在网络快速发展的今天，计算机已经成为人们生活中不可或缺的小助手，但是随之而来的计算机网络安全问题却需要我们的重点关注和防范。

计算机网络之所以出现安全问题，是因为受到网络各种威胁，从而引发一些网络安全事故。网络面临的主要威胁有：1.系统漏洞。计算机网络系统本身的漏洞会引发安全维修，比如我们常见到的计算机网络补丁，就是要提醒要定期对系统漏洞进行修复，从而警惕出现安全隐患。2.物理威胁。这方面的威胁主要来自身份识别出现差错、偷窃行为、间谍行为等。由于受到不法分子侵犯，造成计算机网络受到物理威胁。3.身份鉴别威胁。主要是指在进行计算机平台登录或者各种账号登录时出于保护信息严防泄密的目的从而设置一定的访问权限，包括设置用户名和密码，如果忘记或者系统不完善就会造成信息泄密，产生网络威胁。4.网络终端链接出现故障，比如进行拨号上网时密码被泄露或者在公共场所进行无线局域网查找等造成的信息泄露等，从而产生的网络安全维修。5.受到有害程序的维修。有害程度包括病毒、木马、下载或者更新等，计算机病毒是全球关注的计算机网络难点问题，受到病毒侵害或者攻击，严重时甚至引发整个系统崩溃，并且病毒侵犯都是隐蔽的、强大的、极具破坏力的、潜伏期很长，很难提前预见。

随着数字化时代的不断推进，计算机的应用已经融入了人们的日常生活中。然而，数字化的快速发展也为逐渐开放的网络带来了安全问题。网络安全，也就是一些不法分子通过网络对网络系统的硬件进行攻击，进而窃取、篡改用户的信息和[资料](http://www.ruiwen.com/ziliao/" \t "_blank)，甚至有些黑客会通过网络进行诈骗和勒索。进入新世纪以来，有关网络安全的问题开始逐渐增加，在无形中对人们的生活造成了一定的影响，同时也对企业的财产和正常运营造成了影响。目前，鉴于网络系统的复杂性，想要彻底解决网络安全问题几乎不可能，所以，广大用户必须充分认识到网络安全问题的严重性，并充分做好防范措施。

计算机网络安全是指运用各种网络管理技术从而保证网络环境安全、数据完整保密等，进而实现计算机网络稳定高效运行。计算机技术更新速度越来越快，对计算机网络安全技术也提出了更多的挑战，加上人们对于计算机网络使用的范围和频率越来越高，因此做好计算机网络安全技术研究非常重要。计算机网络安全包括四个方面，信息安全、运行安全、物理安全和软件安全，也可以分为两大方面信息安全和控制安全。信息安全主要是指计算机网络中所有的存储信息和传输数据的安全，具体功能包括信息是否隐蔽，信息是否能够被随意修改。运行安全是指计算机网路系统中的各个子系统是否能够正常运行。物理安全主要是指计算机的各类硬件、存储介质以及外部环境等涉及计算机硬件相关的设施是否安全。软件安全是指计算机网络相关的各类服务器、主机等软件安全性能指标。计算机网络安全从另一个层面上可以分为信息安全和控制安全两大类。信息安全是基础，控制安全是关键。信息安全的内容主要包括计算机网络各类信息的完整性、可靠性和保密性；控制安全的内容包括身份认证、授权访问控制和不可否认性三方面。

　　网络安全的特点是网络系统的保密性，而通过网络的信息传递一旦遭到破坏就打破了其保密性的特点。通常导致信息泄露的途径有：网络监听、非法授权进入、流氓软件、钓鱼网站等。一旦用户被盯上，这一过程将会在不知不觉中进行，用户的信息会持续泄露，直至发现后进行修复漏洞。信息篡改是指不发分子通过网络接入的方式，对用户计算机中的信息进行修改，或者通过截取用户信息的传递进行修改再传递给用户，这也是大家所熟知的网络安全中信息保密性。

　　计算机病毒具有传播迅速、传播范围广、用户损失大的特点。早在本世纪初，熊猫烧香的出现已经让广大用户欲哭无泪，随后今年的Wannacry的强大也让广大用户见识了计算机病毒的威力。计算机病毒作为引起现代计算机安全问题的主要因素，必须引起用户的重点关注。

　　随着网络技术的发展，越来越多的黑客开始活跃起来。他们拥有高超的网络技术，通过系统的漏洞或者账户的漏洞侵入用户的电脑系统，对用户的信息进行篡改、窃取。网络黑客现在正在逐渐成为一种职业，他们利用掌握的网络知识黑进用户的计算机窃取用户资源或篡改信息，最终甚至会导致用户的电脑系统瘫痪。如果国家不能对黑客进行严格的控制，将会严重影响国家的政治和经济发展。

　　作为现代通讯中的重要工具，电子邮件已经占据了人们生活工作的方方面面。而电子邮件的地址却具有公开性，同时加之用户使用不注意，也就给了不法之人可乘之机。他们将广告或者思想强制传播给他人，让人们对垃圾邮件无法拒绝。更严重的是，有人为了故意报复将垃圾信息进行大量群发导致用户的正常生活受到严重影响。这样的方式不会对系统造成破坏，但是为用户的信息泄露和信息丢失提供了便利。

　　网络防火墙是指用户通过对系统的控制加强网络之间的数据传递和访问控制。通过设置防火墙，除用户之外的外部用户就不能通过非法手段随便进入用户系统，进而对用户的信息资源进行保护，并保护计算机内部的网络操作环境不受外来环境的干扰，从而做到保护用户计算机网络安全问题。所以，用户在使用计算机时，需要注意养成良好的使用习惯，设置合理的防火墙，并且在使用网络时，尽量不要越过防火墙使用网络，这样可以最大可能的保护网络的安全性。

　　数据备份是指用户在使用计算机时，对计算机硬盘中的文件、数据进行复制，然后存储到另外的地方，这样的方式可以有效避免由于计算机被恶意攻击。用户可以选择将重要的资料备份或者选择全盘备份。这种方法是最简单有效，但是无形之中增加用户的工作量。作为企业或者个人，为避免用户的信息丢失，对数据的及时备份还是十分有必要的。

　　物理安全防护主要是指用户在使用中设置隔离网闸，他是通过多种控制功能的固态开关对主机和读写介质进行控制。物理隔离主要设置在两个独立的主机系统之间，其之间的物理连接、信息传输是相互独立的，也就隔离开了不同用户之间的连接。除此之外，物理隔离网的存在不存在其信息协议包的存在，仅仅是对固态内存的“读”、“写”两种状态。所以物理隔离网的存在使得计算机系统之间的一切连接，当一台计算机遭遇网络安全问题时，另外一台计算机不会受到影响，从而达到真正的安全。

漏洞扫描是指计算机终端对远端和本地主机安全进行分析扫描，然后查询TCP/IP协议的终端，并记录目标主机对其的响应，收集有用的信息。漏洞修复就是通过漏洞扫描后，对有缺陷的系统进行修复。漏洞扫描和修复主要是通过计算机软件完成的，这样的方式十分方便。所以，用户需要养成良好的使用习惯，定期进行系统的漏洞扫描和修复。

　在计算机网络的现实应用中，用户接触到的最多的是软件，而大多数用户为了经济而选择盗版软件。而用户这样的选择也就意味着放弃了正版软件自身的防御能力。除此之外，盗版软件的使用本来就属于违法行为，因为它是对知识产权的侵害。所以，用户在日常使用中，需要考虑使用正版软件，无论是从安全性还是对知识产权的尊重。

　　网络的快速发展，也提醒这人们要重视网络安全问题。然而，计算机网络的复杂性让计算机网络的安全防护变得较为困难。计算机网络技术发展突飞猛进，计算机网络遍及全社会各个领域、各大行业、各个角落。人类社会已经全面进入了网络时代，随之而来带来和引发的各种安全问题也日益突出，因此做好计算机网络安全课题研究是非常必要的，计算机网络安全问题迫在眉睫，急需解决，才能更好地保证计算机网络有效安全稳定运行，进而推动人类生产生活更好地发展和进步。