中等职业教育改革创新示范教材

网络安全实例教程

◎ 谭建伟　主编

▶ 本书配有电子教学参考资料包

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http: //www.phei.com.cn

中等职业教育改革创新示范教材

网络安全实例教程

谭建伟 主 编

邹孔华 刘 红 赵 玲 副主编

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书贴近网络安全应用实例，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。

全书共分为 9 个单元。单元 1 全面介绍网络安全的基础知识；单元 2 讲解信息加密和网络中的密码应用；单元 3 介绍防治计算机网络病毒和木马的基本方法；单元 4 介绍防范黑客技术；单元 5 讲解网络防骗技术；单元 6 介绍常用的防火墙和入侵检测技术；单元 7 讲解网络安全管理技术；单元 8 讲述计算机网络领域应该遵守的法律道德规范，以及不当行为可能承担的法律责任；单元 9 介绍网络安全整体解决方案。

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。

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教科书。

图书在版编目（CIP）数据

网络安全实例教程 / 谭建伟主编. —北京：电子工业出版社，2014.4
中等职业教育改革创新示范教材
ISBN 978-7-121-14665-7

Ⅰ. ①网… Ⅱ. ①谭… Ⅲ. ①计算机网络—安全技术—中等专业学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 194722 号

策划编辑：关雅莉
责任编辑：肖博爱
印　　刷：北京天宇星印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：18.5　字数：473.6 千字
印　　次：2014 年 4 月第 1 次印刷
定　　价：32.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

21 世纪是信息时代，现今人们利用计算机网络工作学习、游戏娱乐，充分享受计算机网络带来的快乐，同时，人类社会也面临来自网络的威胁。网络病毒、网络攻击、信息网络盗窃、网络侵权、网络战争等问题，使人们不得不把网络安全提升到国家安全的战略高度予以关注。许多重大黑客事件表明，计算机网络存在严重的安全漏洞，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 Internet 相连的主机曾遭受过黑客攻击，2011 年 5 月，中国大陆被篡改的网站数量达 3358 个，比 4 月增长 5%。由此可见，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，就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性教材。书中内容没有涉及过多过深的计算机安全技术理论和空洞生涩的网络安全专业术语，对可操作的内容也尽量列出完整的操作过程，期望对学习者提高计算机网络安全防护技能有所帮助。

全书以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网络安全防护知识和技能，更能实现技能学习与社会应用的无缝对接，达到学以致用的目的。

全书共分为 9 个单元。单元 1 全面介绍网络安全的基础知识，帮助学习者建立网络安全防护理论的整体概念。单元 2 讲解信息加密和网络中的密码应用，帮助学习者了解信息加密的概念，掌握实用的加/解密技术，有效保护应用环境和信息的安全。单元 3 介绍防治计算机网络病毒和木马的基本方法，教会计算机用户高效率地使用专门工具查找、清除计算机病毒和木马，并掌握手工清除特殊木马的技巧。单元 4 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。单元 5 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。单元 6 介绍常用的防火墙和入侵检测技术，它是防范黑客入侵技术的延伸，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。单元 7 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，树立安全管理的基本理念，学会利用最基本的安全管理技术安全管理网络。单元 8 讲述计算机网络领域应该遵守的法律道德规范和不当行为可能承担的法律责任，强化法制意识，做遵纪守法和文明的网络应用者。单元 9 介绍网络安全整体解决方案，帮助学习者提高全面解决网络安全问题的能力。

本书教学时数为 64 学时，在教学过程中可参考以下课时分配表：

学习单元编号	学习单元名称	学习工作项目	学时		教学形式	成绩权重
单元 1	网络安全的基本概念	网络安全的基本含义	2	4	授导、探究	6%
		网络安全现状及发展趋势	1			
		网络安全防护整体框架	1			
单元 2	网络应用中的密码技术	信息加/解密的概念	1	6	授导、探究、实践	9%
		PKI 技术	1			
		Windows 系统的加解密	1			
		浏览器的密码应用	1			
		电子邮件的加解密方法	2			

续表

学习单元编号	学习单元名称	学习工作项目	学时		教学形式	成绩权重
单元3	防治计算机网络病毒、木马	计算机网络病毒的基本概念	2	10	授导、探究、实践	16%
		使用杀毒软件清除网络病毒	2			
		网络病毒的管理防范	1			
		计算机木马的概念	1			
		使用木马查杀软件清除木马	2			
		手工清除特殊木马	2			
单元4	黑客防范技术	黑客行为、黑客实施网络攻击的过程	2	10	授导、探究、实践	16%
		应对黑客攻击的基本方法	2			
		口令破解及保护	2			
		网络扫描及网络扫描软件使用	2			
		网络防黑客的基本方法	2			
单元5	网络防骗技术	常见的网络骗术	1	6	授导、探究、实践	9%
		IP 欺骗、防 IP 欺骗	2			
		E-mail 欺骗、防 E-mail 欺骗	2			
		防范网络钓鱼	1			
单元6	网络安全产品应用	防火墙的基本工作原理	1	8	授导、探究、实践	13%
		软件防火墙的使用	1			
		硬件防火墙的使用	4			
		入侵检测技术	1			
		入侵检测设备的使用	1			
单元7	网络安全管理技术	安全管理涉及的基本内容和方法	2	6	授导、探究、实践	9%
		制定有效的网络安全管理策略	2			
		网络安全评估准则	1			
		网络安全风险评估	1			
单元8	网络安全的法律规范	网络应用中的法律规范	4	6	授导、探究	9%
		网络应用中的道德规范	2			
单元9	网络安全解决方案	网络安全解决方案的基本框架	2	8	授导、实践	13%
		制定网络安全解决方案	6			
总计			64	64		100%

本书由谭建伟任主编，邹孔华、刘红、赵玲任副主编，参与教材编写的有谭建伟、邹孔华、刘红、赵玲、王长杰、郭璐青、王卫华、韩忠、邹季刚。全书由谭建伟统稿。河南工程学院李建教授、河南司法警官职业学院王慧斌博士对书稿进行了认真审阅，提出了许多意见和建议，全体作者深表感谢。

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

目　录

单元 1　网络安全的基本概念

计算机网络技术的快速发展为信息传递提供了便利条件，也为扩大计算机应用领域提供了基本保障，但是，在计算机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球共同关注的话题。信息资源在网络环境传播、共享使用的过程中，一些重要的信息可能被网络黑客觊觎而出现被窃取、篡改，也可能因为攻击行为导致网络崩溃出现丢失，诸如此类问题影响了信息产业正常有序的发展，严重时甚至会造成人类社会的动荡。因此，保证网络安全、有序运行是发挥网络作用的基础。2010 年以来，世界各国相继制定和大幅调整网络安全战略，增设专门机构，加大人员和资金投入，最大限度维护自身网络空间的安全和利益。

任务 1　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，内容广泛且技术复杂，因此也造成了网络安全保障工作的复杂性。

任务描述

在人类社会信息化建设的进程中，网络安全问题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，也需要网络应用者提高安全防护意识和安全应用技术，以有效保护应用环节的安全。或许很多人都听说或知道“网络安全”这一热门词汇，但是“网络安全”究竟涵盖哪些内容？是哪些因素导致了网络应用的不安全？人类社会需要什么样的安全网络？等问题未必人人清楚。本任务将帮助学习者了解网络安全的基本概念，全面或重新认识网络安全。

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，则可以通过对已经发生的各种危害案例的分析寻找答案。因此，学习任务可以被分解成以下三个活动。

活动 1　危害网络安全案例研讨。

活动2　了解产生网络危害的原因。
活动3　掌握网络安全的基本要求。

活动1　危害网络安全案例研讨

了解危害网络安全事件既是揭示网络安全重要性的基础，也是提高网络用户对网络安全防护重要性认识的基础。本活动将通过集体研讨、有针对性的信息查询等多种手段，帮助学习者理解学习网络安全知识和提高安全防护技能的重要性。

1．危害网络安全案例展示

案例1：罗伯特制作“蠕虫”事件

“蠕虫”病毒的始作俑者是美国康奈尔大学计算机科学系一年级研究生罗伯特·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的病毒。1988年10月，罗伯特开始了自己的计划，他一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。1988年11月2日美国东部标准时间晚上7点30分，罗伯特完成了病毒的编写工作，一个小时后，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陷入瘫痪。罗伯特吃完晚饭去检查病毒的进展情况，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。

思考：病毒制作者的行为可能造成什么样的可怕后果？

案例2：江西卫生厅考试中心数据库被非法操作事件

2008年6月，江西省公安厅网监总队接到江西省卫生厅考试中心报案，称该厅网站的医师资格查询数据库被他人非法操作，有人修改了数据库内容并制作虚假“医师资格证书”牟利。6月初，有人持假“医师资格证书”到浙江省相关部门办理“行医许可证”，虽经专门机构认定证书是假的，但查询江西省卫生厅网上数据库发现确有其人，于是向江西省卫生厅核实。江西省卫生厅在检查考试中心网站时发现，几个月前该网站曾遭到黑客侵入，数据库被大量篡改，遂向警方报案。

6月19日，江西省公安厅网监总队立案侦查此案。通过对被攻击受控制服务器的现场勘验，民警发现黑客于3月26日起入侵江西省卫生厅网站，并上传网站后门程序对网站服务器进行控制。经查，黑客是利用境外新加坡的IP地址将篡改的数据上传至数据库，手

段非常隐蔽，有较高的反侦查意识。办案民警经过几天的艰苦侦查，终于将黑客在网上的其他虚拟身份锁定，并最终确定犯罪嫌疑人上网的地点。

6 月 24 日，民警展开抓捕行动，在某租住地将犯罪嫌疑人李某及其同伙 5 人当场抓获，缴获作案用笔记本电脑 4 台，打印机 1 台，各类银行卡 25 张，虚假身份证 13 张，虚假空白“医师资格证书”6 本，“医师执业证书”1 本，“建造师证书”2 本。随后，民警又在武汉将另一名主要犯罪嫌疑人王某抓获。

据警方介绍，2007 年，就读于南昌某高校计算机专业的李某因毕业论文没有通过，无法取得毕业证书，遂产生贩卖假证的念头，只是苦于网上数据库查不到这些假证。2008 年 3 月，李某发现网上要求办理“医师资格证书”及“毕业证书”的信息非常多，于是在网上找到王某，要求王某侵入一些网站，在取得使用权限后交给自己使用，然后通过入侵修改数据—办理假证—贩卖假证—用假证办理从业许可证等环节从中非法牟利。

经查，王某先后入侵江西省卫生厅考试中心网站、湖北省卫生厅网站、贵州人事考试网、四川人事考试网、湖北荆州人事局网站、江苏自考网、辽宁省建设厅网站等 10 余个网站，并以每个网站管理员权限 5000～8000 元的价格卖给李某。李某则对下线收取代理费，每添加一个客户收取 1000～2500 元不等。据李某交代，他共添加了包括江西省卫生厅网站在内的网站数据 700 余个，获利 200 余万元。据一名受害者反映，为了弄到一个上网可查的假证书，他就花了 8000 多元。

思考：此案暴露出了网络应用中的哪些不安全问题？危害性有哪些？

案例 3：以奥运为名的网络诈骗案

2008 年 1 月 4 日，南京公安局网络警察支队接到举报，称有人假冒 2008 年奥运会名义建立网站，实施诈骗活动。南京警方经过缜密调查，于 1 月 28 日在海南儋州抓获许某、陈某等 9 名犯罪嫌疑人。

据该团伙成员交代，2007 年 12 月底，许某和陈某等建立了网站，假冒“系统提示”信息，向众多网络游戏玩家发送中奖消息。当游戏玩家登录他们建立的网站后，中奖页面会显示用户中得 18800～38800 元不等的“惊喜奖金”及奥运会门票一张，但领奖的前提是向一个银行卡号汇款 998 元作为手续费。案发时，全国各地共有 100 多名受害者向涉案银行账户汇款共 30 余万元。

思考：为什么网络诈骗的危害性比传统形式的诈骗更严重？

案例 4：美国加州 5 名用户指控 Facebook 违反隐私法事件

据国外媒体报道，2009 年 8 月美国加利福尼亚州 5 名 Facebook 用户向奥兰治县法院提起民事诉讼，指控 Facebook 违反该州隐私法，并在如何使用个人信息方面误导用户。

原告要求 Facebook 支付赔偿金和诉讼费用，并要求陪审团参与审理。原告诉称，Facebook 将用户提交的个人信息提供给第三方，违反了加州隐私与网络隐私法。该网站还在未向用户披露的情况下进行数据挖掘等工作。5 名原告分别包括 1 名专业摄影师、2 名 13 岁以下的儿童、1 名原 Facebook 用户，以及 1 名洛杉矶女演员兼模特。

Facebook 发言人巴里·斯彻内特拒绝对此做出评论，他表示：“我们认为该指控毫无

根据，并将积极应诉。”Facebook 目前的用户已增长至 2 亿多，隐私保护方面的问题日益突出。2009 年初，由于数万名用户抗议 Facebook 滥用在该网站上共享的个人信息，该网站宣布调整隐私控制方式，转而让用户选择多种不同的隐私政策。Facebook 于 2 月份表示，在采取新的隐私政策前，将允许用户对隐私、内容所有者，以及共享方面的调整进行评估、评价和投票。2007 年末，Facebook 推出了“Beacon”跟踪工具，该工具可以在用户毫不知情的情况下将其行为发布到其他网站，在自由主义 MoveOn 和会员的压力、抗议下，网站最终允许用户关闭该工具。

思考：网络隐私泄露会带来哪些严重危害？

2. 危害网络安全案例收集

学生自主分组并充分利用网络资源进行案例收集，小组活动结束后应形成以下成果：

（1）收集到若干个危害网络安全的真实案例。

（2）一份简单的网络安全危害案例分析报告。

（3）简短的小组活动总结。

3. 危害网络安全案例讨论

根据对教材展示案例和自己收集案例的讨论结果，分组发言表达各组对危害网络安全问题的看法，最终形成对危害性问题较为统一的认识。讨论可以围绕以下问题展开：

（1）目前的网络安全形势如何？

（2）对网络安全产生危害的形式有哪些？

（3）网络中的不法行为可能带来的危害是什么？

（4）如何看待提高网络安全的急迫性？

活动 2　了解产生网络危害的原因

只有充分了解发生网络危害的基本原因，才能更好地找出应对策略，从根本上解决网络安全危害问题。本活动将帮助学习者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。

1. 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，一是各种外在或内在因素对计算机网络造成的危害，二是利用计算机网络对人类社会产生的危害。前者又分为人为与非人为两种，非人为危害主要指自然灾害对计算机网络造成的危害，如地震、水灾、火灾、战争等原因出现的网络中断、系统破坏、数据丢失等。人为危害是指对网络人为攻击，达到破坏、欺骗、窃取数据等目的。与其他危害相比，计算机应用领域的危害包含有较强的技术性，影响范围较大，由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 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，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，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 秒期间，额外交易 1099 宗，成交额约 1 亿多元。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 6000 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 6000 多个系统瘫痪，直接损失 9600 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）人为恶意破坏

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，有对着计算机设备撒尿、浇油漆的物理破坏，有放置逻辑炸弹的应用系统破坏，有格式化磁盘的信息破坏，有篡改信息、盗窃程序数据的个人牟利行为，也有侵入重要、机密信息系统严重危害国家安全的重大事件。

（6）网络欺诈

网络欺诈已成为阻碍网络应用的重要顽疾，现在的网络不但是滋生欺诈性犯罪的新土壤，花样繁多、数量巨大的网络欺诈内容也严重影响了人们对网络信息的信任度。

（7）网络传黄

在互联网有害信息中，传播面最为广泛的就是网络色情信息。资料统计显示，互联网上的色情网站有 420 万之多，占全部网站的 12%，色情网页约有 3.72 亿个，每天色情主题

搜索约 6800 万次，占全部搜索问题的 25%。大量的不良信息对青少年网民的影响比例高于世界平均水平的中国，已经产生了严重的恶果，网络也成为引发一系列社会问题的根源。

（8）网络赌博

2009 年以来，全国破获了多起网络赌博案件，涉案金额之巨，危害之大，令人触目惊心。湖南省赌博案中的涉案金额高达百亿元以上，上海赌博案中的短期投注金额高达 66 亿元，这其中的大部分投注赌资通过网络流向境外，网络赌博已经成为一种严重的“灾害”，成为危害国家经济建设和社会治安稳定的重要因素。

2. 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，说明危害网络安全有较为特殊的诱发原因，值得深究，认清引发危害网络安全事件的原因也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倍受人们青睐。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，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困难等问题，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、时刻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和网络系统管理复杂性有直接关系。

（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，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，高技术和犯罪权衡，人们更看重技术姑息犯罪。

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。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。

3．网络危害问题讨论

根据教师对网络危害知识的讲解和自己对网络危害的认识，分组讨论遏制网络危害的必要性，强化提高网络安全防范的意识。讨论可以围绕以下问题展开：

（1）危害网络安全形式的演变趋势如何？

（2）网络黑色利益产业链的形成对网络安全有什么影响？

（3）如何解决管理复杂性带来的安全问题？

（4）网络行为的低风险表现在哪些方面？

活动 3　掌握网络安全的基本要求

本活动将帮助学习者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。

1．什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的安全要求有不同的理解，通常会出现以下几种情况。

（1）网络用户需要的安全

网络应用者在借助计算机网络处理信息时，不能出现非授权访问和破坏，即便是在信