提出了许多解决办法，例如数据加密技术和防火墙技术等。数据加密是对网络中传输的数据进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。防火墙技术是通过对网络的隔离和限制访问等方法来控制网络的访问权限。

2.安全防范意识

拥有网络安全意识是保证网络安全的重要前提。许多网络安全事件的发生都和缺乏安全防范意识有关。

网络安全知识资料

**网络安全安全教案中班篇二**

一、活动目的：

以新的《中学生日常行为规范》中的第二十条中的“文明上网，不进入不适宜中学生的活动的场所，不沉溺游戏”为主题，结合本班学生实际来进一步讨论：中学生上网是利大于不弊还是弊大于利?从中让学生切身体会到行为规范的点点滴滴，以及让我们这个主题能够灌输到学生的认知头脑中去，促进他们的是非辨别能力，并让网络的利广泛运用到平时的学习中去。

二、活动形式：

ppt讲解，辩论，宣誓

三、活动过程：

1、谈话导入，揭示主题。

2、看ppt

我们现在所说的网络也就是internet，那么网络到底给我们的生活带来了哪些便利呢?(呈现图片)

3、组织辩论：

看了这么多，相信大家对internet有了更深入的了解，近几年来，在互联网快速发展的同时，出现了大量网吧，网吧的出现为普及网络知识起到了积极的推动作用，虽然网吧给人们提供了快捷的信息和崭新的交流平台，但是随着互联网信息垃圾的不断出现，网吧的负面效应也日益显现。那么，我们中学生上网到底是是利大于弊还是弊大于利呢?请同学们来说说自己的观点。

1，2，3组为正方：上网利大于弊

4，5，6组为反方：上网弊大于利

4、班主任总结。

网络是把“双刃剑”既有好的一面，也有不健康的一面。对于网络，我们要保持敏锐的洞察力和是非分辨能力，给自己树立一道坚不可催的防护墙。我们要从网上寄去一些健康的、进步的、积极向上的有利信息，为我们的学习和生活服务，要让网络为我们的健康成长积蓄更多的力量!

如何正确上网呢?

1、提高自身素质，抵制网络诱惑

2、发现不良信息，通知朋友共同抵制，并报告有关部门

3、千万不要在父母或监护人不知道的情况下与陌生人约会

4、不要在网上轻易透露与自己身份有关的信息资料

5、不要轻信网上朋友的信息资料。

**网络安全安全教案中班篇三**

时代发展，科技进步，人们的生活水平和质量不断提高，愈来愈好。网络的普及，给人们日益增长的物质文化需要插上了翅膀。网民根据自己的需要，可以在网络上找到自己的.天地。可是，网络到底好不好，回答是肯定的，利大于弊。但是，任何事情都要一分为二，具体情况具体分析。什么事情超过了一定的限度，就会走向反面，也就是人们常说的，物极必反。倘若一味沉溺网络，势必给人们的生活、工作和学习带来不利因素，会产生这样那样的问题，甚至会走极端，这绝不是危言耸听。本次班会组织同学们了解自己，知道良好利用网络的方法以及正确与网络交朋友的方法，帮助同学们了解自己并且促进自我身心健康发展。

1.将班级分成甲乙两组，进行辩论。

2.准备8道心里测试题。

3.小品《远离网吧》。

4.寻求帮助如何戒掉网瘾的方法。

活动1：各抒己见，甲乙辩论赛

在班长的领导下班级分成了两组。甲组同学认为网络利大于弊，而乙组同学认为网络弊大于利，双方各抒己见进行辩论。甲组的a同学首先站起来说道：“我方坚信：中学生上网利大于弊。21世纪将是计算机网络时代，今日的莘莘学子将担任未来社会的栋梁。了解和掌握计算机网络知识，就是闯荡未来信息时代的最强有力的武器。！”乙组的a同学站起来反驳说道：“刚才对方辩友滔滔不绝，无非是向在座各位展示了网络在信息交流方面的快捷性和方便性。但在美国权威杂志《今日美国》的调查表明：86%被调查的教师、图书管理员以及电脑管理人员相信，孩子们使用因特网不会提高他们的课堂成绩。”……在辩论中，同学们说出了自己的心里话。

活动2：心理测试，让同学了解自己

班长将8道心里测试题打在了班中的多媒体上，并让每位同学都拿出一张空白的纸，让他们在纸上表上序号，如果你认为是就在序号旁写上是，最后把纸交给班长（不记名）。只见有的同学抓耳挠腮、东张西望，不知道该如何回答，而有些同学只是埋头写，并把自己的纸藏在胸前。最后班长将纸收起后看了看，发现有些同学还是有网瘾的隐患的。在8到测试题前，同学们重新审视了自己，决定要改变！

活动3：小品《远离网吧》

两位同学大摇大摆地走上了讲台。为同学们表演了小品--《远离网吧》。两位同学展现了自己超高的演技，把小品中的tom表现的淋漓尽致。听完小品后，同学们也在欢声笑语中明白了网络带来的坏处以及只要下定决心就可以戒掉网瘾。看完了小品，有些同学们也对自己戒掉网瘾有了更大的信心！

活动4：寻找方法，共同进步

在前几个活动中，同学们都重新审视了自己。接下来就是如何改掉网瘾的办法了。这时，老师走了过来，微笑地对同学们说：“同学们，其实网瘾并不可怕。在这里，我教给大家如何改掉网游：首先别急着一下子戒掉网瘾，那是不可能的，因为你已经形成一定程度的依赖！

“小a同学原本每天放学都要打电脑、去网吧、不做作业，现在已经减少到每天只玩一小时，而且也开始做作业了”

“小b同学的父母认为网络会影响学习便没有给小b安装网络，使小b一些需要查找资料的作业无法完成。经过这次班会，小b同学与父母商量后，装上了宽带。现在小b可以更高效率的完成作业了”

“小c同学由于网络游戏和父母闹矛盾了，有了分歧。经过班会讨论，小c和父母都明白了自己身上的不足，互相改正、理解，现在他们又和好如初了”

正确地使用网络，劳逸结合。小a小b小c都有了慢慢的改变，学习成绩也慢慢地提高了，和父母、同学的关系也越来越好了。

温馨提示：

各位网迷们，你们知道该怎么做了吗？只要保持一个正常的心态在网络活动，是有益的，毕竟网络总体上是好的，有国家有关职等部门监管着，有许多有良知的网络经营者遵守着游戏规则，有众多的网民洁身自好。但是，沉溺网络是绝对有害的，无度则迷，迷之毁己。让我们一起健健康康地成长！不做网络的“奴隶”！

**网络安全安全教案中班篇四**

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。

**网络安全安全教案中班篇五**

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。

**网络安全安全教案中班篇六**

市林业局目前运行网站为xx林业局信息网，为了做好网络安全运维，我局通过建立组织机构，制定了网络安全保障方案，加大网络巡查频率制定工作纪律等手段，确保网络正常运行，主要方式如下：

一、成立组织机构

市林业局成立了以局长、党组书记万瑞年为组长，各科室负责人为成员的网络安全保障小组，全面开展我局网站网络与信息安全工作，采用层层分解，责任到人的模式，把重点工作分解到人，确保任何网络故障和网络攻击，相关人员能够迅速开展应急处理，防止问题扩大。

二、制定了网络安全保障方案

为做好我局网络与信息安全工作，局长办公会特别强调要求各科室重视重要设备管理、重要信息数据备份，并制定网络安全管理制度和应急处置预案，并随时与省厅网络平台上报网络运营情况，确保网络安全工作都落到实处。

三、加大网络巡查频率制定工作纪律

市林业局为保障网络安全不出问题，安排专人负责网络巡查工作，实施每天早、晚最少巡查二次，确保突发重大网络事件及时有效处置。时刻与省林业厅保持联系，省林业厅已要求网络平台代维公司进行逐个安全加固，并定期对各市县开展网络安全培训，部署防病毒acl策略，封闭病毒端口和数据流，保障用户数据不容易被扫描到。市林业局网络安全保障小组要求局工作人员登陆网站电脑需要全部安装终端杀毒软件和防火墙，升级到最新的病毒库，并强调使用人员每天杀毒，确保电脑无病毒。

四、做好网络安全应急工作

8月份，市林业局网站被国家安全检查信息共享平台监测到http参数污染等安全漏洞，严重影响了网站安全运行，对于出现了网页篡改这种严重的为害网络安全事件，我局领导高度重视，立刻召集相关科室负责人，启动网络安全应急预案，由于我局站隶属省林业厅后台管理，我们立即上报省厅，发函至林业厅办公室，请求网络运维公司彻查原因，并迅速消除了隐患。自此我局引以为戒，为避免此类事件的再次发生，局领导要求全局每位工作人员都要调高警惕，时刻关注网络安全，一旦发现网络受攻击，及时反馈网络公司，及时进行清理处置。

**网络安全安全教案中班篇七**

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。

让学生对互联网有一个正确的`态度，正确利用网络。

提高网络自制力，让学生有节制的上网。

讲授法，讨论法，演讲法。

1课时

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。

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。

众所周知，我们在家里，只要一根网线，甚至不要线，我们就可以方便的与来自各地的人们交谈，但是你从不知道他的真实状况，青少年对社会没有任何经验，容易上当受骗，因此家长应该讲清网络的虚拟，告诉孩子辨别网络骗局的技巧，使孩子树立正确的上网观念。

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。

**网络安全安全教案中班篇八**

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。

**网络安全安全教案中班篇九**

1、网络安全作为学校安全教育之一，通过班会使迷恋网游的学生从思想上深刻认识网络的危害，调节自己的心态，引导到迎战中考的学习中去。

2、针对同学们对电脑游戏的热爱与迷恋，想以此正确引导，疏导同学们对游戏的把握度。

3、使学生认识到作为一名合格中学生，处在当今的网络时代，我们更应该利用网络资源，搞好我们的学习，提高自身素质。

课前制作赠言小卡片。

班会活动

一、开场导语

师：同学们今天我们班会的主题是有关网络的话题。你们上网吗？你们认为上网有益还是有害？结合你们的体验谈谈你们的看法。

二、畅谈网络

甲：我经常上网，网络提供给我们沟通的平台。

乙：网上有很多信息、知识，可以增长我们的知识，开扩视野。

丙：网络打发了闲暇时光，网上有很多好玩的东西。

师：同学们都讲到了网络给我们的生活带来的好处，但利用网络要合理，如果沉迷于网络那将会造成什么样的危害呢？现在请同学们看这些数据。

（幻灯片展示）：据北京市150多位政协委员历时4个月完成的调查报告显示：中学生上网网达到81.3%，有七成学生网民沉迷于网上聊天，有四成多光顾网站，互联网成为一部分青少年名副其实的“电子”。

三、案例分析

师：网络是一只邪恶的怪兽，它拥有令人惧怕的三大魔爪，如网络游戏，网络上的不良信息，网络聊天。其中对同学诱惑最大的是网络游戏，我们来看看一些沉迷于网络游戏的故事。（幻灯片展示）

同学们看了之后都很有感触和启发。

四、同学互动

师：我知道我们班上也有个别同学沉迷于网络游戏，现在你们知道了网络的危害，为了让那些沉迷于网络的同学能从网络的诱惑中走出来，健康文明地运用网络，快乐生活，同学们，请你们拿起手中的.笔，在制作的小卡片上写下自已鼓励他们的话。

同学们纷纷动起笔来，写完之后把小卡片贴在事先布置好的墙上，以此来激励同学们。

五、结束语

同学们的行为令人鼓舞，希望从此以后我们每一位同学都能，从我做起；遵纪守法，文明上网；自尊自爱，远离网害；珍惜青春，发愤学习；自强自立，做一个健康文明的中学生，为此老师希望大家从以下几个方面来努力：

（1）、自我提醒。把上网的好处与坏处分别写在一张纸上，贴在房间的显眼处，每天默念几遍。

（2）、自我暗示。一有上网的念头，反复自我暗示。如：“现在应该学习，等周末再上等。

（3）、放松训练。当网瘾发作时，常出现紧张、不安等情绪，此时可做些深呼吸等放松练习。

（4）、注意力转移。如欣赏自己喜欢的音乐，做自己感兴趣的事情，如：散步、郊游等。

（5）、规范生活。重新规范自己的作息时间，让自己更充实。

**网络安全安全教案中班篇十**

为提高我镇网络信息安全突发事件应急反应能力，加强网站、网络信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网站网络与信息安全突发事件的危害，维护正常办公秩序，特制定本方案。

根据上级相关文件精神，为妥善应对和处置我单位网站及重要信息系统的突发事件，确保重要信息系统安全、稳定、持续运行，防止造成重大损失和影响，进一步提高网络与信息系统应急保障能力，以维护我镇网站、重要业务系统网络及设备的正常运行为宗旨。按照“预防为主，积极处置”的原则，进一步完善应急处置机制，提高突发事件的应急处置能力。

应急演练工作组

组长：

成员：

职责：负责信息系统突发事件应急演练的指挥、组织协调和过程控制；报告应急演练进展情况和总结报告，确保演练工作达到预期目的。负责信息系统突发事件应急演练的具体工作；对信息系统突发事件应急演练业务影响情况进行分析和评估；收集分析信息系统突发事件应急演练处置过程中的数据信息和记录；向应急指挥部报告应急演练进展情况和事态发展情况。

（一）演练时间

20xx年11月30日举行应急演练。

（二）演练内容

网络与信息安全突发事件应急反应与处置。

（三）演练目的.

突发事件应急演练以提高相关工作人员应对突发事件的综合水平和应急处置能力，以防范信息系统风险为目的，建立统一指挥、协调有序的应急管理机制和相关协调机制，以落实和完善应急预案为基础，全面加强信息系统应急管理工作，并制定有效的问责制度。坚持以预防为主，建立和完善信息系统突发事件风险防范体系，对可能导致突发事件的风险进行有效地识别、分析和控制，减少重大突发事件发生的可能性，加强应急处置队伍建设，提供充分的资源保障，确保突发事件发生时反应快速、报告及时、措施得力操作准确，降低事件可能造成的损失。

（一）学习教育。组织工作人员学习网络信息安全事件应急方案，认真学习和模拟演练应急预案，提高每个工作人员对于突发事件的应急处置意识；熟悉在突发事件中各自的职责和任务，保证网站及各业务系统的安全稳定运行。

（二）演练工作组全面负责各项准备工作的协调与筹划。明确责任，严格组织实施演练活动，确保演练活动顺利完成，达到预期效果。

（三）应急演练组要提前在中心机房要做好充分准备，在演练前一天准备好所有应急需要联系的电话号码，检查网络线路，计划好断电点，演练时模拟网络信息安全突发事件；并按演练背景做好其它准备。

（一）工作组组长讲解演练知识及演练过程中的注意事项，并与其他相关同事一起详细了解应急预案。

（二）按照预定发生突发事故的时间表，组长逐项发出演练通知；

（三）参与部门及人员。把演练当成实战，认真对待。

（四）演练预设场景

本次演练预设场景为网络技术中心服务器感染计算机病毒。

场景：20xx年11月30日上班后，发现部分网络不通，网站后台管理系统都无法打开，并且网站前台页面访问速度缓慢，立即报告至技术维护部门管理员，技术维护部门人员立即将此情况报告应急演练指挥部。指挥部启动相关应急预案并组织人员进行故障排除，对服务器进行病毒查杀后，网络故障排除，网络恢复正常，网站可正常访问、后台管理可正常登陆并进行信息工作。

1、加强领导，确保演练工作达到预期目的。在指挥部的统一部署下，各部门人员要高度重视，提高认识，积极参加，确保演练效果。

2、技术维护部门调整好工作，确保全体人员参加，增强自己处理突发事件的能力技能。

3、完善规章制度，强化责任制的落实。演练结束后，网络应用科要对这次演练活动进行认真的总结，针对演练中出现的问题要及时进行整改，设备需要更新的立即请示行领导进行解决，制度不完善的立即着手完善，对于各岗位的责任制要再次加以明确和落实。

演练结束后，工作组要对演练进行总结，针对演练中出现的问题要及时汇总讨论并进行整改。

文档为doc格式

**网络安全安全教案中班篇十一**

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。

**网络安全安全教案中班篇十二**

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！

**网络安全安全教案中班篇十三**

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。

**网络安全安全教案中班篇十四**

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。

**网络安全安全教案中班篇十五**

(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。

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