



“十三五”职业教育国家规划教材

电子商务支付与安全

(第5版)

电子工业出版社版权所有
盗版必究

主 编◎臧良运

副主编◎周晓菊 朱甜甜 纪香清

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本教材按照高等职业教育“以服务为宗旨，以就业为导向”的培养目标，通过对电子商务支付与安全的基本概念、基本理论的介绍，以及经典案例的解读，全面系统地阐述了支付和安全在电子商务领域中的应用。本教材内容共分 9 个模块，以电子交易与支付为核心，叙述了电子支付工具、网络金融知识及应用；从电子商务系统的安全角度出发，详细叙述了技术层面的网络安全技术、安全协议与认证的内容，并介绍了电子商务支付的法律保障。本教材采取了模块、单元和工学结合、任务驱动相结合的编写体例，在每个单元开篇，用“情景案例”对任务进行描述，在“任务思考”中提出问题，在“任务分析”中简要分析解决方法和思路，通过“相关知识”阐述理论知识，并插入“课程思政”元素和相关链接，最后由课堂讨论、案例分析、实务训练和课后拓展等组成“实践训练”来检验学习效果，以提高学生的动手能力。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

电子商务支付与安全 / 臧良运主编. —5 版. —北京：电子工业出版社，2022.5

ISBN 978-7-121-43441-9

I. ①电… II. ①臧… III. ①电子商务—支付方式—安全技术—高等教育—教材 IV. ①F713.363

中国版本图书馆 CIP 数据核字（2022）第 078333 号

责任编辑：贾瑞敏

文字编辑：杜 皎

印 刷：

装 订：

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：787×1092 1/16 印张：15 字数：384 千字

版 次：2006 年 1 月第 1 版

2022 年 5 月第 5 版

印 次：2022 年 5 月第 1 次印刷

定 价：49.80 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）88254888，88258888。

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

本书咨询联系方式：（010）88254019，jrm@phei.com.cn。

《电子商务支付与安全》第1版于2006年1月出版，被评为第一批普通高等教育“十一五”国家规划教材。第2版被评为职业教育“十二五”国家规划教材，第4版被评为职业教育“十三五”国家规划教材。教材的优点是知识技能先后有序、知识积累循序渐进、教学体系严谨，符合当前的职教形势和生源特点。

电子商务的发展日新月异，高等职业教育人才培养方案也发生了很大的变化，课程改革对教材提出了更高的要求。为了适应新形势下电子商务专业的发展要求，《电子商务支付与安全（第5版）》进行了较大的修改。

本教材内容及时反映产业升级和行业发展要求，体现了新知识、新技术、新工艺和新方法，符合《职业院校教材管理办法》和《“十四五”职业教育规划教材建设实施方案》规定的编写要求。除此之外，本教材与前几版以及其他同类教材相比，具有以下四个特点。

1. 内容符合高职人才培养方案

教材内容力求体现“以就业为导向，以能力为本位”的精神，注重对学生技能的培养，整合理论知识，合理安排知识点、技能点，注重实训教学，突出对学生实际操作能力和解决问题能力的培养，强化实际工作任务培训，与学生考证相结合。

结合课程内容，增加了“课程思政”栏目。

2. 体现了新知识、新技术、新工艺和新方法

教材根据当前电子商务的实际工作的发展和需要进行了调整：原有的模块六与模块七部分内容整合为数字认证技术，补充了移动支付、第三方支付、数字货币、虚拟货币、《电子商务法》等新知识；模块四增加了互联网众筹单元；对于难度太大的内容，如密码技术、安全协议的原理等知识点进行了调整。

教材对部分案例和内容进行了更新，案例、课外拓展、相关链接等内容都采用了二维码链接新技术，便于学生学习。

3. 贯彻理论实践一体化的教学思想

教材在内容安排上，将“任务”贯穿始终，通过解决电子商务支付和安全的实际工作问题，讲解理论，培养学生的技能。

(1) 体例实用化：每个单元构建了情景案例、任务思考、任务分析、相关知识、相关链接、实践训练等板块；每个模块后有知识小结和练习测试；符合“工学结合”和任务驱动的教学理念。实践训练包括课堂讨论、案例分析、实务训练和课后拓展，即学即用。

(2) 任务形象化：情景案例和任务思考的内容都是学生日常遇到的实际问题，能够激发学生的学习兴趣，有利于教师教学的展开，便于学生解决实际工作中的具体问题。

(3) 逻辑图表化：本教材运用了大量的图表说明任务的解决方案和流程，减少了文字叙述，具有很强的直观性和可读性。

(4) 版式生动化：本教材的版式、插图等新颖、生动，具有良好的视觉效果。



4. 配套资源丰富

本教材提供丰富的教学配套资源。为更好地发挥教材的作用，体现以人为本的教育理念，提高学生的学习兴趣和调动学生学习的积极性和主动性，本教材提供了系列配套教学辅助资源（可到华信教育资源网下载）。

(1) 提供课程手册，包括教学大纲及教学活动设计，可供教师备课时使用。

(2) 制作精致的多媒体电子教案，可在教学时直接使用，也可供教师根据具体需要加以修改，满足多媒体教学的需要。

(3) 提供课后练习测试题的参考答案，模拟试卷与参考答案，方便教师选用。

本教材共分 9 个模块，模块一为电子商务支付与安全概述，模块二为电子商务支付系统，模块三为电子商务支付工具，模块四为网络金融，模块五为电子商务系统的安全，模块六为网上支付安全与加密技术，模块七为数字认证技术，模块八为电子支付安全协议，模块九为电子商务支付与安全的法律保障。

本教材是集体劳动的成果，由多所高校教师共同承担编写任务。本书由臧良运教授担任主编，并负责拟订编写提纲、统稿和定稿；周晓菊、朱甜甜和纪香清任副主编。模块一、模块二由贺州学院臧良运老师编写，模块三、模块四由青岛大学纪香清老师编写，模块五、模块六和模块七由福州理工学院朱甜甜老师编写，模块八、模块九由山西经济管理干部学院周晓菊老师编写。在教材的编写过程中，得到了各位作者所在学校的大力支持，对前几版的作者青岛职业技术学院刘春侠、西安工业学院张娟、黄河水利职业技术学院陈萱老师做出的贡献，一并表示感谢！

本教材在编写过程中参考了大量相关领域的文献，已在书后参考文献中列出，但仍可能有遗漏。在此谨向已标注和未标注的参考文献的作者表示诚挚的谢意。

由于编者水平所限，书中难免出现疏漏和不妥之处，敬请广大读者和专家批评指正。

臧良运

模块一 电子商务支付与安全概述	1
第一单元 电子商务支付	2
一、网上支付的产生和发展	3
二、电子商务支付面临的问题	5
三、网上支付的运行环境	6
四、网上支付流程	6
第二单元 电子商务安全	9
一、电子商务面临的安全威胁	10
二、电子商务安全要素	12
三、电子商务安全技术	13
四、电子商务安全体系结构	15
五、电子商务安全法律要素	16
第三单元 安全电子商务支付	18
一、电子商务支付的安全问题	19
二、安全电子商务支付的途径	21
三、安全电子商务支付的意义	22
知识小结	23
练习测试	24
模块二 电子商务支付系统	25
第一单元 电子商务支付系统概述	26
一、电子商务支付系统的构成	28
二、电子商务支付系统的功能	29
三、电子商务支付系统的安全要求	30
四、电子商务支付手段	31
第二单元 电子商务支付系统应用	33
一、ATM 系统	34
二、POS 系统	36
三、电子汇兑系统	38
四、网上支付系统	39
第三单元 第三方电子商务支付系统与移动支付	41
一、银联在线支付平台	42
二、支付宝	43



三、首信易支付	44
四、网银在线	45
五、PayPal	45
六、快钱	45
七、财付通	45
八、易宝支付	46
九、移动支付	46
知识小结	48
练习测试	48
模块三 电子商务支付工具	50
第一单元 电子货币	51
一、电子货币概述	51
二、电子货币分类	53
三、电子货币的职能与作用	53
四、电子货币的发展现状	54
第二单元 银行卡	56
一、银行卡概述	57
二、信用卡	58
三、借记卡	58
四、金融 IC 卡	58
五、中国银联	59
六、国际信用卡及其发卡组织	60
第三单元 网络货币	62
一、信用卡型网络货币	63
二、电子现金	65
三、电子支票	67
四、电子钱包	69
五、微支付	71
知识小结	73
练习测试	74
模块四 网络金融	76
第一单元 网上银行	77
一、网上银行的产生	78
二、网上银行的类型	79
三、网上银行服务	79
四、网上银行的安全	82
第二单元 网上证券	84
一、网上证券交易概述	85
二、网上证券交易模式和系统	85
三、网上证券交易的基本方法	87



四、网上证券投资的步骤	89
五、网上证券交易的资金支付	90
第三单元 网上保险	92
一、网上保险的主要内容	93
二、网上保险系统	95
三、网上保险经营模式	98
第四单元 互联网众筹	101
一、互联网众筹	102
二、互联网众筹的模式	102
三、互联网众筹的安全	104
知识小结	106
练习测试	107
模块五 电子商务系统的安全	108
第一单元 安全问题的产生	109
一、网络中支付信息的保密性	110
二、网络中支付信息的完整性	111
三、交易信息的不可否认性	111
四、交易双方身份的真实性	111
第二单元 网络攻击	112
一、计算机病毒	113
二、口令破解	116
三、拒绝服务攻击	117
四、网络监听工具	118
第三单元 交易环境的安全性	120
一、客户机的安全性	121
二、通信信道的安全性	121
三、服务器的安全性	121
四、网上银行和手机银行的安全性	122
知识小结	124
练习测试	125
模块六 网上支付安全与加密技术	126
第一单元 网络安全防范	127
一、网络安全规划	127
二、防火墙技术	128
三、计算机病毒的防治与管理	130
四、物理安全控制	132
五、移动端安全解决方案	133
第二单元 加密技术	135
一、信息加密原理	137
二、私有密钥密码技术	138



三、公开密钥密码技术	138
第三单元 公开密钥基础设施	140
一、PKI 的组成	140
二、PKI 的原理和功能	141
知识小结	144
练习测试	144
模块七 数字认证技术	146
第一单元 数字签名	147
一、数字签名	147
二、数字时间戳	149
第二单元 身份认证与认证技术	151
一、身份认证	152
二、认证技术	153
第三单元 数字证书与认证机构	157
一、数字证书的概念	157
二、数字证书的内容	158
三、数字证书的安装和使用	159
四、数字证书的类型	159
五、认证机构	161
知识小结	164
练习测试	164
模块八 电子商务支付安全协议	166
第一单元 安全协议概述	167
一、电子商务安全体系	167
二、HTTP 协议简介	169
第二单元 安全套接字层	172
一、安全套接字层概述	173
二、SSL 工作流程	175
第三单元 安全电子交易协议	179
一、SET 协议简介	180
二、SET 协议的目标和特点	180
三、SET 安全协议涉及的对象和技术范围	181
四、SET 协议的工作原理	182
五、SET 协议的不足之处	183
六、SSL 协议和 SET 协议的比较	184
第四单元 其他电子商务支付协议简介	185
一、Digicash 协议	186
二、First Virtual 协议	187
三、Netbill 协议	187
知识小结	188



练习测试	188
模块九 电子商务支付与安全的法律保障	190
第一单元 电子商务参与各方的法律关系	191
一、电子商务带来的法律问题	192
二、买卖双方当事人的权利和义务	194
三、网络交易中心的法律地位	195
四、关于网站经营者侵权的法律责任	196
五、网络交易客户与网上银行间的法律关系	196
六、认证机构在电子商务中的法律地位	197
第二单元 电子商务交易安全保护法	200
一、联合国对电子商务交易安全的法律保护	201
二、我国对电子商务交易安全的法律保护	207
第三单元 《电子签名法》和《电子商务法》概述	221
一、《电子签名法》概述	222
二、《电子商务法》概述	225
知识小结	228
练习测试	229

电子工业出版社版权所有
盗版必究

模块一



电子商务支付与安全概述



学习目标

知识目录

- 掌握电子商务支付的内涵、支付流程
- 了解电子商务安全威胁、防范技术和法律要素
- 掌握电子商务支付与安全对电子商务的作用

能力目录

- 掌握电子商务支付一般流程，了解其他支付工具的支付流程
- 对电子商务支付与安全有深刻认识

素质目录

- 激发并保持学习兴趣
- 养成良好的电子商务支付与安全的职业道德素养
- 具有严谨、规范的安全防范习惯



第一单元 电子商务支付



情景案例

中国内地第一笔互联网电子交易

张丽艳是寿城职业技术学院电子商务专业的一名大学生,喜欢电子商务,想在大学期间学好专业知识,毕业后在电子商务领域创业。她想了解中国电子商务交易的历史,在网上看到了以下资料。

1998年3月18日,在北京友谊宾馆,世纪互联通信技术有限公司向首都各新闻单位的记者宣布:中国内地第一笔互联网电子交易成功。为本次交易提供网上银行服务的是中国银行,扮演网上商家的是世纪互联通信技术有限公司。

中国内地第一笔互联网电子交易的时间是1998年3月18日下午3时30分。第一位网上交易的支付者是浙江电视台播送中心的王轲平;第一笔费用的支付手段是中国银行长城卡;第一笔支付的费用是100元;第一笔认购物品是世纪互联通信技术有限公司的100元上网机时。中国银行开展网上银行服务的最早时间是1996年。1997年底,王轲平发现这个站点,并填写了申请书。在接到王轲平的申请后,世纪互联通信技术有限公司开始着手进行这次交易的筹备,实质性的时间大约为15天。王轲平成为第一个在互联网上进行电子商务交易的中国人。这次交易也是国内企业与消费者在网上的“第一次亲密接触”。



任务思考

张丽艳看后,产生了以下疑问:如果王轲平没有长城卡,那他如何完成这次交易?如果现在要完成这样的交易,需要有哪些结算手段?怎样确保世纪互联通信技术有限公司能安全收到王轲平支付的100元?王轲平的其他信息会被泄露给第三者吗?目前电子交易的支付安全吗?现在进行这样的一笔电子交易还需要15天的时间吗?周围的同学进行过电子商务和电子商务支付活动吗……

张丽艳产生的这些疑问,实际上就是和电子商务支付与安全相关的一系列问题。



任务分析

迄今为止,商品交易经历了原始的物物交换、简单商品交换和发达商品交换三种形式与阶段。随着网络技术的发展,电子商务已经渗透到了各行各业,对以货币为媒介的传统商品交换活动产生了巨大的冲击。

从商业角度看,电子商务是指用互联网作为商务平台实现整个商业贸易活动的电子化。从涵盖范围来看,电子商务指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。

电子商务经过多年的快速发展,电子商务支付,即网上支付,已经越来越被人们所知所用。在网上购买火车票、飞机票,在网上交纳水费、电费、煤气费、电话费已经非常普遍,支付宝、

财付通和手机本身的移动支付等电子商务支付平台争夺电子商务支付市场，电子商务支付逐渐成为人们关注的热点。网上支付促进了电子商务的发展，方便了人们的生活。那么，网上支付需要什么环境？网上支付的具体操作流程是什么呢？如何才能安全地进行网上支付结算呢？

在网上购买火车票、交纳电话费、购物等电子商务活动要成为一个完整的过程，网上支付及其安全是非常重要的。客户和商家之间不使用现金进行结算，而是使用信用卡、电子钱包、电子支票和电子现金等多种支付方式进行网上结算，省去了很多人员开销。网上支付能够即时到账，缩短了交易时间。与传统的现金结算相比，网上支付的手段更多，也更复杂，不同的支付工具的操作流程也是不一样的。

由于电子商务活动的参与者具有虚拟性，网上支付需要更为可靠的信息传输安全性控制，以防止欺骗、窃听、冒用等非法行为。对于网上支付的安全问题，现在已有技术来保证信息传输的安全性。



相关知识

随着电子商务市场的高速发展，电子商务支付已经成为消费者最重要的支付手段之一，电子商务支付行业呈现爆发式增长。自 2011 年以来，中国人民银行先后批准了超过 280 张第三方支付牌照，电子商务支付产业体系日趋完善。即便如此，还有千余家无证经营的支付机构在从事互联网电子商务支付活动。电子商务支付迎来了包括互联网支付企业、移动支付企业、预付卡企业、银行卡收单企业在内的更多运营主体的参与。

未来，电子商务支付的“全能化”将主要体现在“3A 服务”方面——Anytime（任何时间）、Anywhere（任何地方）和 Anyhow（任何方式）。服务的便利性、支付的安全性成为消费者认定电子商务支付优劣的两大重要指标。

一、网上支付的产生和发展

在网络经济时代，企业和客户对效率更高、安全性更高、成本更低的交易和支付方式的迫切需求，以及互联网的普及应用，使电子交易和电子商务支付得到迅猛发展。从根本上来讲，电子商务支付的产生源自电子交易。

1. 电子交易

所谓电子交易，就是指在网上进行交易。电子交易不是简单地开辟一条新的网上销售渠道，它采用电子技术手段改善企业经营模式，提高企业运营效率，进而增加企业收入；它将降低经营成本并帮助企业与客户、供货商及合作伙伴建立更为密切的合作关系。这样，企业不但能赢得客户的信任，更能提高订货效率、降低库存损耗、提高资金周转率和降低实际销售支出，进而降低成本、增加利润。电子交易也使人们足不出户就可以购买到物美价廉的商品和便捷舒心的服务。

与传统交易方式相比，电子交易具有以下几个优点。

(1) 电子交易超越了传统商务的四大障碍——地域障碍、时间障碍、价格信息对比障碍和更换供货商的障碍。电子交易的实施可使厂商真正提供 24 小时不间断服务和全天候营业，方便客户和优化服务，客户可以足不出户、随心所欲地浏览网页和订货，并具有更多的选择余地。

(2) 厂商可以根据客户浏览网页的习惯，掌握客户的喜好和消费模式，有助于调整产品结



构、生产和进货规划；同时，厂商的直销、广告、宣传和市场调查也可以不受地理位置的限制。

(3) 降低企业内部人与人之间的互动成本。

(4) 减少中间流通环节，实现零库存，降低成本，从而可让用户和厂商双双得利，也有利于遏制假货的出现。借助网络和众多的用户之间实现信息流通，扩大产品销路和选择低价优质的原料。

(5) 减少交通费用，减缓交通压力，节省差旅费用。

从 2013 年起，我国连续 7 年成为全球最大的网络零售市场，截至 2021 年 6 月，我国网络购物用户规模达 8.12 亿人，占网民整体的 80.3%。



相关链接

DELL 笔记本电脑网络交易流程

张丽艳考入寿城职业技术学院电子商务专业后，准备买一台笔记本电脑。她在对众多的笔记本电脑公司调查后，选中了一款。后来，张丽艳在 DELL 的网站上看到，此型号产品在网上购买，折后价比笔记本电脑公司的售价便宜 999 元，而且包括增值税和运费，还可以免费得到电脑包和鼠标。张丽艳最后决定在网上购买，操作步骤如下所述。

(1) 在百度上输入“DELL”，搜索 DELL 的网站主页，进入主页后，单击“笔记本电脑”图标。

(2) 找到要购买型号的笔记本电脑后，单击图标，按照网上提供的基本配置标准选定商品。

(3) 将商品放入购物车。在进入“放入购物车”界面后，单击“注册新账户”按钮。

(4) 系统生成了一份订单，并显示了报价单号和订单号。

(5) 在“支付宝”上按照要求进行注册，利用自己的中国邮政储蓄银行的借记卡支付。详细支付流程在模块二讲解。

张丽艳在 DELL 网站的购物流程如图 1-1 所示，一笔电子交易顺利完成。一周后，张丽艳收到了笔记本电脑。DELL 的这种网络直销模式，不仅促进了公司产品的销售，而且给消费者带来了很多的便利和实惠。



图 1-1 DELL 网站的购物流程

2. 电子商务支付

电子商务支付是指进行电子商务交易的当事人（包括消费者、厂商和金融机构）使用安全手段和密码技术，通过电子信息化手段进行的货币支付和资金流转。从广义上说，电子商务支付就是发生在购买者和销售者之间的金融交换，而这一交换方式往往借助银行或其他机构支持的某种电子金融工具完成，如电子现金、电子支票和电子银行卡等。它无须任何实物形式的标记，以纯粹电子形式的货币，一般以二进制数字的方式保存在计算机中。

信用卡专线支付结算方式在 20 世纪 70 年代就开始了，因此电子商务支付与结算方式的出

现要早于互联网的出现。20世纪90年代,随着互联网在全球的普及和应用,电子商务深入发展,标志着信息网络经济时代的到来。一些电子商务支付结算方式逐渐采用费用更低、应用更为方便的公用计算机网络,特别是将互联网作为运行平台,网上支付(Internet Payment)就应运而生了。本书所讲的电子商务支付,主要指的就是网上支付。

与传统的支付方式相比,电子商务支付具有以下优势。

(1) 电子商务支付适应整个社会向信息化、数字化发展的趋势。电子商务支付是通过网络以先进、安全的数字流转技术完成信息传输;而传统的交易支付方式则以传统的通信媒介通过现金、票据、银行兑汇等物理实体完成,无法满足信息社会高效、便捷的商务活动需求。

(2) 电子商务支付的工作环境是基于开放的系统平台(如互联网),而传统的交易支付方式则在较为封闭的系统中运行(如某银行的各分行之间)。工作环境的开放性使得商家加入电子商务支付系统更加方便快捷,没有障碍;而开放性带来的普遍性也使消费者可以随时随地进行消费支付活动。

(3) 电子商务支付是跨时空的电子化支付,能够真正实现全球每周7天24小时的服务保证。交易方只要有一台能够上网的计算机或手机,就可以足不出户,在很短的时间内完成整个支付过程。

(4) 电子商务支付有助于降低交易成本,最终为消费者带来更低的价格。传统的支付系统要求银行、银行职员、自动柜员机及相应的电子交易系统来管理现金和转账,成本非常高。而电子商务支付只需现有的技术设施、互联网和现有的计算机(手机)系统就可以,而且只需要少数系统维护人员。电子商务支付的交易效率较高,从而加快了资金周转速度,降低了企业的资金成本。

3. 电子商务支付发展历程

银行采用计算机等技术进行电子商务支付的形式有五种,分别代表电子商务支付发展的不同阶段。

第一阶段是银行利用计算机处理银行之间的业务,办理结算。

第二阶段是银行计算机与其他机构的计算机之间资金的结算,如代发工资等业务。

第三阶段是利用网络终端向客户提供各项银行服务,如自助银行。

第四阶段是利用电子付款机(POS机),即银行销售点终端,向客户提供自动扣款服务,这是现阶段电子商务支付的主要方式。在这一阶段,以各发卡行的行内授权系统为基础,全国银行卡信息交换中心和城市银行卡中心的建立为银行卡的跨行交互和跨行交易创造了条件,网络现行的支付系统也自然成为第五阶段网上支付的软件和硬件基础。

第五阶段是最新阶段,也是正在发展的阶段。电子商务支付可随时随地通过互联网进行转账结算,形成电子商务交易平台。这一阶段的电子商务支付又叫网上支付。

二、电子商务支付面临的问题

与传统支付相比,电子商务支付具有很大的优势。但就目前而言,电子商务支付仍然存在一些缺陷,限制了其发展,主要表现为以下方面。

(1) 安全性和支付信息私密性问题。这是一直困扰电子商务支付发展的关键问题。目前主要采用行政管理和计算机安全技术双管齐下的方法进行防范,如防止内部作案、建立安全认证体系、设立防火墙等。



(2) 对软件和硬件要求很高。电子商务支付一般要求有联网的计算机、服务器、相关的软件与配套设施和专业人员，而传统支付则没有这么高的要求。对于原来没有实现电子化办公、没有建设内部网的企业而言，一步到位实现电子商务支付的投入太高。

(3) 电子商务支付工具需要相应的系统支持。消费者选用的电子商务支付工具必须满足多个条件，首先要由消费者账户所在的银行发行，要有相应的支付系统和商家所在银行的支持，被商家认可。如果消费者的支付工具得不到商家的认可，电子商务支付还是难以实现的。而对消费者来说，同时持有各种流行的支付工具，也是不现实的。所以，电子商务支付的推广要求商家支持多种支付工具，各种电子商务支付系统能够相互兼容，实现系统互通。

三、网上支付的运行环境

电子商务支付是一种通信频次大、数据量不定、实时性要求较高、分布面很广的电子通信行为，因此电子商务支付的运行环境（网络平台）必须是交换型、通信时间较短、安全保密好且稳定可靠的通信平台，并面向全社会，对所有公众开放。

电子商务支付的常见网络平台有公用电话交换网、公用数据网、专用数据网、EDI（电子数据交换）专用网络平台及近年发展起来的互联网等。最早的电子商务支付网络平台主要有公用电话交换网、x.25 和 x.400 网络等，后来出现了 x.435、x.500 等网络平台。随着网络时代的到来，这些网络的普及面及速度都明显跟不上业务发展的需要，特别是不能支撑以互联网为平台的电子商务支付结算的需要。

目前，网上支付的支撑网络平台主要有两类：一类是传统成熟的 EDI 专用网上支付平台；另一类是大众化网络平台互联网，它们各有优缺点和应用环境。随着在各行各业的大规模普及应用，加上方便快捷、多媒体互动性强及经济的应用特点，大众化网络平台互联网已成为网上支付平台的发展趋势。EDI 正从专用网络逐渐向互联网转移，如 Web-EDI 的发展就是支付平台的关注热点，也体现出上述两个平台的融合趋势。所以，本书的叙述重点是基于互联网平台的电子商务支付。

四、网上支付流程

1. 网上支付结构

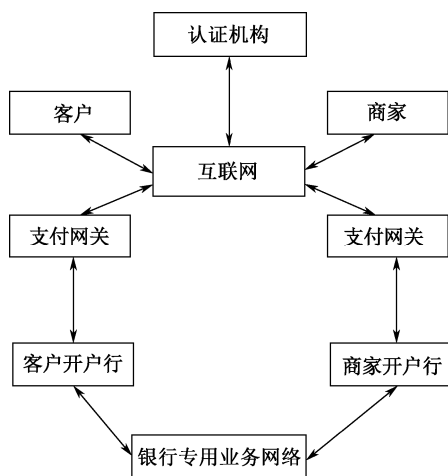


图 1-2 互联网网上支付平台结构

互联网网上支付平台主要由互联网、支付网关、银行专用业务网络三部分组成，其网络结构如图 1-2 所示。支付网关的作用是特殊而重要的，它是位于互联网和传统的银行专用网络之间，用于连接银行专用网络与互联网的一组专用服务器。设置支付网关的主要目的是安全连接互联网和银行专用网络，完成两者之间的通信、通信协议转换和进行相关支付数据的加密、解密，将安全性低的互联网上的交易信息传给内部封闭的、安全的银行专用网络，起到隔离和保护银行专用网络的作用。正是因为有了支付网关，互联网网上支付平台才安全可靠，大大方便了商家与客户对网上支付系统的应用，因为支付网关的运作对商家与客户来讲均是“透明”的，它由第三方或银行来研发

和运作。

2. 电子商务支付流程

电子商务支付借鉴了很多传统支付方式的机制和流程，只不过一个是运用传统纸质货币与票据，大多手工作业，另一个是运用电子货币，网上作业。基于互联网平台的网上支付结算流程与传统的支付结算流程是类似的。如果熟悉传统的支付结算方式，如纸质货币、支票、电子付款机等方式的支付结算过程，将有助于对网上支付结算流程的理解。例如，用户通过互联网进行电子商务支付的流程与目前商店中的销售点系统的支付结算流程非常相似，其主要不同在于，电子商务支付的客户通过计算机，以互联网服务器作为操作和通信的工具，而电子付款机支付结算使用专用刷卡机、专用终端和专线通信。

基于互联网平台的电子商务支付的基本流程如图 1-3 所示。

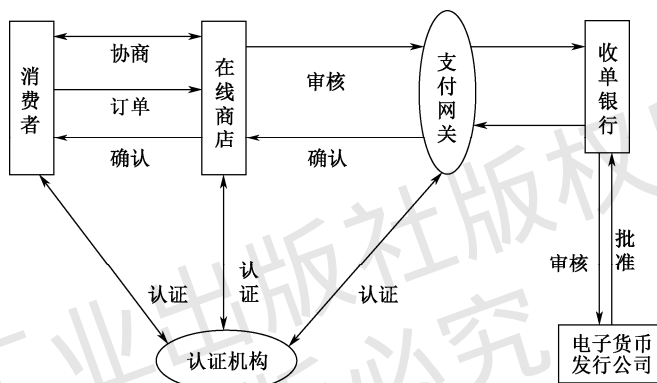


图 1-3 基于互联网平台的电子商务支付的基本流程

根据工作流程图，可将整个电子商务支付工作程序分为下面 7 个步骤。

- (1) 消费者利用自己的计算机通过互联网选定所要购买的物品，并在计算机上输入订单，订单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。
- (2) 通过电子商务服务器与有关在线商店联系，在线商店做出应答，告诉消费者所填订单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。
- (3) 消费者选择付款方式，如信用卡、电子钱包、电子现金、电子支票或网上银行账户等，确认订单，签发付款指令。此时安全电子交易协议开始介入。
- (4) 在安全电子交易协议中，消费者必须对订单和付款指令进行数字签名，利用双重签名技术保证商家看不到消费者的账户信息。
- (5) 在线商店接受订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再由电子货币发行公司确认。电子货币发行公司批准交易后，返回确认信息给在线商店。
- (6) 在线商店发送订单确认信息给消费者。消费者端软件可以记录交易日志，以备将来查询。
- (7) 在线商店发送货物，或提供服务，并通知收单银行将钱从消费者的账户转移到在线商店账户，或通知电子货币发行公司请求支付。

在认证操作和支付操作中间一般会有一个时间间隔。例如，在每天下班前请求银行工作人员结当天的账。



上面所讲的网上支付的基本流程只是对目前各种网上支付结算方式的应用流程的简单归纳,并不表示各种网上支付方式的应用流程与此一样。事实上,在实际应用中,各种网上支付方式的应用流程因技术、资金数量、管理机制不同而有所区别,但大致遵循该流程。不过,像信用卡、电子现金、网上银行账户的网上支付结算流程还是有所区别的。

网上支付流程还有一个特点,即实现的是资金立即支付,它适用于数目众多的较小金额的电子商务业务,对消费者与商家来说都是方便的。对较大金额的资金支付结算,如大企业与大企业之间的电子商务,实现互联网上的立即支付并不现实。在这种情况下,独立于商务交易环节的金融 EDI 或银行专业电子资金转账系统,还是目前被普遍采用的支付结算方式。



实践训练

1. 课堂讨论

- (1) 电子商务支付产生的根源是什么? 电子交易有哪些优点?
- (2) 什么是电子商务支付? 电子商务支付具有哪些优势, 存在哪些问题?
- (3) 电子商务支付的基本流程是什么?

2. 案例分析

比尔·盖茨曾断言“传统银行将成为 21 世纪即将灭绝的恐龙”,该结论未免有些夸张,至少在国内是不现实的。但是,银行的电子化能力确实远远落后于发展的需要,甚至可以说,正因为如此才造就了中国特色的电子商务支付业务。

飞速发展的互联网彻底颠覆了银行对持卡用户的传统服务思维,使之变得更加电子化、便捷化和个性化。网上银行是第一个由互联网推动而标准化的银行电子通道,接下来会是什么呢? 快捷无卡、IVR 语音、代收代付、空中发卡……无论如何,银行的电子通道将越来越丰富、越来越标准化。另外,这些电子通道的承载能力、安全保障、产品易用性、资费定价方式等需要大幅优化,才能满足“80 后”“90 后”主流用户急速膨胀的消费需求。

讨论与分析

传统银行的银行卡、网上银行等电子商务支付工具在电子交易过程中具有哪些优势和劣势,需要做哪些改进?

3. 实务训练

(1) 你进行过电子商务支付吗? 你下载过收费的彩铃吗? 搜索并登录一家音乐网站,找到你喜欢的彩铃,试着下载一首。你是怎么支付的? 与到营业厅交纳手机费相比,你认为这种电子商务支付有哪些优势?

- (2) 上网查找信用卡支付流程,画出流程图。

实训说明

- (1) 请同学们在课后完成本单元实训。
- (2) 对比银行卡和网上银行支付的异同。

4. 课后拓展

- (1) 上网查询你持有的银行卡和该银行网上银行的支付流程。

(2) 上网查询, 了解其他支付工具, 如信用卡、电子现金等的支付流程。

第二单元 电子商务安全



情景案例

拿什么拯救我们的“手机钱包”

随着电子商务的快速发展, 吃饭、打车、购物、看电影、充值、发红包……人们的日常行为已经与移动支付密不可分。与此同时, 一些不法分子也瞄准这一新生事物, 利用移动支付领域存在的技术漏洞以及监管不到位等从事诈骗活动, 且作案手段不断翻新, 令打击难上加难。

2022年1月, 北京市王先生收到一条某电商网站的推销短信, 是他以前浏览过的一家网店发来的, 其空调价格要比之前便宜近千元。王先生用手机扫描了店主发来的二维码后, 进入一个网页, 该网页与王先生以前浏览的官方网站非常相似。王先生进入一个支付界面, 输入银行账号和密码后却显示支付失败, 之后发现自己的银行账户被转走1万余元。



任务思考

通过上述情景案例可以发现, 网上支付安全是电子商务面临的重大安全问题。只有建设良好的电子商务安全系统, 才能保障网上支付的安全性, 促进电子商务的健康发展。

电子商务安全面临哪些威胁? 具体包括哪些安全要素? 技术方面应该采取什么防范措施? 管理方面应该怎么加强监管? 如何才能实现安全的电子商务? 如何才能使王先生遭遇的事件不再重演?



任务分析

随着互联网的发展, 电子商务已经逐渐成为人们进行商务活动的新模式。越来越多的人通过互联网进行商务活动。电子商务的发展给人们的工作和生活带来了新的尝试和便利, 前景十分诱人, 也为人们带来无限商机。但是, 许多商业机构对是否进入电子商务领域仍持观望态度, 主要原因是网上运作的安全问题存有疑虑。美国密歇根大学的一个调查机构曾对2.3万名互联网用户进行调查, 结果显示: 超过60%的人由于担心电子商务的安全性问题而不愿进行网上购物。

木马病毒的猖狂泛滥、人们防范意识的不足, 使电子商务的安全性, 尤其是电子商务支付的安全性, 越来越成为人们关注的热点。

当许多传统的商务方式应用在开放的互联网上时, 便会带来许多安全方面的问题。电子商务的交易安全就是对交易中涉及的各种数据的可靠性、完整性和可用性进行保护。做到传输的安全性、数据的完整性、交易各方的身份认证和交易的不可否认性, 才能确保电子商务的安全。

电子商务安全可以分为信息传输与访问过程中的安全, 以及电子商务系统的安全, 电子商务安全协议、网上支付安全、移动商务安全、移动支付安全、电子商务身份认证和计算机及其网络的安全。



从国内外的情况来看，电子商务发展的速度太快，致使相关安全技术和安全管理跟不上，这是一个越来越突出的问题。“安全”是一个系统的概念，电子商务安全问题是一个技术性的问题，不仅涉及技术，还有管理，而且与社会道德、行业管理及人的行为模式密切相关。

电子商务面临哪些安全威胁，如何进行有效防范？



相关知识

在运用电子商务模式进行贸易的过程中，安全问题就成为电子商务最核心的问题，也是电子商务得以顺利推行的保障。

电子商务在全球范围内的迅猛发展，使电子商务中的网络安全问题日渐突出。在传统交易过程中，买卖双方是面对面的，因此比较容易保证交易过程的安全性和建立起信任关系。但在电子商务过程中，消费者、商户、银行是通过网络来联系的，彼此远隔千山万水，通过网络来完成购物、支付等一系列商务活动；如果系统安全性被破坏，入侵者就有可能假冒成合法用户来改变用户数据、解除用户订单或生成虚假订单，使商户遭受损失；消费者在将个人数据或自己的身份数据（如口令）发送给商户时，这些信息也可能在传递过程中被窃听，使消费者受到损失。因此，电子商务系统中交易各方都面临着安全威胁。

一、电子商务面临的安全威胁

信息在网络上传递时，要经过多个环节和渠道。由于计算机技术发展迅速，原有的病毒防范技术、加密技术、防火墙技术等始终存在被新技术攻击的可能性。计算机病毒的侵袭、黑客非法侵入、线路窃听等很容易使重要数据在传递过程中泄露，威胁电子商务交易的安全。一般来说，在电子商务中普遍存在以下几种安全隐患。

1. 信息的截获和窃取

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或在数据包通过的网关和路由器上截获数据等方式，获取机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，找出有用信息，如消费者的银行账号、密码及企业的商业机密等。

2. 信息的篡改

当攻击者熟悉了网络信息格式以后，通过各种技术方法和手段对网络传输的信息进行中途修改，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三方面。

(1) 篡改：改变信息流的次序，更改信息的内容，如篡改购买商品的出货地址等。

(2) 删除：删除某个消息或消息的某些部分，例如，一些淘宝店铺雇用黑客删除差评，误导消费者。

(3) 插入：在消息中插入一些信息，让接收方读不懂或接收错误的信息。

3. 信息假冒

当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以假冒合法用户或发送虚假信息来欺骗其他用户，主要有以下两种方式。

(1) 伪造电子邮件。虚开网站和商店，给用户发电子邮件，收订货单；伪造大量用户发电子邮件，耗尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应；伪造用户发大量电子邮件，窃取商家的商品信息和用户信息等。

(2) 假冒他人身份。冒充领导发布命令、调阅密件；冒充他人消费、栽赃；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。由于攻击者掌握了数据格式，并可以篡改在网络节点通过的信息，可以冒充合法用户发送虚假信息或者主动获取信息，而远端用户通常很难分辨真伪。

4. 恶意破坏

攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，其后果是非常严重的。

5. 交易否认

交易否认包括多个方面。例如，发信者事后否认曾经发送过某条信息或内容；收信者事后否认曾经收到过某条消息或内容；购买者下了订货单后否认；商家卖出商品后因价格变化而不承认原有的交易。

此外，各种外界的物理性干扰，如通信线路质量较差、地理位置复杂和自然灾害等，都可能影响到数据的真实性和完整性。



相关链接

互联网信息安全不容乐观

2016年，准大学生徐玉玉被骗后不幸死亡、清华大学教授被骗1760万元，这些案件轰动全国。

如何才能提高我们的信息安全性呢？

根据第46次《中国互联网络发展状况统计报告》显示，截止到2020年6月，网民遭遇各类网络安全问题的比例如图1-4所示。

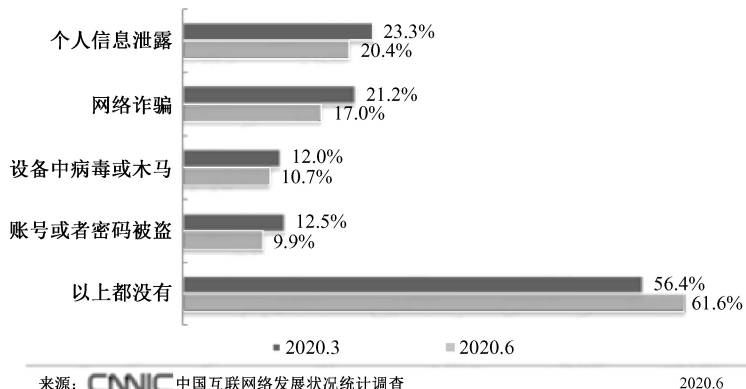


图 1-4 网民遭遇各类网络安全问题的比例



我国境内被篡改网站数量如图 1-5 所示。

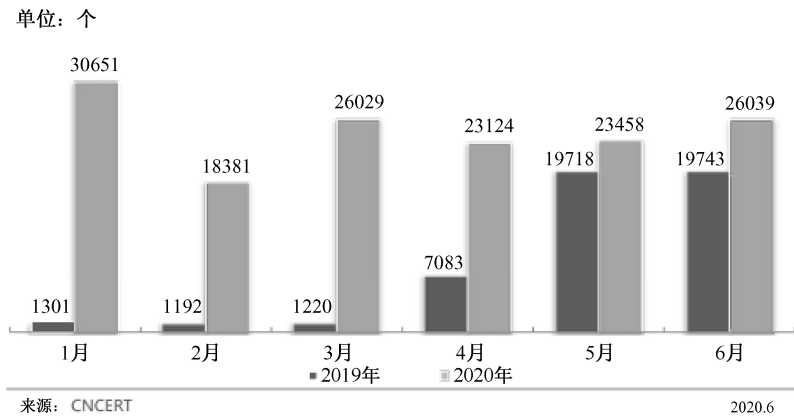


图 1-5 我国境内被篡改网站数量

二、电子商务安全要素

电子商务随时面临威胁，使用户对电子商务安全有迫切需求。一个安全的电子商务系统要求具有有效性、真实性、保密性、完整性和不可否认性。下面分析电子商务的安全要素。

1. 有效性

有效性是指贸易数据在确定的时刻、确定的地点是有效的。

电子商务以电子形式取代纸张，保证信息的有效性就成为开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉，所以要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误，以及计算机病毒产生的潜在威胁加以控制和预防。保证计算机系统的安全是保证电子商务系统数据传输、数据存储及电子商务完整性检查的正确和可靠的根基。

2. 真实性

真实性是指接收方可以确信信息来自发信者，而不是第三者冒名发送的；发送方可以确信接收方的身份是真实的，而不至于将商品发往与交易无关的第三方。

由于网络电子商务交易系统的特殊性，企业或个人的交易通常都是在虚拟的网络环境中进行的，要使交易成功，必须做到：首先要能确认对方的身份，商家要考虑客户端不能是骗子，客户也会担心网上的商店是不是一个黑店，所以对个人或企业实体进行身份确认成了电子商务中很重要的一环；其次对人或实体的身份进行鉴别，为身份的真实性提供保证，即交易双方能够在相互不见面的情况下确认对方的身份。这意味着当某人或实体声称具有某个特定的身份时，鉴别服务将提供一种方法来验证其声明的正确性，一般都通过证书认证机构和证书来实现。

例如，在互联网中，计算机系统的身份是由 IP 地址确认的，黑客使用虚假的 IP 地址，以达到隐瞒自己身份的目的。另外，在日常的电子邮件中，很难避免匿名邮件或使用不真实的邮件用户名。因此，在电子商务中必须建立严格的身份认证机制，以确保参加交易的各方身份的真实性。

3. 保密性

保密性是指保证只有发送者和接收者可以接触到信息。

电子商务作为贸易的一种手段，其信息一般包括个人、企业或国家的商业机密。例如，信用卡的账号和用户名被人获悉，就可能被盗用；订货和付款的信息被竞争对手获悉，就可能丧失商机。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的；而电子商务建立在开放的网络环境中，所以要求对传送的信息加密，以预防非法的信息访问和信息在传输过程中被非法窃取。

4. 完整性

完整性是指信息在传输过程中未经任何改动。

由于数据输入时的意外差错或欺诈行为，或者在数据传输过程中信息丢失、重复或传送次序的差异都可能导致贸易各方得到的信息不同。由于互联网是开放体系，只要网络用户具备特定的知识和工具，完全可以更改传输中的数据。因此，必须预防对信息的随意生成、修改和删除，同时防止在数据传送过程中信息丢失和重复，并保证信息传送次序的统一。另外要采取适当的访问控制措施，以保证数据存取系统的安全。在电子商务中，务必保存数据原始的格式和内容，因为贸易各方信息的完整性会影响交易和经营的策略。保持贸易各方信息的完整性是电子商务应用的基础。

5. 不可否认性

不可否认性是指在交易数据发送完成以后，双方都不能否认自己曾经发出或接收过信息。

在传统的纸面贸易中，贸易双方通过交易合同、契约或贸易单据等书面文件上的签名或印章来鉴别贸易伙伴，确定合同、契约或单据的可靠性，以预防否认行为的发生，这也就是人们常说的“白纸黑字”。为了保证通信过程的各个环节都是不可否认的，电子交易必须为交易双方提供可靠的标识。

不可否认性主要包含数据的原始记录和发送记录，确认数据已经完成发送和接收，防止接收用户更改原始记录，或者否认已收到数据并拖延下一步工作。为了保证交易过程的可操作性，必须采取可靠的方法来确保交易过程的真实性，保证参加电子交易的各方承认交易过程的合法性。

三、电子商务安全技术

一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护的资源间建立多道严密的安全防线，能够极大地增加恶意攻击的难度，并增加审核信息的数量，利用这些审核信息可以跟踪入侵者。下面主要介绍密码技术、安全协议、PKI（public key infrastructure，公开密钥基础设施）技术、网络安全技术等内容。实际上安全协议和 PKI 技术都源于密码技术。

1. 密码技术

密码技术是保证电子商务安全的重要手段，是信息安全的核心技术。它主要包括加密、密钥管理、数字签名三大技术。



(1) 加密。加密就是使用数学方法来重新组织数据，除合法的接收者外，任何其他人要想恢复原先的“报文”或读懂变化后的“报文”是非常困难的。许多密码算法现已成为网络安全和商务信息安全的基础。密码算法利用密钥来对敏感信息进行加密，然后把加密好的数据和密钥（要通过安全方式）发送给接收者，接收者可利用同样的算法和传递来的密钥对数据解密，从而获取敏感信息并保证网络数据的机密性。

(2) 密钥管理。密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁及保密等内容。其中分配和存储是最棘手的问题。密钥管理不仅影响系统的安全性，而且涉及系统的可靠性、有效性和经济性。用密码技术保护的现代信息系统的安全性主要取决于对密钥的保护，而不是对算法或硬件本身的保护，即密码算法的安全性完全寓于密钥之中。

(3) 数字签名。数字签名是公开密钥加密技术的一种应用，是指用发送方的私有密钥加密报文摘要，然后将其与原始的信息附加在一起，合称为数字签名。利用数字签名能够实现对原始报文的鉴别与验证，保证报文的完整性、权威性和发送者对所发报文的不可否认性。数字签名机制提供了一种鉴别方法，保证网络数据的完整性和真实性。其被普遍用于银行业务、电子贸易等，以解决伪造、否认、冒充、篡改等问题。

2. 安全协议

安全协议是许多分布式系统安全的基础，是电子商务系统运行的安全通信标准。目前国际上流行的电子商务采用的协议主要包括以下方面。

(1) 电子商务支付协议。电子商务支付是电子商务中最重要的内容，目前已经出现了很多的电子商务支付协议。在现实生活中常见的有基于银行卡的支付协议、基于支票的支付协议和基于现金的支付协议，著名的有 First Virtual、SSL、SET、iKP、NetBill 等。

(2) 安全 HTTP (S-HTTP) 协议。

(3) 安全电子邮件协议（如 PEM、S/MIME 等）。

(4) 用于公对公交易的互联网 EDI (UN/EDIFACT) 等。

3. PKI 技术

PKI 是利用公开密钥算法原理和技术为网上通信提供通用安全服务的基础设施。它为电子商务、电子政务、网上银行证券等提供安全基础平台。

密钥管理是电子商务中普遍存在的安全问题。为解决在互联网上开展电子商务的安全问题，世界各国经过多年研究后，初步形成了一套完整的解决方案。PKI 采用证书管理公开密钥，即结合 x.509 标准中的鉴别框架来实现密钥管理，通过证书认证机构把用户的公开密钥及其他标识信息捆绑在一起，在互联网上验证用户的身份，保证网上数据的保密性和完整性。

PKI 的核心元素是数字证书，其核心执行者是认证机构。有关数字证书服务的应用、实施是广泛开展电子商务的基本前提，电子商务的深入开展离不开数字证书技术和认证机构的正确督导。

4. 网络安全技术

网络安全是电子商务安全的基础，一个完整的电子商务系统应建立在安全的网络基础设施之上。网络安全涉及的方面比较多，如操作系统安全、防火墙技术、VPN (Virtual Pager Network, 虚拟专用网) 技术、各种反黑客技术和漏洞检测技术等。其中最重要的就是防火墙技术。

防火墙建立在通信技术和信息安全技术之上，它用于在网络之间建立一个安全屏障，根据

指定的策略对网络数据进行过滤、分析和审计，并对各种攻击提供有效的防范，主要用于互联网接入和专用网与公用网之间的安全连接。其具体工作原理，在模块六将进行详细叙述。



相关链接

防 火 墙

防火墙一般有 3 个端口，如图 1-6 所示。其中一个接外网（互联网），一个接内网，一个接 DMZ（demilitarized zone，隔离区），在 DMZ 中有网络服务器。防火墙要达到的效果：内网区的计算机可以任意访问外网，可以访问 DMZ 中指定的网络服务器，互联网和 DMZ 中的计算机不能访问内网；互联网可以访问 DMZ 中的服务器。

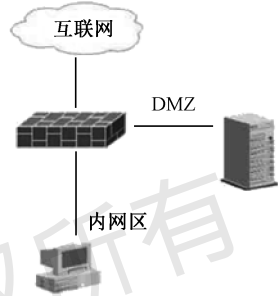


图 1-6 防火墙

VPN 也是一项保证网络安全的技术之一，它是在公共网络中建立一个专用网络，数据通过建立好的虚拟安全通道在公共网络中传播。企业只需要租用本地的数据专线，连接上本地的公众信息网，其各地的分支机构就可以互相安全传递信息；同时，企业还可以利用公众信息网的拨号接入设备，让自己的用户通过公众信息网连接进入企业网。VPN 具有节省成本、远程访问、扩展性强、便于管理和实现全面控制等优点，是企业网络发展的趋势。

四、电子商务安全体系结构

电子商务的安全体系应包括：安全可靠的通信网络，保证数据传输的可靠性和完整性，防止病毒、黑客入侵；电子签名和其他身份认证系统；完备的数据加密系统等。

1. 支持服务层

支持服务层包括密码服务、通信、归档、用户接口和访问控制等模块，它提供了实现安全服务的安全通信服务。

2. 传输层

传输层发送、接收、组织商业活动所需的封装数据条，在客户和服务器之间根据安全设定来传递信息。数据条的基本类型：签名文本、证书、收据、已签名的陈述信息、数字化的商品、访问某种服务所需的信息、获得物理商品所需的信息等。传输层包括付款模块、文档服务模块和证书服务模块等。

3. 交换层

交换层提供封装数据的公平交换服务。公平是指 A 和 B 同意进行交换，则 A 收到 B 封装数据条的充分必要条件是 B 收到 A 的封装数据条。

4. 商务层

商务层提供商业方案，如邮购零售、在线销售信息等。商务层也称一般业务服务层。这一层实现各种网上商务活动与服务，如标准的商品目录（价目表）、电子商务支付工具等，保证



商务信息安全传送、认证交易各方的合法性、商务活动协同和商品交易等。

五、电子商务安全法律要素

安全的电子商务除依赖技术因素外，还必须依靠法律手段、行政手段来最终保护参与电子商务各方的利益。法律规范的建设成为当前电子商务发展不可或缺的要素。

开展电子商务需要在企业和企业之间、政府和企业之间、企业和消费者之间、政府和政府之间明确各自需要遵守的法律义务和责任，其主要涉及以下几方面的法律要素。

1. 有关证书认证机构的法律

证书认证机构（certificate authority, CA）是在电子商务中买卖双方之外的公正的、权威的第三方，是电子商务中的核心角色，它担负着保证电子商务公正、安全进行的任务。因此，必须由国家法律来规定证书认证机构的合法地位、设立程序和设立资格及必须承担的法律义务和责任，也必须由法律来规定由谁对证书认证机构进行监管，并明确监管的方法及违规处罚措施。

2. 有关保护个人隐私的法律

本着最小限度收集个人数据、最大限度保护个人隐私的原则来制定法律，以消除人们开展电子商务时对泄露个人隐私及重要个人信息（如信用卡账号和密码）的担忧，从而吸引更多的人进行电子商务活动。

3. 有关电子合同的法律

需要制定有关法律，对电子合同的法律效力予以明确；对数字签名、电子商务凭证的合法性予以确认；对电子商务凭证，电子商务支付数据的伪造、变更、注销做出相应的法律规定。

4. 有关电子商务的消费者权益保护法

在网络交易过程中，消费者对商家信誉的信心只能寄托于为交易提供服务的第三方，如证书认证机构和收款银行等。其中，证书认证机构能够核实商家的合法身份，收款银行则能掌握商家的信誉情况。一旦因商家不交货、不按时交货或者货不符实而对消费者产生损害时，可以由银行先行赔偿消费者，再由银行向商家追索损失，并降低商家在银行的信誉度，或取消商家电子商务支付账户，或将商家违规情况记入证书认证机构的黑名单，甚至取消商家的数字证书。

5. 有关网络知识产权保护的法律

网络对知识产权的保护提出了新的挑战，因此在研究技术保护措施时，还必须建立适当的法律框架，以便侦测仿冒和欺诈行为，并在上述行为发生时提供有效的法律援助。

值得指出的是，在制定电子商务法律时，要坚持灵活性和安全性的高度辩证统一。为了电子商务的安全性，电子商务立法必须加快。但是，由于电子商务还处在快速发展之中，在很多方面（如数字身份认证）应该首先考虑行业的自律机制，以避免不灵活或不协调的政府法规的“锁定”效应。



相关链接

手机成用户第一钱包，移动支付安全状况堪忧

360 公司发布《2020 年中国手机安全状况报告》，该报告显示，“90 后”是手机诈骗的主要受害者，占比高达 37.5%，“00 后”占比为 28.7%，而“70 后”“60 后”占比还不到 10%。

2020 年，360 公司共接到手机诈骗举报 2656 起。其中诈骗 1340 起，涉案总金额高达 1520.2 万元，人均损失 11345 元。

在所有诈骗类型中，金融理财类诈骗是举报人数最多的诈骗类型，占比高达 23.4%；其次是虚假兼职诈骗（占比 18.4%）和交友诈骗（占比 15.8%）等。男性被骗人数明显高于女性，男性受害者占 61%，女性为 39%。

手机正成为个人财富中心，但移动支付安全状况仍然堪忧，钓鱼网站、恶意程序威胁个人财产。一条短信、一个链接都可能使人倾家荡产。



实践训练

1. 课堂讨论

- (1) 电子商务面临的安全威胁有哪些？
- (2) 电子商务安全要素有哪些？
- (3) 电子商务安全技术主要有哪两类？

2. 案例分析

支付机构需平衡快捷与安全

针对网上支付风险，阿里小微金服集团安全副总裁江朝阳详解了支付宝的安全策略，通过实时风险监控系统将资损率控制在十万分之一以下，远低于业内平均水平。

针对用户支付账户被盗的事件，支付宝从终端环境、用户认证、隐私保护、安全产品、交易行为监控等方面保障用户安全。以交易行为监控为例，支付宝开发了一套国内先进的智能风险实时监控系統，可以实时为用户提供保护。

据支付宝方面统计，2012 年因电信运营商二次放号带来的账户风险显著降低。“我们已经宣布，类似案例我们会进行补偿，可以说风险非常低。但考虑到用户的诉求，我们还是开通了安全度更高的‘双因子’验证机制，增加了身份证输入验证。”江朝阳坦言，双因子提高了安全度，但降低了便捷性。“提升了密码通过手机重置的安全级别，有 20%的用户因无法找回密码而投诉，而这个机制对相关案件发生率的下降几乎没有作用。”

因此，支付宝方面认为，解决此类安全问题更好的方式是运营商等上下游伙伴通力合作。

讨论与分析

在电子商务支付过程中，你认为快捷和安全哪个更重要？



3. 实务训练

(1) 上网查找最新的病毒流行排行, 了解一两个电子商务安全事件。掌握电子商务安全的具体内容。

(2) 你的计算机、手机受到过安全威胁吗? 你是如何处理的?

(3) 对于防范网络攻击、保护信息安全, 你有哪些建议?

实训说明

(1) 本部分实训既可在课堂上进行, 也可在课后完成。

(2) 总结电子商务安全事件产生的原因, 指出应该采取哪些相应的预防措施。

4. 课后拓展

(1) 以小组为单位上网收集资料, 开展“电子商务安全技术和法律哪个更重要?”的辩论。

(2) 《中华人民共和国网络安全法》由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布, 自 2017 年 6 月 1 日起施行。扫描二维码 1-1, 了解该法的内容, 分析其重大意义。

(3) 《中华人民共和国电子商务法》(2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过), 扫描二维码 1-2, 进行学习。

【课程思政】 做一名合格的大学生必须树立法律意识, 增强法制观念, 提高法律素质, 简而言之, 要做到学法、知法、懂法、守法。



1-1



1-2

第三单元 安全电子商务支付



情景案例

手机用来打电话、发短信人人皆知, 而现在, 不用兑换零钱, 也不用使用公交 IC 卡, 乘坐公交车时将手机在车上的刷卡机轻轻一“刷”, 就能坐公交车了。手机不仅可用来刷卡乘车, 还可查询余额和空中充值。这种过去听起来有点“天方夜谭”的事, 现在已经非常普遍了。

随着业务的不断发展, 手机除了能乘坐公交车, 还可在超市、便利店等地方刷卡购物, 真正实现“一机在手, 消费随心”。继卡类支付、网上支付后, 手机支付俨然成为消费领域的新宠。

手机支付便利了消费者, 也为商家带来了机遇, 电子商务支付促进了电子商务的发展, 其前景广阔。淘宝的成功, 除网站自身的优势以外, 支付宝起到的作用也是不可低估的。

消费者在进行电子商务支付的时候, 最担心的就是安全问题。银联手机支付使用了目前国际上比较先进、比较安全的智能加密技术, 采用硬件级加密, 无法破译, 比传统的银行卡和网上银行更加安全。因此, 如果手机遗失, 无须担心银行卡信息的丢失和账户资金的安全, 挂失并补办智能 SD 卡后就可继续使用。

任务思考

手机支付大大地便利了人们的生活,拓展了电子商务支付的新领域。无论使用信用卡、网银还是手机移动支付,人们除了关心便捷性,最为担心的还是安全问题。那么,电子商务支付面临哪些安全威胁?其应对措施是什么?安全的电子商务支付对电子商务的发展和我们的生活有什么意义?

本单元主要讲述安全电子商务支付的内容,本单元可以激发同学们学习“电子商务支付与安全”的积极性。



任务分析

以电子商务支付技术为基础的信用卡、电子货币、网上银行和移动支付等的普及应用,为电子商务的发展提供了金融基础。信用卡以其方便、快捷、安全等优点成为人们消费支付的重要手段,并由此形成了完善的全球性信用卡计算机网上支付与结算系统,为电子商务中的网上支付提供了重要的技术手段。

从 2012 年“双十一”支付宝无线业务单日 900 万笔的业绩,可以看出移动支付的潜力。另外,智能终端的普及也给移动支付在硬件上带来了更大的可操作性。移动支付产业链各方都在积极寻求合作,共同开发、抢占市场。为使自身利益最大化,银行、运营商、第三方机构各方激烈博弈,分别推出了适合自身发展的移动支付方式。例如,中国移动大力倡导的 RF-SIM 方案,银联推广的 SD 卡方案,手机制造商推广的 NFC 方案等,激烈的多方博弈导致我国的移动支付市场一度处于比较混乱的状态。

2012 年是移动支付爆发式增长的前兆,移动支付在这一年占尽了天时、地利、人和,其后以惊人的速度改变了整个支付产业。

继手机一卡通支付后,微信支付已经上线。用户只需在微信中关联一张银行卡,并完成身份认证,即可将装有微信 App 的智能手机变成一个全能钱包,之后即可购买合作商户的商品及服务,用户在支付时只需在自己的智能手机上输入密码,无须任何刷卡步骤即可完成支付,整个过程简便流畅。

无论是银行卡、网上银行还是手机移动支付,都极大地方便了消费者。电子商务的发展,除了依靠计算机技术、互联网技术,支付技术和安全技术是其最重要的基础。相应的法律制度、管理规范是我国电子商务有序发展的重要保障。

作为 2012 年涌现出来的创新热点,移动支付很有可能改变产业发展与未来生活。电子商务支付的不断创新,保障了电子商务的快速发展。但像用户被盗刷资金的事件,也给消费者的网上支付带来了隐忧。



相关知识

一、电子商务支付的安全问题

信息流、商流、资金流、物流是商务活动的四大环节,而资金流是商务运作模式的核心,是政府、商家、客户最为关心的对象,政府、企业及家庭和个人对资金流的运行效率和服务质量的要求越来越高。



电子商务安全和网络安全问题已经变得日益突出,在这种背景下,网络金融服务面临和很多普通互联网服务相同的安全威胁,电子商务支付的有效性、真实性、保密性、完整性和不可否认性等安全要求面临危机,支付的安全性变得尤为重要。

1. 电子商务支付面临的安全问题

2021年1—5月,全国共破获电信网络诈骗案件11.4万起,打掉犯罪团伙1.4万余个,抓获犯罪嫌疑人15.4万名,同比分别上升60.4%、80.6%和146.5%。相关部门成功劝阻771万名群众免于受骗,为群众挽回经济损失991亿元。针对电子商务支付的违法犯罪案件时有发生,犯罪手法不断翻新,安全问题日益困扰蓬勃发展的中国电子商务支付行业。

电子商务支付面临的安全问题主要表现在以下几方面。

(1) 计算机病毒。计算机病毒是被插入计算机程序的破坏计算机功能或者数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。计算机中毒后,可能导致正常的程序无法运行,计算机内的文件受到不同程度的损坏,通常表现为增、删、改、移。中毒的计算机很可能无法正常完成电子商务活动,或者无法进行正常的电子商务支付。

(2) 黑客攻击。利用计算机的安全漏洞,入侵计算机系统的行为被称为“黑客攻击”。黑客以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的。在利益的驱使之下,入侵者在网上获取用户信息,将账单转嫁到目标主机上,或设立钓鱼网站,对用户进行诈骗。



相关链接

遭受境外黑客攻击严重

来自国家互联网应急中心的最新数据显示,中国遭受境外网络攻击的情况日趋严重。2020年,约1.9万台位于美国的木马或僵尸网络控制服务器,控制了中国境内约446万台主机。这两个数字较上一年分别增长了10.2%和4.1%。

针对中国网上银行、支付平台和网上商城等的钓鱼网站有96%位于境外。

(3) 系统安全漏洞。系统安全漏洞是指可以用来对系统安全造成危害,系统本身具有的或在设置上存在的缺陷。安全漏洞主要是因为系统在设计和实施中出现错误所致,造成信息完整性、可获得性和保密性受损。错误通常在软件中,也存在于各个信息系统层,从协议到设计及物理硬件。系统在安全方面存在漏洞,非法网站、病毒和非法插件会通过漏洞入侵系统,破坏系统的安全性,给电子商务支付带来巨大的威胁。

2. 电子商务支付安全问题产生的主要原因

(1) 技术原因。由于受到计算机和网络科学技术水平的限制,系统的安全漏洞还无法彻底消除,电子商务支付系统的软件、硬件和协议等存在安全漏洞,很容易被不法分子利用。电子商务支付依赖现代化的电子信息传递和电子处理系统,一旦通信或系统出现故障,将会出现资金汇划延误,严重时将导致整个电子商务支付业务瘫痪。

(2) 安全意识低。在国内,互联网用户账号、密码信息被盗取现象已存在多年,甚至已形成“灰色产业链”。一些单位和个人安全意识不强或防范手段有疏漏,导致账号、密码等通过网络泄

密,造成资金损失。在当前网络安全形势尖锐的环境下,加强对信息系统的安全保护,提升安全防范意识尤为重要。养成良好的上网习惯,尽可能不在网吧等公共场合进行网上支付。

(3) 法律因素。现有的法律规范对网络安全犯罪缺少具体司法解释,缺少具体定罪量刑标准。《计算机信息网络国际联网安全保护管理办法》规定制造和传播计算机病毒是违法的,但对于木马、黑客程序等并没有清晰的界定,这也是木马程序制造者敢于利用网络公开叫卖的根本原因。

病毒软件只是一种计算机程序,每个环节都不违法,但如果将其应用于窃取账号等行为时,就违法并危害了网络安全,但很难查处。例如,虚拟资产在现实中难以认定价值,定盗窃罪没有依据。受害者有权利提起民事诉讼请求,但在操作上有些困难,包括收集证据、赔偿的标准和计算方法,目前在立法上缺少统一的规定。

(4) 安全管理滞后。由于我国电子商务支付方面的法律相对滞后,对电子商务支付市场(特别是非金融机构)监管不够,目前商业银行和非金融机构的支付产品质量参差不齐,机构员工安全意识淡薄,安全防护措施不够,用户的交易安全和个人信息存在很大的风险。有些电子商务支付平台要求用户提供真实姓名、联系方式、住址、银行账号甚至身份证号,个别网站在设计上存在问题,致使这些信息很容易泄露。

(5) 信用体系不健全。我国的信用机制建设启动较晚。2002年,上海资信有限公司运营的个人信用联合征信服务系统投入使用,中国第一个“个人信用档案数据中心”诞生。随后,其他信用建设项目陆续开始启动。美国建立完善的信用体系,足足用了100年的时间。

信用评价体系落后,信用缺失成本低,失信甚至违法行为大行其道。进行电子商务支付时,交易双方相互不信任,都害怕对方不守信,担心自己的利益受到侵害。

电子商务能够促进交易的发生,降低交易的成本。在电子商务支付阶段,如果没有足够的诚信体系做保证,交易成本反而会提升。尽快建立起健全的社会信用评价体系是解决我国电子商务支付信用问题的当务之急。

二、安全电子商务支付的途径

1. 技术保障

技术保障是指实现电子商务所需的设备、技术等能够稳定、安全地运行,其中主要包括实体的安全和网络技术的安全。通过提高设备和网络技术的安全性能,保证电子商务支付信息传递的完整性和可靠性。利用加密技术保证电子商务支付的机密性,利用验证技术保证电子商务支付的真实性和完整性,利用防火墙、杀毒软件等保证计算机系统不受侵害,完善安全协议、认证技术,保证电子商务支付的安全性。

2. 加强宏观管理

加强对企业和个人的安全防范教育,企业要建立保密制度、病毒防范制度,加强人员管理,有安全预案。个人要保护好密码、账号等信息,保持良好的上网习惯。建立全社会的信用评价体系,对于失信者给予惩罚,保证电子商务支付安全地进行。

3. 建立健全法律规范

尽快完善电子商务、电子交易和电子商务支付方面的法律规范,以法律条文的形式来保护电子商务信息的安全,惩罚网络犯罪,建立良好的电子商务法制环境,约束人们的支付行为。



具体内容将在模块五~九详细学习。

三、安全电子商务支付的意义

电子商务支付的广泛应用,基本满足了社会经济多样化的支付服务需求,对减少现金流通、降低交易成本、提高支付效率、培育社会信用、促进金融创新、塑造新型支付文化和促进电子商务的发展发挥了重要的作用。包括中国在内的许多国家开始重视网上支付与结算方式,这也是学习、研发、推广、应用网上支付与结算方式的必要性所在。

电子商务支付作为新型的支付方式,已经对电子商务和金融发展产生了重大影响。这些影响主要表现在以下几方面。

(1) 能够提高电子商务和金融运行的效率,节约交易成本,促进经济发展。

(2) 为电子商务的发展提供了广阔的前景,有利于缓解并最终解决电子商务中的支付瓶颈问题。

(3) 突破时空的限制,丰富支付手段,促进金融改革创新和发展。

(4) 方便人们日常生活支付需要,有利于培养健康文明的支付习惯。

(5) 将对货币政策,主要是对货币的基本定义、货币发行方式、货币流通速度和货币乘数等方面产生一定的影响。

(6) 安全的电子商务支付工具,特别是信用卡的使用,将促进消费信贷发展,有助于社会信用体系建设。



相关链接

手机钱包移动支付安全状况

中国银联发布的《2020 移动支付安全大调查报告》显示,“网诈”损失率下降,新型诈骗仍需警惕。2020年消费者在移动支付中遭遇的诈骗损失率有所下降,相较上一年减少了4%。但网络赌博(杀猪盘)、跑分等新型犯罪导致的受损金额依然较大。参与过网络赌博的群体中近六成遭受诈骗且损失金额超过2500元。同时,在参与“跑分”的群体中,近五成有损失发生,人均损失金额超过1000元。



实践训练

1. 课堂讨论

- (1) 电子商务支付面临哪些安全威胁?
- (2) 安全支付的作用有哪些?

2. 案例分析

一项网上调查显示,信用和安全是人们不愿意采用电子商务支付方式的两大影响因素。调查显示,91.1%的消费者把安全因素作为是否使用网上支付的第一要素,而有61.2%的网民不使用网上支付也是由于安全的问题。而这两大问题,也成为横亘于电子商务和消费者之间的最

大障碍，阻碍了网上支付这一新兴的支付服务的发展。

讨论与分析

(1) “魔高一尺，道高一丈”，对于提高支付工具的技术水平来保障交易安全，你有哪些更好的建议？

(2) 法律制度的健全是促进支付良性发展的主要保障，你认为应该建立哪些相关的电子交易法规制度？

3. 实务训练

对电子商务支付与安全认知进行实训。

实训说明

- (1) 本部分实训既可在课堂上进行，也可在课后集中完成。
- (2) 比尔·盖茨说“传统银行将成为 21 世纪即将灭绝的恐龙”，请谈谈你的理解。
- (3) 上网查询银行卡和网银的支付流程。
- (4) 上网了解网络安全防范手段。
- (5) 从支付和安全两方面谈谈如何解决制约电子商务发展的瓶颈。

4. 课后拓展

(1) 上网搜集关于移动支付资料，结合课程学习内容，写一篇关于移动支付现状、前景和安全问题的小论文，题目自拟。

(2) 你了解闪付、云闪付吗？扫描二维码 1-3，了解银联手机闪付的更多内容。



1-3

知识小结

电子商务是计算机网络的又一次革命，是通过电子手段建立一种新的经济秩序，它不仅涉及电子技术和商业交易本身，而且涉及金融服务、诚信和安全等其他层面。信息化、互联网和电子商务支付是实现电子商务的基础条件。

电子商务支付是指进行电子商务交易的当事人（包括消费者、厂商和金融机构）使用安全手段和密码技术，通过电子信息化手段进行的货币支付和资金流转。用互联网作为运行平台的网上支付，极大地促进了电子商务的发展。

网上支付平台主要由互联网、支付网关和银行内部专用业务网络三部分组成。电子商务支付工作程序主要包括七个步骤。

病毒的侵袭、黑客非法侵入、线路窃听等很容易使重要数据在传递过程中泄露，威胁电子商务的安全。安全的电子商务系统的要素有有效性、真实性、保密性、完整性和不可否认性。可以通过密码技术、网络安全技术和法律规范来提高电子商务的安全性。

支付与结算问题已经成为电子商务发展的瓶颈，电子商务支付的安全对于电子商务的开展起着非常重要的作用，任何在互联网上进行商务活动的企业和消费者都要积极采取相应的安全措施，以确保自身交易的安全，避免利益损失。



练习测试

1. 名词解释

电子交易 电子商务支付 计算机病毒 黑客攻击 网络安全漏洞

2. 选择题

- (1) 下面哪个不是电子商务支付的“全能化”的“3A 服务”? ()
- A. Anytime B. Anywhere C. Anyhow D. Anyone
- (2) () 是公开密钥基础设施的简称。
- A. SET B. PKI C. EDI D. Intranet
- (3) 电子商务支付的特征不包括哪些? ()
- A. 通过现金的方式进行款项支付
- B. 工作环境是基于互联网开放的系统平台
- C. 使用的是最先进的通信手段, 对软件、硬件设施的要求很高
- D. 具有方便、快捷、高效、经济的优势
- (4) 以下哪些问题会涉及资金的安全? ()
- A. 黑客入侵 B. 内部作案
- C. 密码泄露 D. 以上都是
- (5) 电子商务系统必须具有十分可靠的安全保密技术, 必须保证网络安全, 具有 ()。
- A. 不可修改性 B. 信息的稳定性
- C. 交易者身份的确定性 D. 数据的可靠性
- (6) 信息的完整性是指 ()。
- A. 信息不被他人接收 B. 信息内容不被指定以外的人知悉
- C. 信息不被篡改 D. 信息在传递过程中未经任何改动

3. 简答题

- (1) 与传统交易相比, 电子交易有哪些优势?
- (2) 与传统的支付方式相比, 电子商务支付具有哪些优势?
- (3) 电子商务支付的流程包括哪些内容?
- (4) 电子商务面临的威胁有哪些?
- (5) 密码技术具体包括哪些?
- (6) 电子商务支付面临哪些安全威胁?

4. 论述题

试论述电子商务支付安全的重要作用。