【全国职业教育精品课程规划教材】

Wangluo anquan yingyong yidiantong

网络安全应用一点通

◎谭建伟 赵艳莉 主编

- 如何确保银行账号之类的密码不被盗取
- 如何在网络环境中保护自己的隐私
- 如何避免电脑不受黑客攻击
- 如何使用网络安全防护产品
- 如何避免遭受网络欺骗
- 如何应对网络病毒侵害

……

解决方法尽在本书中

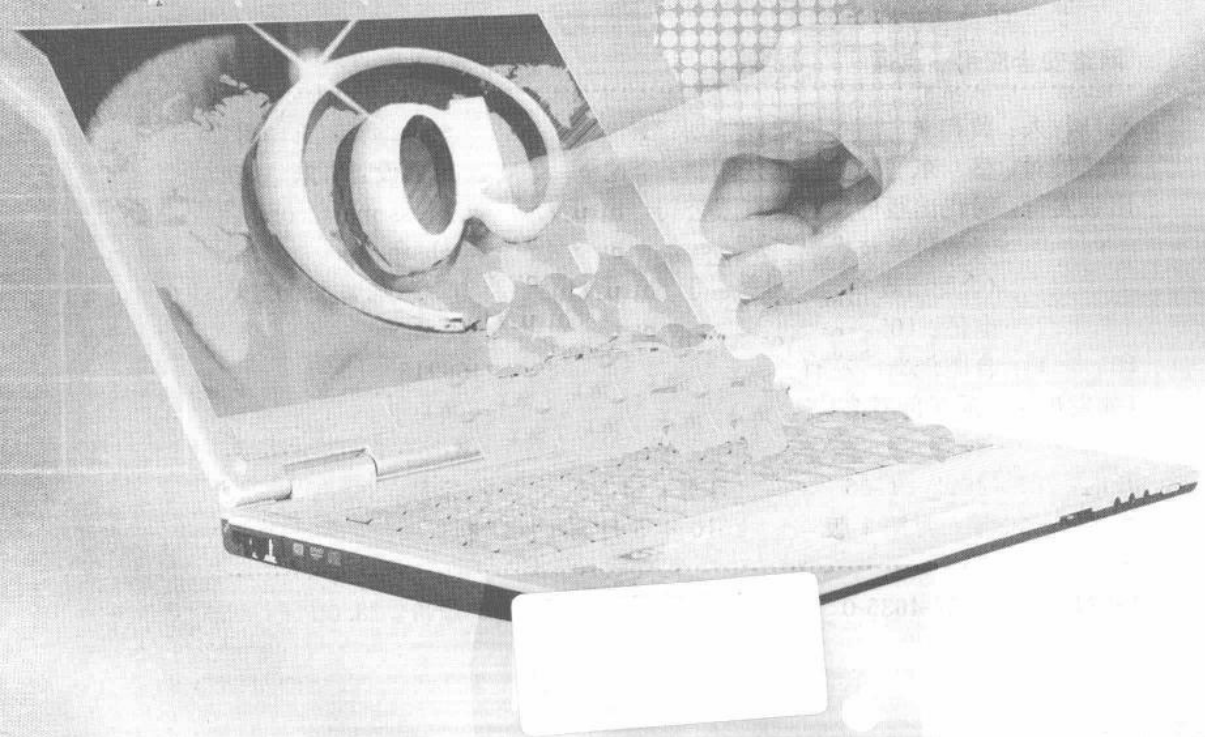
时代出版传媒股份有限公司
安徽科学技术出版社

【全国职业教育精品课程规划教材】

Wangluo anquan yingyong yidiantong

网络安全应用一点通

◎谭建伟 赵艳莉 主编



时代出版传媒股份有限公司
安徽科学技术出版社

图书在版编目(CIP)数据

网络安全应用一点通/谭建伟等主编. —合肥:安徽科学技术出版社,2010.5
ISBN 978-7-5337-4636-0

Ⅰ.①网… Ⅱ.①谭… Ⅲ.①计算机网络-安全技术 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 061416 号

网络安全应用一点通 谭建伟 等 主编

出 版 人:黄和平 选题策划:王 勇 责任编辑:王 勇
责任校对:盛 东 责任印制:李伦洲 封面设计:朱 婧
出版发行:时代出版传媒股份有限公司 http://www.press-mart.com
安徽科学技术出版社 http://www.ahstp.net
(合肥市政务文化新区圣泉路 1118 号出版传媒广场,邮编:230071)
电话:(0551)3533330
印 制:合肥创新印务有限公司 电话:(0551)4456946
(如发现印装质量问题,影响阅读,请与印刷厂商联系调换)

开本:787×1092 1/16 印张:14.75 字数:368 千
版次:2010 年 5 月第 1 版 2010 年 5 月第 1 次印刷

ISBN 978-7-5337-4636-0 定价:28.00 元

内 容 简 介

本书从技术和管理的角度讲解了计算机网络安全防护和安全应用知识，内容涉及常用的网络加密技术、防范黑客入侵技术、防范网络病毒技术、防范计算机木马技术、防范网络欺骗技术、网络安全管理技术以及相应的法律规范。书中内容相互关联又自成体系，能够满足读者全面、系统学习网络安全防护技能的需要。本书注重网络安全技术的实用性，力求做到内容简洁、通俗易懂，其中实例、习题和实际应用紧密关联，能有效提升学习者的网络安全防护技能水平。

本书可作为职业院校计算机网络安全课程的教材，也可作为普通计算机用户学习网络安全防护技能的读本。

前　言

目前，计算机网络这一人类伟大的发明已经广泛深入到社会生活的各个角落，人们利用计算机网络进行工作学习、游戏娱乐，充分享受着计算机网络带来的快乐。在计算机网络帮助人们工作、学习、生活的同时，也带来了新的威胁，产生了计算机网络病毒、信息网络盗窃、网络侵权等问题，使人们不得不关注计算机网络的安全。许多重大黑客事件表明，计算机网络存在安全漏洞，而中国计算机网络的安全防护能力尤其薄弱。据报道，中国95%以上的与因特网相连的主机曾遭受过黑客攻击。2010年1月4日至10日，国内被篡改的政府网站数量达178个，比前一周增长409%。作为计算机网络的应用者，如果不了解网络安全防护知识、不具备安全应用防护技能，很难有效、可靠地使用计算机网络，所以普及计算机网络安全知识是大势所趋。

本书是一本以网络安全基本原理为基础、以网络安全基本技术为落脚点、以贴近网络安全应用实际内容为对象的计算机网络安全技术基础教材。书中内容不涉及过多、过深的计算机安全技术理论和空洞、生涩的专业术语，但对可操作内容则列出完整的操作过程，以期对学习者提高计算机网络安全防护技能有所帮助。

全书以项目引领、任务驱动的模式编写，学习内容围绕实际工作中的任务展开，完成任务学习不但可以学会知识、技能，更能实现学习与应用的无缝对接。

全书共分9个项目。项目一全面介绍网络安全的基本概念，帮助读者建立网络安全防护理论的整体框架；项目二讲解信息加密和网络中的密码应用，帮助用户了解信息加密的概念，掌握实用的加/解密技术，保护应用环境和信息的安全；项目三介绍防治计算机网络病毒的基本方法，教会计算机用户高效率地使用防病毒软件查找、清除计算机病毒；项目四讲解防治计算机木马的基本技术，帮助用户掌握手工或使用专门工具清除计算机木马；项目五介绍防范黑客技术，旨在帮助学习者认识黑客危害，了解黑客入侵手段，学会防范黑客入侵；项目六讲解网络防骗技术，帮助学习者识别常见的网络骗局，防止上当受骗；项目七介绍了常用的防火墙和入侵检测技术，是防范黑客入侵技术的延伸，也是防范黑客入侵最基本的手段，学会使用个人防火墙对保护自己的计算机安全有极大的帮助作用；项目八讲解网络安全管理技术，帮助用户了解安全管理涉及的基本内容和方法，建立安全管理的基本思想，学会最基本的安全管理技术；项目九讲述计算机网络领域应该遵守的法律规范和可能承担的法律责任，强化法制意识，做遵纪守法的计算机网络应用者。

本书由谭建伟等编著。项目一、项目二、项目五由谭建伟编写，项目三、项目四由陈良庚编写，项目六由赵艳丽编写，项目七由王卫华编写，项目八由王长杰编写，项目九由王文平编写。潘文林、刘洁、余建普、彭玮也参与了书中相关资料收集、整理及编写工作。全书由谭建伟统稿。曲宏山对书稿进行了认真审阅，提出了许多意见和建议，全体作者对此深表感谢。

由于编者水平有限，编写时间仓促，加之对计算机网络安全问题认识、理解的局限性，难免存在错误和不当之处，敬请读者批评指正。

目　录

项目一　初识网络安全问题

网络技术的高速发展为信息传递提供了便利条件，也为扩展应用领域提供了基本保障。但是，在网络应用层次不断提高、应用领域不断扩大的同时，网络安全管理也成为全社会共同关注的话题。信息资源在网络环境传播、共享使用的过程中，一些重要的信息，如政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据甚至是游戏玩家的装备，都可能被网络“黑手”觊觎而出现窃取、篡改，也可能因网络崩溃而丢失，诸如此类的问题会影响信息产业正常有序发展，严重时甚至造成社会动荡。因此，保证网络安全、有序运行是发挥网络作用的根本。

·知识点
网络安全的含义
威胁网络安全的因素
网络安全防护的现状

任务一　了解网络安全的基本含义

从社会学的角度看，网络安全是关系国家安全、社会稳定、民族文化继承和发扬的重要问题。从技术的角度看，它又是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

任务描述

在社会信息化的进程中，网络安全是一项长期而复杂的社会系统工程，既需要网络管理者充分运用先进的管理手段和专门技术进行专项治理，也需要全社会的高度重视。或许很多人都听说、知道“网络安全”一词，但“网络安全”究竟涵盖哪些内容？哪些因素导致了网络的不安全？什么样的网络是安全的？诸如此类的问题未必人人清楚。本任务将帮助计算机用户了解网络安全的基本概念。

任务分析

了解网络安全的基本含义，是深入学习网络安全防护技术的基础，究竟网络安全涵盖哪些内容，我们可以通过以下活动来寻找答案。

- 危害网络安全案例研讨；
- 了解危害网络安全的因素；
- 理解网络安全的基本要求。

活动一 危害网络安全案例研讨

本活动了解危害网络安全事件既是揭示网络安全重要性的基础，也是提高对网络安全作用认识的重要基础。本活动将帮助计算机用户理解学习网络安全知识和提高安全防护技能的重要性。

(一)危害网络安全案例展示

案例 1　罗伯特的"蠕虫"病毒

"蠕虫"病毒的始作俑者是美国康奈尔大学计算机科学系--年级研究生罗伯特·泰潘·莫里斯。罗伯特从小就表现出了超出常人的计算机天分，在康奈尔大学享有"孤独的才华横溢的程序专家"的名声。

在 20 世纪 80 年代，苹果Ⅱ型 PC 机首次出现病毒，当时人们对计算机病毒并不十分了解，而此时罗伯特心中的目标就是编写一个无害的、能够传染尽可能多的计算机病毒。1988 年 10月，罗伯特开始了自己的计划，他一方面集中精力编写病毒程序，另一方面寻找计算机系统中可以施放病毒程序的漏洞。11 月 2 日美国东部时间晚上 7 点 30 分，罗伯特完成了病毒的编写工作。1 个小时后，他在麻省理工学院人工智能实验室的计算机上以 RTM 名登录，并下达了病毒执行指令。在罗伯特按下"Enter"键的瞬间，病毒开始扩散，几分钟之内已在网上肆虐，一台台计算机被感染病毒而陷入瘫痪。罗伯特吃完晚饭去检查病毒扩散的进展情况，发现计算机已经毫无反应。他意识到大事不妙，病毒已经失去了控制，这时才想起编写病毒时把复制参数设置错了。

这一事件使互联网上 10%的计算机受到感染，美国的直接经济损失将近 1 亿美元，罗伯特也因此受到控告，被判 3 年缓刑、1 万美元罚款和 400 小时的社区服务。

案例 2　李某倒卖股票案

李某是我国著名大学主攻证券管理专业的硕士研究生，当他看到昔日的同学一个个走入"大款"行列时，内心极度失衡，于是利用在证券公司实习的机会，了解了股票全国联网的计算机程序，开始盘算破解程序。经过几十天的苦心钻研，李某成功进入股民信息系统，众多股民的股票密码、投资金额、交易情况等核心机密在他面前一览无余。他从此开始干起低价抛售别人的股票，然后自己再去抢购的罪恶勾当，造成了股民钟某损失 17 万、郭某损失 38 万、林某损失 100 多万元的直接后果。后迫于警方压力，李某投案自首。

案例 3　攻击会考网站删除万份试卷

2002 年江苏省举行普通高中高三信息技术等级考试，共有 30 万名考生分别参加上、下午考试。当天中午，省会考办发现有人闯入网站删除了部分学生的考试文件，下午意外再次发生，下午参考的部分学生的试卷也被删除。这次信息技术考试对高三学生意义非同寻常，只有通过了这次考试的学生才能参加全国高考，因此试卷被删除的后果十分严重。省会考办立即查清了丢失试卷的学校，要求学校保留试卷备份重传考试文件，同时向省公安厅网络监察处报案。经过公安机关的缜密侦查，查获了行为人罗某。由于罗某的行为涉及全省的 85 所考试学校，尽管会考办采取了补救措施，但仍然造成了 5 万元左右的经济损失。后经法院审理，以破坏计算机信息系统罪判处罗某有期徒刑 6 个月，缓期两年执行。

(二)思考并回答以下问题

(1)搜集、列举其他影响网络安全的案例。

(2)网络环境中的犯罪行为给网络安全应用带来了哪些危害?

(3)根据实际案例讨论出现问题的原因。

活动二　了解危害网络安全的因素

本活动将帮助计算机用户认识危害网络安全的各种因素,全面了解出现网络安全问题的原因,为深入学习网络安全技术做好铺垫。

(一)危害计算机网络安全的形式

对于计算机网络应用领域的"危害",可以从两个方面理解:一是各种因素对计算机网络造成的危害,二是利用计算机网络对社会产生危害。与其他危害相比,对计算机应用领域的危害由于其含有较强的技术性,影响范围较大,因此造成的后果也更为严重。

危害计算机网络安全的表现形式多种多样,危害后果和抑制手段也不尽相同,这里归类列出常见的几种,旨在帮助大家认识出现危害事件的严重性,提高网络安全防护意识。

1.自然灾害

自然灾害对计算机网络造成危害的事件在世界各国时有发生。如果建造机房、安装设备时没有考虑防水、防火、防静电、抗震、避雷等问题,计算机网络工作环境抵御自然灾害的能力会很差,发生灾害后有可能给网络系统造成灭顶之灾。例如,辽宁某铁路局控制机房因缺乏雷电防护设施曾3次遭受雷击,致使控制系统和一些终端设备损坏,严重影响了正常编组运输。日本东京电信局在电缆维护时,工人操作不慎造成火灾,由于缺乏有效的火灾控制手段,大火持续16个小时,烧毁了大量的通信设备,导致数家银行和邮局的计算机通信网络中断,使银行分布在各地的自动付款机被迫停机,邮局的一些业务只能暂停。

2.系统漏洞

计算机网络系统本身存在的致命漏洞是威胁网络安全的重要因素。网络系统大型化使控制管理网络的复杂程度不断增加,隐藏其中的漏洞也越来越多,它们有可能引起网络系统崩溃,也有可能成为渗透网络系统的工具或通道。例如,微软公司曾在IE浏览器安全建议书中证实,IE浏览器存在安全漏洞,由此可能引起零位指针失效或内存失效等错误。思科曾承认它的Internetwork操作系统存在处理IPv6包的漏洞,若向受影响的思科设备发送特制的IPv6包,有可能迫使设备重新启动,导致DoS攻击。

3.操作失误

工作人员缺乏责任心或因专业知识滞后造成操作失误,也会导致意想不到的灾难事件。例如,由于美国防空司令部指挥中心计算机操作员输入数据错误,引起防空警报,最高指挥部随即命令1 000枚核导弹进入待发状态,核战争一触即发。香港联合交易所工作人员在停电后按停警钟时,意外地按下后备电源的"紧急停止掣",截断了大堂及自动对盘系统主机的电源,造成停电使系统停止工作4分58秒,结果导致收市延误,在延误收市的4分58秒内,额外

交易 1 099 宗,成交额约 1 亿元。延误时间内交易的合法性,引起了巨大争论。

4.病毒侵袭

计算机网络病毒的产生和全球性蔓延对网络安全应用构成了严重威胁,且已经造成了巨大的损失。计算机网络病毒的危害之大,不亚于人类社会发生的瘟疫。台湾大学生陈盈豪制造的"CIH"病毒,首次发作就使全球约 6 000 万台计算机受害。美国的罗伯特在互联网上传播"蠕虫"病毒,导致美国 6 000 多个系统瘫痪,直接损失 9 600 万美元。"爱虫"病毒发作,全球损失约 100 亿美元。某省财政厅财务管理系统感染病毒,破坏了 3 年的财务数据,造成无法挽回的巨大损失。

5.违法、违纪

人为恶意的攻击、破坏是威胁网络安全的重要原因,也是最难控制和防范的危害因素。此种危害的表现形式很多,如对着计算机设备撒尿、浇油漆的物理破坏,放置逻辑炸弹的应用系统破坏,格式化磁盘的信息破坏,篡改信息、盗窃程序数据的个人牟利行为,甚至侵入重要、机密信息系统严重危害国家安全的重大事件。

(二)发生危害网络安全事件的诱因

危害网络安全事件的发生数量居高不下,且逐年增加,说明危害网络安全的事件有较为特殊的诱发原因,值得深究。认清发生危害网络安全事件的实质有助于开展防范工作。

1.网络系统本身存在脆弱性缺陷

计算机网络系统本身的脆弱性是诱发危害网络安全事件最根本的原因。计算机以高速度、高精度处理信息见长,它有许多其他设备不能比拟的优点。如信息存储密度高、易修改、能共享、网络传递方便等,正是这些优点使计算机备受人们青睐。也正是这些特点使计算机具有先天的脆弱性,高存储密度使处理大量信息成为可能,而在大量信息中隐藏少量非法信息不易察觉,信息一旦丢失损失会很惨重;信息易修改的特性给正常工作带来很多方便,但修改后不留痕迹又使犯罪分子有机可乘,使追查犯罪困难重重;网络传递、共享能使人们快速、充分地利用信息资源,但信息传递过程中的电磁泄露、搭线窃听、接收信息对象的甄别等问题,又使网络安全控制难以把握。

计算机网络系统的脆弱性和计算机技术的开放性,使针对网络系统的危害易于发生。而防护的薄弱又给了危害行为人可乘之机,所以计算机网络系统的脆弱性不可避免地导致了危害网络安全事件的发生。

2.网络系统存在管理的复杂性问题

计算机网络系统的功能日益强大,计算机软、硬件的复杂程度随之成倍增长,计算机网络系统的管理也日趋复杂化。正是因为网络和计算机信息系统具有管理的复杂性,工作中稍有不慎或管理策略不当,都会使网络系统出现安全隐患。这些不易察觉的安全漏洞,对拥有高技术、法制观念不强、想捞取不法利益者是不小的诱惑,对刻意显示自己才能的人来说也是不可多得的机会。

计算机网络系统管理的复杂性,使管理难度增大,同时,保证网络安全的难度也增大。这必然导致网络的安全性相对下降,使非法渗透网络系统更为容易,更多的人有机会、有可能使用计算机网络或针对计算机网络从事非法活动。危害网络安全事件的数量居高不下与网络系统管理的复杂性有直接关系。

3.网络信息的重要性使之成为攻击目标

计算机应用环境逐渐增多，使存储其中的信息量和信息重要程度相应增加，许多信息和财富直接关联，有些计算机中存储的数据和信息的价值远远超过计算机系统本身。因此，大量危害网络安全事件的指向是计算机网络系统中的信息。通过渗透网络系统能够窃取机密信息、能够获取钱财，这对于掌握计算机网络技术又想一夜暴富的人来说是不小的诱惑，也促使一些人甘冒风险以身试法。信息、机密、财富密不可分是导致危害网络安全事件发生的主要原因。

4.低风险的诱惑

从犯罪心理的角度看，犯罪行为人在实施犯罪前，既关心该行为刑罚的轻重，更关心受到刑罚的可能性。刑罚很重，但受到刑罚的可能性微乎其微，会降低刑罚的威慑作用，犯罪人在趋利避害的侥幸投机心理支配下实施犯罪。危害网络安全的活动需要技术支持，隐蔽性较强，被发现和查获的可能性小，这一特征对有机会从事危害活动的人有极强的诱惑力。高回报低风险的利益驱动，是许多人甘愿冒险从事危害网络安全活动的主要原因。

5.道德理念的差异

人类长期形成的道德观念与计算机技术不协调，也是诱发危害网络安全事件发生的一个原因。在计算机网络应用普及过程中，高技术人才一直是人们崇拜的对象，他们所做的越轨行为往往被当成“天才”杰作，即使有触犯法律的行为，也会放宽限制条件、降低处罚尺度。权衡高技术与犯罪，人们更看重技术而姑息犯罪。

计算机网络应用环境固有的思维定式，也淡化了犯罪概念。私拆别人信件的人一定会有罪恶感，因为大多数人知道这是违法行为，但是不经允许点击、浏览别人的 E-mail 是什么性质，多数人认为不能与私拆信件相提并论。认为私人文件加密是计算机使用者在使用计算机过程中达成的默契，未加密文件是共享的，然而，这一惯例不能为法律所容。

(三)思考并回答以下问题

(1)根据已发生的危害案例总结未列出的危害形式。

(2)利用已具备的网络知识阐述网络的脆弱性。

活动三　理解网络安全的基本要求

本活动将帮助计算机用户了解什么样的计算机网络是安全的网络这一基本问题，为今后构建安全、可靠的网络应用环境做好基础准备。

(一)什么是安全的计算机网络

从计算机网络应用的角度看，计算机网络是处理信息的具体工具，而信息则是以某种目的组织起来，经过加工处理使之形成一定结构的数据。因此，谈及计算机网络的安全问题，一定要涉及信息处理的全过程。

不同人站在不同的角度对计算机网络安全有不同的理解。

● 网络用户需要的安全是指他们借助计算机网络处理信息时，不会出现非授权访问和破坏，即便是在信息交换、传输过程中也不能出现任何意外事件。

● 计算机网络系统管理者认为的安全是对管理对象完全可控，任何时候都不能因黑客攻击、系统故障等问题出现管理失控，管理者按约定给用户提供井然有序的网络服务。

● 公共信息受众理解的网络安全是过滤一切有害信息，享受信息带来的便利和快乐。

● 机密信息拥有者要保证的网络安全是敏感信息不会以任何形式泄露。

综合以上要求，我们认为计算机网络安全是指网络中的信息不会被故意的或偶然的非法授权泄露、更改、破坏，不会被非法系统辨识、控制，网络设备安全可靠，人们能有益、有序地使用计算机网络，安全、可靠地获取网络信息。

(二)网络安全的基本内容

网络安全不仅涉及技术问题、管理问题，还涉及法学、犯罪学、心理学等问题，是一门由多学科综合形成的新学科。

1.网络安全涉及的方面

计算机网络系统是由计算机实体、信息、人组成的人机系统，安全问题也应包括实体安全、信息安全、运行安全和安全管理等几个方面。内容涉及安全技术、安全管理、安全评价、安全产品、安全法律、安全监察等。

网络安全主要涉及信息存储安全、信息传输安全、网络应用安全 3 个方面，包括操作系统安全、数据库安全、访问控制、病毒防护、加密、鉴别等多类技术问题，可以通过保密性、完整性、真实性、可用性、可控性 5 种特性进行表述。

● 保密性指网络信息不会泄露给非授权对象的特性。

● 完整性指网络信息本身完整，且不会在未授权时发生变化的特性。

● 真实性指保证网络处理过程真实可靠的特性。

● 可用性指合法对象能有效使用网络资源的特性。

● 可控性指对网络资源能进行有效控制的特性。

2.网络安全控制层次

网络安全控制是复杂的系统工程，需要安全技术、科学管理和法律规范等多方面协调，并构成层次合理的保护体系，只有这样最终才能达到保证网络安全的目的。安全防护技术是保证实体、软件、数据安全的基础，有效管理是保障安全技术发挥作用的前提，法律规范是制约和打击危害网络安全的武器。所以，网络安全控制应在以下 4 个层次上考虑。

● 实体安全防护　对计算机网络实体进行安全防护是保证网络安全的重要环节，如果计算机硬件和工作环境出现安全问题，存储其中的信息和正常的网络应用很难幸免。所以，设置必要的实体安全防护设施是保证网络安全的基础。

● 软件安全防护　在实体安全的基础上增加软件安全防护措施是保证网络安全的进一步要求，软件系统故障同样会导致网络安全问题。所以，软件和软件运行安全也是保证网络安全的基础。

● 安全管理　设置硬件、软件安全防护设施固然重要，让安全设施充分发挥作用更重要，而它主要依赖于对安全设施的科学管理。统计结果表明，70%以上的安全问题是管理不善造成的，真正由于技术原因出现的安全问题很少。由此可见，安全管理在保证网络安全中的作用极其重要。

● 法律规范　安全法律是安全防护技术以外的网络安全保障因素。在发生安全问题以前，安全法律起规范网络应用行为、威慑破坏行为的作用，是网络安全的法律保障。在发生安全问题以后，安全法律是处理安全问题的法律依据。

(三)思考并回答以下问题

(1)如何理解“不同人会对网络安全有不同要求”这一说法？

(2)为什么认为安全管理在保证网络安全中有极其重要的作用？

任务二　了解网络安全现状及发展趋势

随着网络安全问题日益增多，人们对网络安全的防护意识不断增强，安装网络安全防护产品的环境也越来越多，网络安全防护产品和相应技术也不断发展。

任务描述

保证网络安全就是要解决网络中存在的不安全问题，不同问题有相应的解决之道，安全问题不断变化，解决方案也将随之改变。所以，全面认识网络安全防护产品及技术发展趋势，是学习网络安全技术，保证网络安全的重要基础。网络用户只有充分了解安全现状，了解安全防护产品，才能有效地选择安全防护措施。

任务分析

了解网络安全现状是认识网络安全问题的前提，更是强化网络安全防护的基础。只有了解网络中存在的安全问题和相应的防护技术，才能有效保证网络安全。因此，本任务可以分解成以下活动：

- 了解网络安全问题的现状；
- 了解网络安全防护产品应用现状；
- 了解网络安全技术的发展趋势。

活动一　了解网络安全问题的现状

了解网络中出现的安全问题是实施安全防护的基础，也是预测网络安全防护技术发展的风向标。本活动将帮助计算机网络用户了解网络安全问题的现状。

(一)互联网的主要安全问题

从发生的互联网安全事件看，近两年中国没有发生大规模的病毒威胁，也没有发生影响恶劣、损失严重的网络攻击事件，但网络安全威胁形势依然严峻，危害变化的趋势令人担忧。

1.网页仿冒依然活跃

仿冒者充分利用更有效的技巧和自动操作技术，借助热点、敏感问题强化仿冒的可信度，使网页仿冒问题依然棘手。

2.垃圾邮件猖獗

随着垃圾邮件组织团伙 McMolo 曝光和反垃圾邮件过滤技术的提高，全球垃圾邮件的比例显著下降，但问题没有根绝，电子邮箱的使用者依然会收到干扰用户的垃圾邮件。有网络公司预测，未来垃圾邮件数量会大幅回升。

3.数据泄露十分严重

数据泄露事件持续增长是由经济大环境中种种因素造成的，由此凸显防数据丢失对于数据拥有者的重要性和强化技术防护、管理防护的必要性。

4.系统漏洞不容忽视

新发现的漏洞数量不断增加，能够产生危害的严重程度也相当高，由此对网络应用安全构成了重大威胁。2009 年 3 月之内，CNCERT/CC 接收到国内外安全组织报告的漏洞多达 22 个，其中高危漏洞 4 个，影响的软件、硬件系统包括思科、微软等厂商。

5.网站被篡改事件屡禁不止

2009年 3 月中国大陆地区共有 2 225 个网站被篡改，其中政府网站 104 个，占总量的 4.67%。

6.僵尸网络遍布全球

CNCERT/CC 在 2009 年 3 月，发现国内外 1 309 个 IP 地址对应的主机被利用作为僵尸网络控制服务器，其中 386 个在中国大陆。被控服务器最多的地区是广东，占 30.05%。国内外共有 420 024 个 IP 地址对应的主机为僵尸网络的客户端，位于中国大陆的有 135 349 个。客户端最多的地区是河南，占 15.68%。在僵尸网络中，规模大于 10 万的有 12 个，规模大于 5 000 的有 56 个，规模在 1 000 以下的占 90%。

(二)网络病毒整体形势

病毒制造、传播者在巨大利益的驱使下，利用病毒、木马技术进行各种网络盗窃、诈骗活动，严重干扰网络的正常应用，应予以高度关注。

1.恶意代码的主流是木马

木马在中国的恶意代码数量中占有绝对多数，2008 年公布的 10 大流行病毒中，主要以木马、后门为主。排在榜首的“网游大盗”，就是用于盗取网络游戏账号的木马程序。木马制作者的牟利目的十分明确，盗取互联网上有价值信息资料转卖后获利。

2.“挂马”成为病毒传播的主要手段

网站挂马成为病毒传播的主要手段，无论是主动或被动的挂马都为病毒滋生和传播提供了优越的环境，当前相当数量的病毒变种来自于这类网站。中国国家计算机病毒应急处理中心检测发现，被挂马的网站覆盖政府、新闻、软件下载、娱乐等各种网站。当用户使用有安全漏洞的浏览器访问这些网站时，病毒利用脚本下载木马程序并激活。

3.病毒的自我保护能力增强

一些新技术，如主动防御技术、磁盘过滤驱动技术、影像劫持技术、穿透还原卡或还原软件技术被应用到恶意代码的编写中，使病毒从修改样本特征值躲避查杀逐渐过渡到直接与安全软件对抗。如“AV 终结者”可以通过释放并加载驱动程序，在获得系统权限后试图结束安全软件进程，让用户的计算机处于无防护状态。“机器狗”利用突破系统还原卡技术，让感染病毒的计算机在重启后，病毒样本仍存活在系统中。