NEW HORIZON

工学结合新视野
高职高专
“十二五”规划教材

总主编 王宗湖

电子商务安全

Dianzi Shangwu Anquan

主 编 王 鑫

对外经济贸易大学出版社
University of International Business and Economics Press

工学结合新视野高职高专“十二五”规划教材

总主编　王宗湖

电子商务安全

主　编　王　鑫
副主编　刘天宝　陈照义　陈洪梅

对外经济贸易大学出版社
中国·北京

图书在版编目（CIP）数据

电子商务安全 / 王鑫主编. —北京：对外经济贸易大学出版社，2011
工学结合新视野高职高专“十二五”规划教材
ISBN 978-7-81134-922-1

Ⅰ.①电… Ⅱ.①王… Ⅲ.①电子商务－安全技术－高等学校：技术学校－教材 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2010）第 257205 号

电子商务安全

王　鑫　主编

责任编辑：刘　尧　高　卓

对外经济贸易大学出版社
北京市朝阳区惠新东街 10 号　　邮政编码：100029
邮购电话：010－64492338　　发行部电话：010－64492342
网址：http://www.uibep.com　　E-mail：uibep@126.com

山东省沂南县汇丰印刷有限公司印装　　新华书店北京发行所发行
成品尺寸：185mm×260mm　　17.25 印张　　399 千字
2011 年 1 月北京第 1 版　　2011 年 1 月第 1 次印刷

ISBN 978-7-81134-922-1
印数：0 001－5 000 册　　定价：26.00 元

工学结合新视野高职高专
“十二五”规划教材编委会

总　　序

经过十几年的跨越式发展，我国高职教育取得了长足进步，无论是办学数量还是招生规模都占了我国高等教育的半壁江山。但是，我们必须清醒地看到，目前我国经济的飞速发展及结构的重大调整，已经对高职教育提出更高的要求。为使高职教育尽快适应新形势，2006 年教育部、财政部联合启动了《国家示范性高等职业院校建设计划》，建设了百余所示范院校。2010 年 7 月教育部再度发布《教育部、财政部关于进一步推进“国家示范性高等职业院校建设计划”实施工作的通知》，新增 100 所左右骨干高职建设院校。两次示范性院校建设计划的实施，主要目的就是通过示范性建设工程，引领、带动所有高职院校，不断提高办学适应能力，提升办学质量和育人水平，增强服务区域经济和社会发展的功能。

最近，国务院颁布的《国家中长期教育改革和发展规划纲要》（2010—2020 年）（以下简称“规划纲要”）指出：“职业教育要面向人人、面向社会，着力培养学生的职业道德、职业技能和就业创业能力……”，提出“要把提高质量作为重点。以服务为宗旨，以就业为导向，推进教育教学改革。实行工学结合、校企合作、顶岗实习的人才培养模式”。可见，国家已将提高教育质量作为今后一段时间高职教育教学改革的重点，并将“工学结合、校企合作、顶岗实习”列为人才模式改革的方向，明确提出高等职业教育主要培养具有“职业道德、职业技能和就业创业能力”的人。

教材作为“整个教育系统的软件”，是培养人才的蓝本。客观地讲，经过十几年的探索，我们已经认识到高职教育的培养目标、课程体系、教学模式与普通本科院校实施的学科教育之间的差异，并进行了多方面的教学改革研究与实践，也试图引进国外先进的课程模式以推动课程改革。但职业教育毕竟与其他高等教育不同，其中，“就业”和“高技能”是其主要的目标指向。因此，职业教育的课程设计应以满足产业发展为宗旨，以新的职业能力内涵为目标构建系统化的课程，突出体现“就业导向”的职业能力培养。但目前，我国职业教育教学和管理模式受传统教育思想和教育模式的影响较深，以能力为本位的教育观还未完全形成，课程改革和教材开发还远远满足不了形势发展对高职教育的要求。因此，为更好地适应我国走新型工业化道路，实现经济发展方式转变、产业结构优化升级需要，高等职业教育必须加快课程体系改革和教材建设的步伐，建立符合时代特征和具有中国特色的职业教育新思维、新模式、新课程体系。

鉴于此，对外经济贸易大学出版社为适应教育发展的新形势，并努力推动高职高专院校的教材建设，委托我们组织全国职业院校的教师及具有企业工作经验的业务骨干，编写这套工学结合新视野高职高专“十二五”规划教材。本系列教材暂包括基础课程、国际经贸、工商管理、财会金融、物流管理、连锁经营、电子商务、旅游与酒店管理等八大专业。

为使教材编写尽量适应高职教育的特点及时代发展的新要求，我们在编写教材过程

中，尽可能把最新的研究成果吸收渗透到教材中来，在内容安排、教法选择、编写体例等方面也进行了较多的改革，甚至是新尝试。本套丛书具有以下特点。

1. 以“能力培养”和“创新教育”为主线，架构教材总体框架

本套丛书各册教材，在基础理论讲授之后，每篇均加列“技能训练”专章，通过采用典型案例分析、模拟操作等形式，引导学生对本篇的重点、难点内容进行分析、讨论、练习和模拟训练；每章结束后针对本章重点内容设计了“个案分析、学以致用、讨论思考”等项目，以达到强化学生对基础理论和业务环节处理技巧的掌握。这些新增加的关于“能力培养”和“技能训练”等新内容，约占整本教材篇幅的1/3，体现了国家对职业教育课程改革的诉求。这种编写体例的运用在目前经济类课程的教材中还较少见，希望这种新的尝试能经日后的教学实践验证，是一种“能力培养”和“创新教育”的有效方法。

2. 改革人才培养模式，尝试教学模式与教法创新

《规划纲要》要求各高职院校不断创新人才培养模式，“深化教育教学改革，创新教育教学方法，探索多种培养方式”，“倡导启发式、探究式、讨论式、参与式教学，帮助学生学会学习。激发学生的好奇心，培养学生的兴趣爱好，营造独立思考、自由探索的良好环境”。为此，在本套教材的编写过程中，我们注意到国家对高职院校的这种改革要求，在编写方法上尽量运用提示、启发、引导、讨论和模拟等方法，其目的是使学生运用所学知识在进行初步的分析、综合、比较、分类后，达到将知识、技能抽象概括具体化，提高学生灵活分析和解决问题的能力。这样，既与国家对高职教育培养的目标相吻合，又适合学生的学习思维特点，并容易激发学生的学习兴趣，所以，较之传统的教学方法有了较大的改革与突破。

3. 建立综合性、实践性新课程，提高人才培养的针对性、实效性

江泽民同志在第三次全国教育工作会议上指出：“职业教育和成人教育要使学生在掌握必要的文化知识的同时，具有熟练的职业技能和适应职业变化的能力。”可见，现代职业教育呼唤综合型、应用型、技能型的新课程的设立。为反映这些要求，我们在每个专业都增设了《综合技能》课程，以此作为经济管理类各专业实践课的应用教材。该科目在内容上以各专业的主要业务为线索，将骨干核心课程的知识高度浓缩，有机串联。将主干课中没有系统讲授而实际工作中必然涉及的知识纳入其中，弥补了原来系列教材的欠缺与不足。同时，该系列教材大量采用模拟教学和案例教学，让学生以“业务员、经济师、总经理”的身份参与学习与训练，独自策划交易，进行经济活动等，刻意营造一种仿真情境，让学生在“训练”中学习，在“情景”中增长才干和积累经验，有效地将知识转变为专业性的技能技巧，提高其解决和处理实际问题的综合能力。总之，各专业《综合技能》的设立，是按照国家对教育学科的设置“要多增加综合课”的要求而设立的新型试验科目，其主要目的是通过运用灵活有趣的模拟训练及案例教学等手法，启发诱导学生的立体思维，全面提高其独立操作经济业务的综合实践能力。由于是初次尝试，所以希望大家多加关注，并提出指导性的建议。

本套丛书的编写，得到了有关院校领导和学者、教授的大力支持，并引用了有关作者的部分资料，在此一并表示谢意。

本套丛书无论从体例安排到内容设置，从知识点的归纳到教法的运用，都进行了大胆探索和尝试，意欲为我国财经类高职高专教材的编写与探索尽微薄之力，但由于时间和水平有限，疏漏和不足甚至是错误在所难免。希望广大教师、读者多提宝贵意见，以便日后充实与完善。

工学结合新视野高职高专“十二五”规划教材编委会

2010 年 8 月

前　言

电子商务作为一种新的生产方式，正在显示其巨大的现代经济管理的价值和社会变革的影响力。随着互联网的应用日趋广泛，世界经济向全球化和信息化方向发展成为新世纪鲜明的特征和趋势，人类社会开始跨入一个全新的网络经济时代，这是现代社会发展的必然。网络经济时代的到来，标志着一个以互联网为基础的网络虚拟市场开始形成，这是一个具有全球性、数字化、跨时空等特点的飞速增长和潜力巨大的新兴市场。面对这样一个自身在不断变化着的全新的网络虚拟市场，安全问题一直是电子商务用户特别关注的主题。对于电子商务的应用而言，安全与风险一直伴随着商务运作的全过程，如何使电子商务运作过程的安全性和风险控制得到保证，是关系到电子商务能否顺利发展的关键问题，也成为电子商务人士越来越关注的问题。因此，保障电子商务安全是实施电子商务的关键环节，在推进电子商务进一步发展的过程中起着举足轻重、不可低估的作用。电子商务的安全问题是一个庞大的系统性工程，必须在具体实施过程中采取综合防范的思路，从技术、管理、政策、法律法规等诸多方面提供一套完备的安全解决方案，如此才能为交易和支付活动提供富有保障的商务安全环境。

由于我国电子商务的发展起步总体较晚，相应的安全理论体系还未完善，安全策略也相对滞后，安全技术的应用水平较低，而且与之相关的研究成果及其实践积累不多，与此相关的人才十分匮乏，特别是缺少既掌握电子商务安全的基本理论，又熟悉安全技术实际操作的实用型人才。各类高等院校作为培养电子商务安全管理人才的主要机构，迫切需要相关且适用的教材来承担教学和传播知识的任务。

本书作为电子商务的系列教材之一，遵循了“立足基础、联系实际、注重实用、体系完善”的指导原则，在结构设计、内容组织、章节安排上突出自己的特点。它从电子商务安全以及网络安全出发，首先介绍了防火墙和入侵检测技术，接着论述了密码技术与数字签名问题，然后讲述了公钥基础设施及应用，随后系统讲述了安全电子支付技术、移动电子商务安全、开放系统中的商务风险与管理，最后讲解了电子商务安全评估与法律保护问题。

本书系统性强，内容丰富，注重基础理论的呈现，克服了理论分析过深问题，减少了相关公式推导，突出了针对性和实用性，使之特别适合高职高专的培养目标和教学特点。特别是每章前面都配有“任务驱动”和“先行案例”等内容，后面都设有与本章内容相关的“关键术语”、“知识窗”和“学以致用”等环节，这样既有利于开阔学生的视野，又有利于培养学生联系实际来分析问题和解决问题的能力。

本书由王鑫担任主编，刘天宝、陈照义、陈洪梅为副主编。其中王鑫编写第1、2、9章，刘天宝编写第3～4章，陈照义和王涛编写了第5～6章，陈洪梅和袁淑玲编写了第7～8章。

本书在编写过程中，参考和引用了国内许多相关专家的著作、教材和有关资料，作者已尽可能在参考文献中列出，在此谨向他们表示衷心的感谢。

由于编者水平有限，书中缺点、错误在所难免，欢迎学者、同仁以及使用本教材的老师和同学们批评指正。

目　录

第1章　电子商务安全概述

课前准备

【任务驱动】

资源的共享、快速、便捷是电子商务迅速发展的原因，而这种基于 Internet 网络的开放性使电子商务在安全方面先天不足。现在，电子商务的安全问题越来越突出，已经成为制约电子商务快速发展的障碍。如何保障电子商务活动的安全，一直是电子商务研究的核心问题。通过本章学习，学生能够理解电子商务安全的基本概念，了解电子商务面临的安全问题，掌握电子商务的基本安全需求，熟悉电子商务安全的基础知识，并能够说明电子商务安全管理的基本思路和方法。

【先行案例】

2006 年年初，张某在国内一家著名的购物网站上看到有卖家出售联通的 CDMA 包年上网卡，其价格比在营业厅里购买的至少便宜数百元。随后，张某查看了售卡者的信用记录，发现该卖家在此之前已经出售过同一品种的上网卡数十张，且买家都给予了不错的反馈。于是，张某便拍下了一张上网卡。他很快得到了卖家“妖言媚惑”的回应。在短短的十几分钟内，张某和这位叫做“妖言媚惑”的卖家完成了交易。张某得到上网卡的卡号和密码后便开始使用，一切都很正常。按照通常的交易习惯，张某为“妖言媚惑”做出了评价，并将货款全部结清。

一个月后，张某发现自己的上网卡竟然欠费不能继续使用了。他马上联系了当时的那位卖家“妖言媚惑”，然而，对方的电话无法接通，张某尝试了对方所有的联系方式均告失败。张某开始意识到，自己可能被骗了。无奈之下，张某联系了网站的投诉部门，没想到网站也在寻找此人，被骗的人不只张某一个。此时，“妖言媚惑”却已在网上消失得无影无踪。

通过警方和网站的协同努力，真相开始浮出水面。原来，张某所使用的这张上网卡不过是一张包月卡。卖家“妖言媚惑”在联通营业厅办理了一批 198 元和 298 元的包月业务，然后以包年卡的形式从各大网站廉价抛售，每张卡卖 1 500 元左右。2 月份“妖言媚惑”不再为这些包月卡续费，这些卡就到期了。“妖言媚惑”在网站上总共出售了价值 10 万余元的“包年卡”，受骗网友达数十人。

张某认为网站应该承担部分责任，毕竟他是冲着网站的名气和声望才会如此轻信

“妖言媚惑”。网站方面却表示在此案中他们并不负有责任，网站只是为大家提供交易平台，交易过程中的细节性问题需要网友自己留意，何况在当初注册前的协议条款中早已写明，网站在此类纠纷中是免责的，如果要追偿的话必须找到“妖言媚惑”本人。可查找“妖言媚惑”的下落并非易事，此人在网站上留下的信息均是伪造的。说到身份确认，张某认为网站方面是存在问题的。张某本人非常信任网站的身份审核，他本人也是提供了身份证明后，才获得在网站上出售商品的许可，但在“妖言媚惑”的案件中，明显网站的身份审核工作没有到位，因为对方使用的是假的身份证明。

“妖言媚惑”改变了张某对网络购物的一贯看法，原本张某还是抱着“天下无贼”的想法去购物的，但经历过此事后，张某在网络上购物时谨慎多了，他表示以后可能不大会去购买金额较大的物品了。尽管网站方面认为自己没有过错，但是张某仍然认为是他们的信用体系存在漏洞，才会导致自己遭受那么大的损失，既然从法律角度讲网站没有责任，那么只好自认倒霉。

教学内容

1.1 电子商务安全的概念及特点

电子商务（Electronic Commerce，E-Commerce）是指实现整个贸易过程中各阶段贸易活动的电子化，从涵盖范围方面可以定义为：交易各方以电子交易方式而不是通过当面交换或直接面谈方式进行的任何形式的商业交易；从技术方面可以定义为：E-Commerce 是一种多技术的集合体，包括交换数据（如电子数据交换、电子邮件）、获得数据（如共享数据库、电子公告牌）以及自动捕获数据（如条形码）等。它具有广告宣传、咨询洽谈、网上订购、网上支付、电子账户、商品/服务传递、意见征询和交易管理等各项功能。

1.1.1 电子商务安全的概念

随着 Internet 的发展，电子商务已经逐渐成为人们进行商务活动的新模式。越来越多的人通过 Internet 进行商务活动。电子商务的发展前景十分诱人，而其安全问题也变得越来越突出。如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，商家和用户都十分关心。安全问题成为电子商务发展的核心和关键问题，也是电子商务发展的瓶颈问题。首先要明白电子商务安全概念的核心内涵，以及当前的安全处境，即面临的威胁和安全需求，才能正确认识电子商务的安全问题，才能健康地使用和发展电子商务，才能既在电子商务中得益，又不被安全威胁所害。

电子商务的一个重要技术特征是利用 IT 技术来传输和处理商业信息。因此，电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

计算机网络安全的内容包括：计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，

以保证计算机网络自身的安全为目标。

商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，保障以电子交易和电子支付为核心的电子商务过程的顺利进行，即实现电子商务保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起。没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。

电子商务安全是以网络安全为基础。但是，电子商务安全与网络安全又是有区别的。首先，网络不可能绝对安全，在这种情况下，还需要运行安全的电子商务。其次，即使网络绝对安全，也不能保障电子商务的安全。电子商务安全除了基础要求之外，还有特殊要求。

从安全等级来说，从下至上有计算机密码安全、局域网安全、互联网安全和信息安全之分，而电子商务安全属于信息安全的范畴，涉及信息的机密性、完整性、认证性等方面。这几个安全概念之间的关系如图 1－1 所示。同时，电子商务安全又有它自身的特殊性，即以电子交易安全和电子支付安全为核心，有更复杂的机密性概念，更严格的身份认证功能，对不可拒绝性有新的要求，需要有法律依据性和货币直接流通性特点，还需要有网络没有的其他服务（如数字时间戳服务）等。

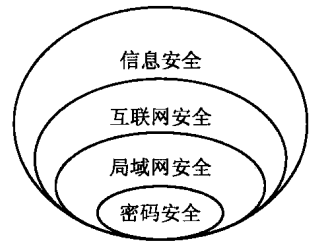

图 1－1　安全概念基本关系示意图

1.1.2　电子商务安全的特点

电子商务安全具有如下四大特点。

1. 电子商务安全是一个系统概念

电子商务安全问题不仅仅是个技术性的问题，更重要的是管理问题，而且它还与社会道德、行业管理以及人们的行为模式都紧密地联系在一起。

2. 电子商务安全是相对的

不能追求一个永远也攻不破的安全系统，安全与管理始终是联系在一起的。也就是说，安全是相对的，而不是绝对的，要想以后的网站永远不受攻击、不出安全问题是不可能的。

3. 电子商务安全是有代价的

无论是 BtoB 还是 BtoC，都要考虑到安全的代价和成本问题。如果只注重速度，就必定要以牺牲安全来作为代价；如果要考虑到安全，速度就得慢一点。当然这与电子商务的具体应用有关，如果不直接牵涉到支付等敏感问题，对安全的要求就可以低一些；如果牵涉到支付问题，对安全的要求就要高一些，所以安全是有成本和代价的。作为一个经营者，应该综合考虑这些因素；作为安全技术的提供者，在研发技术时也要考虑到这些因素。

4. 电子商务安全是发展的、动态的

今天安全，明天就不一定安全，因为网络的攻防是此消彼长、“道高一尺魔高一丈”的事情，尤其是安全技术，它的敏感性、竞争性以及对抗性很强，需要不断地检查、评估和调整相应的安全策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.2 电子商务面临的安全问题

电子商务作为一种全新的商务运作模式，为全球客户提供丰富的商务信息、简捷而快速的交易过程和低廉的交易成本。但是电子商务在给人们带来方便的同时，也带来了种种安全问题。

具体来说，电子商务面临的安全问题表现在电子商务网络系统自身的安全问题、电子商务交易信息传输过程中的安全问题、电子商务企业内部安全管理问题、电子商务安全法律保障问题、电子商务的信用安全问题、电子商务安全支付问题6个方面。

1.2.1 电子商务网络系统自身的安全问题

电子商务是在Internet上实现的商务活动。在开放的Internet上进行电子商务活动时，必然会涉及一般计算机网络系统普遍面临的一些安全问题，主要表现在以下6个方面。

1. 物理实体的安全问题

物理实体的安全问题主要包括以下5种。

（1）设备的机能失常。任何一种设备都不是十全十美、万无一失的，或多或少都存在着这样或那样的缺陷。设备会出现一些比较简单的故障，而有些则是灾难性的。部分简单故障，特别是周期性故障，往往比那些大的故障更难于查找与修复。有些故障是当它们破坏了系统数据或其他设备时才被发现，而这时往往为时已晚，后果也是非常严重的。

（2）电源故障。由于各种意外的原因，网络设备的供电电源可能会突然中断或者产生较大的波动，这可能会突然中断计算机系统的工作。如果这时正在进行某些数据操作，这些数据很可能会出错或丢失。另外，突然断电对系统硬件设备也会产生不良后果。

（3）由于电磁泄漏引起的信息失密。计算机和其他一些网络设备一样大多数都是电子设备，当它工作时会产生电磁泄漏。一台计算机就像一部电台，带有信息的电磁波向外辐射，尤其视频显示装置辐射的信息量最强，用先进的电子设备在一公里之外的地方就能接收到。电子通信线路同样也有辐射。这样，非法侵入者就可以利用先进的接收设备窃取网络机密信息。

（4）搭线窃听。这是非法者常用的一种手段，即将导线搭到无人值守的网络传输线路上进行监听，通过解调和正确的协议分析可以完全掌握通信的全部内容。

（5）自然灾害。计算机网络设备大多是“易碎品”，不能承受重压或强烈的震动，更不能承受强力冲击。所以，各种自然灾害，如地震、风暴、泥石流、建筑物破坏等，

对计算机网络系统也构成了严重的威胁。另外，计算机设备对环境的要求也很高，如温度、湿度、各种污染物的浓度等，所以要特别注意火灾、水灾、空气污染等对计算机网络系统所构成的威胁。

2. 计算机软件系统潜在的安全问题

不论采用什么操作系统，在默认安装的条件下都会存在一些安全问题。只有专门针对操作系统的安全性进行相关和严格的安全配置，才能达到一定的安全程度。我们一定不要以为操作系统默认安装后，再配上很强的密码系统就是安全的。

网络软件的漏洞和“后门”是进行网络攻击的首选目标。随着现代软件系统越来越复杂，对于一个软件，特别是较大的系统或应用软件，要想进行全面彻底的测试已经变得越来越困难了。虽然在设计与开发一个大型软件的过程中可以进行某些测试，但总会多多少少留下某些缺陷或漏洞。这些缺陷可能长时间也发现不了，而只有当被利用或某种条件得到满足时，才会显现出来。目前最常用的一些大型的软件系统，例如 Windows 系列和一些 UNIX 系统软件，以及 MS Internet Explorer 和 Netscape Communicator 等大型应用软件，都不断被用户发现有这样或那样的安全漏洞。另外，对于网站或软件供应商专门开发的一些 CGI 程序，很多都存在着严重的漏洞。对于电子商务站点，可能会由此导致恶意攻击者冒用他人账号进行网上购物等严重后果。

3. 网络协议的安全漏洞

网络服务一般都是通过各种各样的协议完成的，因此网络协议的安全性是网络安全的一个重要方面。如果网络通信协议存在安全上的缺陷，那么攻击者就有可能不必攻破密码体制即可获得所需要的信息或服务。值得注意的是，网络协议的安全性是很难得到绝对保证的。目前协议安全性的保证通常有两种方法：一种是用形式化方法来证明一个协议是安全的；另一种是设计者用经验来分析协议的安全性。形式化证明的方法是人们所希望的，但一般的协议安全性也是不可判定的。所以，对复杂的通信协议的安全性，现在主要采用找漏洞分析的方法。无疑，这种方法有很大的局限性。实践证明，目前 Internet 提供的一些常用服务所使用的协议，例如，Telnet、FTP 和 HTTP 协议在安全方面都存在一定的缺陷。当今，许多黑客的攻击都是利用这些协议的安全漏洞才得逞的。实际上，网络协议的漏洞是当今 Internet 面临的一个严重的安全问题。

4. 黑客的恶意攻击

随着电子商务的兴起，对网站的实时性要求越来越高。早在 2001 年年初，全世界传媒都在关注美国著名网站被袭事件。在这次事件中，包括 Yahoo、Amazon、eBay、ZDNet、CNN 在内的美国主要网站接连遭到黑客的攻击，这些网站被迫中断服务数小时。据估算，造成的损失达到 12 亿美元以上。这次袭击事件不仅使著名商业网站受到安全重创，更使公众对网络安全的信心受到重创。以网络瘫痪为目标的袭击效果比任何传统的恐怖主义和战争方式都来得更强烈，破坏性更大，造成危害的速度更快，范围也更广；而袭击者本身的风险却非常小，甚至可以在袭击开始前就已经消失得无影无踪，使对方没有实施报复打击的可能。

所谓黑客，现在一般泛指计算机信息系统的非法入侵者。黑客的出现可以说是当今信息社会，尤其是在 Internet 互联全球的过程中，网络用户有目共睹、不容忽视的一个

独特现象。黑客们在世界各地四处出击，寻找机会袭击网络，几乎到了无孔不入的地步。黑客攻击，目前已成为计算机网络所面临的重大威胁，无论个人、企业还是政府机构，只要进入计算机网络，都会感受到黑客带来的网络安全威胁。大至国家机密，小到个人隐私，以及商业秘密，都随时可能被黑客发现并窃取或公布。

黑客的攻击手段和方法多种多样，一般可以粗略地分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。

5. 计算机病毒攻击

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义："计算机病毒，是指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。"

目前全球出现的数万种病毒按照基本类型划分，可归为引导型病毒、可执行文件病毒、宏病毒、混合病毒、特洛伊木马型病毒和 Internet 语言病毒 6 种类型。

计算机病毒作为一种具有破坏性的程序，往往会尽可能将自身隐藏起来，保护自己，但是病毒最根本的目的还是达到其破坏目的。在某些特定条件被满足的前提下，病毒就会发作，这就是病毒的破坏性。有些病毒只是显示一些图片、放一段音乐或者开个玩笑，这类病毒属于良性病毒；而有些病毒则含有明确的目的性，像破坏数据、删除文件、格式化硬盘等，这类病毒属于恶性病毒。计算机病毒的破坏行为体现了病毒的杀伤能力，病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能力。

6. 安全产品使用不当

虽然不少网站采用了一些网络安全设备，但由于安全产品本身的问题或使用问题，这些产品并没有起到应有的作用。很多厂商的安全产品对配置人员的技术背景要求很高，超出对普通网络管理人员的技术要求。尽管厂商最初给用户做了正确的安装、配置，但是一旦系统改动，需要改动相关安全产品的设置时，很容易产生许多安全问题。

1.2.2 电子商务交易信息传输过程中的安全问题

1. 信息机密性面临的威胁——信息在传输过程中被窃取

如果没有采用加密措施或加密强度不够，攻击者可能通过互联网、公共电话网、搭线、在电磁波辐射范围内安装截收装置等方式，截获传输的机密，或通过对信息流量和流向、通信频度和长度等参数的分析，推出如消费者的银行账号、密码及企业的商业机密等有用信息。

2. 信息完整性面临的威胁——信息在传输过程中被篡改、删除或插入

当攻击者熟悉网络信息格式以后，通过各种技术方法和手段对网络传输的信息进行选择修改，并发往目的地，从而破坏信息的完整性。这种破坏手段主要有以下三个方面：

篡改——改变信息流的次序，更改信息的内容，如购买商品的出货地址、交货日