

模块1

电子商务支付与安全概述

学习目标

知识目标

掌握电子支付的内涵及其流程

了解电子商务安全威胁，防范技术和法律要素

掌握电子支付与安全对电子商务的作用

能力目标

掌握电子支付的一般流程，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的认识

素质目标

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1单元 电子支付



情景案例

中国内地第一笔因特网电子交易

张丽艳是鹤乡职业技术学院电子商务专业的一名大学生,她喜欢电子商务,想在大学期间学好专业,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,在网上她看到了以下资料。

1998年3月18日,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:中国内地第一笔因特网电子交易成功。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。

中国内地第一笔因特网电子交易的时间是1998年3月18日下午3点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先生;第一笔费用的支付手段是中国银行长城卡;第一笔支付费用是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,王轲平先生发现了这个站点,并填写了申请书。在接到王轲平先生的申请后,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。王轲平先生成为第一个在中国因特网上进行电子交易的人。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:如果王先生没有长城卡,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先生支付的100元?王先生的其他信息会泄露给第三者吗?目前电子交易的支付安全吗?当前进行这样的一笔电子商务交易还需15天的时间吗?周围的同学进行过电子商务和电子支付活动吗?等等。

张丽艳同学产生的这些疑问,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,商品交易经济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Internet作为商务平台实现整个商业贸易活动的电子化。电子商务从涵盖范围方面看,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,电子支付即网络支付已经越来越被人们所知所用。网上购买火车票、飞机票,网上缴纳水电煤气费、电话费已经非常普遍,支付宝、财付通和手机的移

动支付等电子支付平台纷纷争夺电子支付市场，电子支付逐渐成为人们关注的热点。除了购买商品使用网上支付外，现在许多学校的大学生缴纳学费都使用银行卡了。网络支付促进了电子商务的发展，方便了人们的生活。那么，网络电子支付的运行需要什么环境？网络电子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？

网上购买火车票、缴纳电话费、淘宝购物等一系列电子商务要成为一个完整的过程，网上的电子支付及其安全是重要的环节。客户和商家之间不再使用现金进行结算，而是采用信用卡、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，省去了交易中很多人员开销。网上支付的即时到账，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了，也更复杂了，不同的支付工具的操作流程也是不一样的。

由于电子商务双方的虚拟性，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，现在已有实用的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，电子支付已经成为消费者最重要的支付手段之一，电子支付行业呈现爆发式增长。2011 年中国互联网支付业务交易规模达到 22 038 亿元，同比增长了 118.1%。2012 年第三季度中国第三方互联网支付市场交易规模已达到 9764 亿元，同比增长了 73%，2013 年前三季度累计交易规模已超过去年全年。

截至 2013 年，已有六批第三方支付企业相继获得支付业务许可，电子支付产业体系日趋完善化。电子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的运营主体。

未来，电子支付的“全能化”将主要体现在“3A 服务”方面——即 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权衡电子支付优劣的两大重要指标。

1. 网络电子支付的产生和发展

在网络经济时代，企业和客户对更有效率、更快捷安全、成本更低的交易和支付方式的迫切需求，以及 Internet 的普及应用，导致了电子交易和电子支付的迅猛发展。从根本上讲，电子支付的产生源自于电子交易。

1) 电子交易

所谓电子交易就是指在网上进行买卖交易。电子交易将不再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能帮助企业与客户、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、保持资金全部周转和降低实际销售支出，进而降低成本、增加利润。电子交易也使顾客足不出户，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,从而可使用户和厂商双双得利,也有利于遏制假货的出现。借助因特网的覆盖范围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质优的原料。

(5) 减少交通费用,减缓交通压力,节省差旅费用。



相关链接

DELL 笔记本电脑网络交易流程

张丽艳考入鹤乡职业技术学院电子商务专业后,准备买一台笔记本电脑,在众多的笔记本电脑公司调查比较后,选中了一款。后来张丽艳在 DELL 的网站上看到,此型号产品网上购买折后价位比笔记本电脑公司便宜 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,并按以下的流程购买。

(1) 在百度(<http://www.baidu.com/>)上输入“戴尔”,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,张丽艳就按照网上提供的基本配置标准选定了商品。

(3) 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) 张丽艳在“支付宝”上按照要求进行了注册,利用自己的中国邮政储蓄银行的借记卡进行了支付。详细支付流程在模块 2 讲解。

张丽艳在 DELL 网站上的购物流程如图 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,而且也给消费者带来了很多的便利和实惠。



图 1-1 DELL 网站上的购物流程

2) 电子支付

所谓电子支付(Electronic Payment)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。广义地说,电子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,因此电子支付与结算方式的出现要早于现在的 Internet。随着 20 世纪 90 年代全球范围内 Internet 的普及和应用,电子商务的深入发展标志着信息网络经济时代的到来,一些电子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 Internet 作为运行平台,网络支付(Internet Payment)就应运而生了。本书所讲的电子支付,主要指的就是网络支付。

与传统的支付方式相比,电子支付具有以下优势。

(1) 电子支付适应了整个社会向信息化、数字化发展的趋势。电子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) 电子支付的工作环境是基于开放的系统平台(如 Internet),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得消费者可以随时随地进行消费支付活动。

(3) 电子支付是跨时空的电子化支付,能够真正实现全球 7 天 24 小时的服务保证。交易方只要有一台能够上网的 PC 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、分行、银行职员、自动取款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) 电子支付发展历程

银行采用计算机等技术进行电子支付的形式有五种,分别代表着电子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。

第四阶段是利用银行销售点终端(POS)向客户提供自动的扣款服务,这是现阶段电子支付的主要方式。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硬件基础。

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

2. 电子支付面临的问题

与传统支付相比,虽然电子支付存在很大的优势。但就目前而言,电子支付仍然存在一些缺陷限制了其发展,主要表现为以下几方面。

(1) 安全性和支付信息私密性问题。这是一直困扰着电子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、建立安全的认证体系、设立防火墙等。

(2) 对软硬件要求很高。电子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、专业人员的配备,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,一步实现电子支付的投入太高。

(3) 电子支付工具需要相应的系统支持。消费者选用的电子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,电子支付还是难以实现的。而对消费者来说,要求同时持有各种流行的支付工具,也是不现实的。所以,电子支付的推广要求商家认可支持多种支付工具,各种电子支付系统能够相互兼容,实现系统的互通。

3. 网络电子支付的运行环境

电子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,因此电子支付的运行环境即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。

电子支付的常见网络平台有电话交换网 PSTN、公用数据网、专用数据网、电子数据交换 EDI 专用网络平台及近年发展起来的 Internet 等。最早电子支付网络平台主要有 PSTN, 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当前业务发展的需要,特别是不能支撑以 Internet 为平台的电子商务下支付结算的需要。

目前,网络支付的支撑网络平台主要有两类:一类是传统成熟的 EDI 专用网络支付平台;另一类是大众化网络平台 Internet,它们各有优缺点和应用环境,随着 Internet 在全社会各行各业的大规模普及应用,加上其方便快捷、多媒体互动性强及经济的应用特点,大众化网络平台 Internet 已成为网络支付平台的发展趋势。EDI 正从专用网络逐渐向 Internet 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 Internet 平台的电子支付。

4. 网络电子支付流程

1) 网络支付结构

Internet 网络支付平台主要由 Internet、支付网关、银行内部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 Internet 和传统的银行专用网之间,用于连接银行专用网络与 Internet 的一组专用服务器。设置支付网关的主要目的是安全地连接 Internet 和银行专用网,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,将目前不安全开放的 Internet 上的交易信息传给内部封闭的安全的银行专网,起到隔离和保护银行内部网络的作用。正是有了支付网关,整个 Internet 网络支付平台才安全可靠,大大方便了商家与客户对网络支付系统的应用,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运作。

2) 电子支付流程

在处理电子支付时借鉴了很多传统支付方式的应用机制和过程,只不过流通的领域不同,一个是运用传统纸制货币与票据,大多手工作业;一个是运用电子货币且网上作业;但是,基于互联网平台的网络支付结算流程与传统的支付结算过程是类似的。如果熟悉传统的支付结算

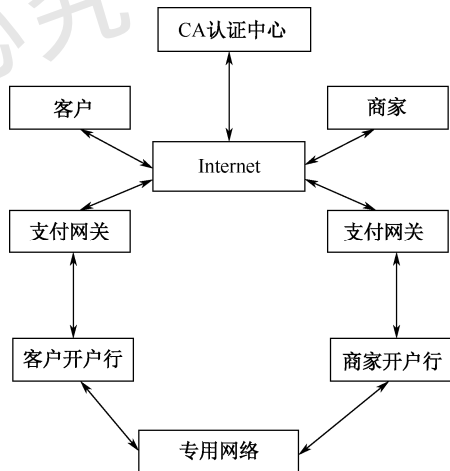


图 1-2 Internet 网络支付平台结构

方式，如纸制现金、支票、银行 POS 等方式的支付结算过程，将有助于对网络支付结算流程的理解。例如，用户通过互联网进行电子支付的流程与目前商店中的销售点系统的支付结算过程非常相似，其主要不同在于电子支付的客户通过 PC，以互联网服务器作为操作和通信的工具，而 POS 支付结算使用专用刷卡机、专用终端、专线通信。

基于互联网平台的电子支付的基本流程如图 1-3 所示。根据工作流程图，可将整个电子支付工作程序分为下面 7 个步骤。

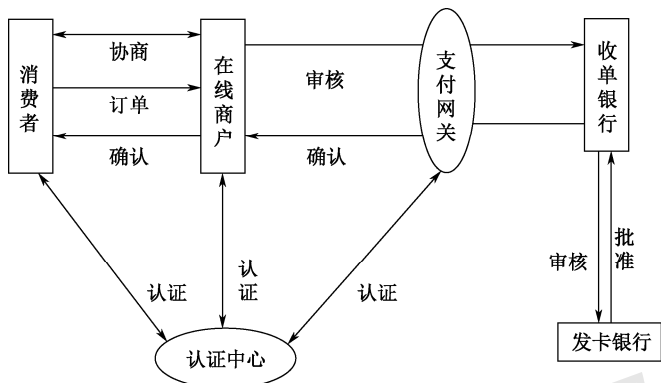


图 1-3 基于 Internet 平台的电子支付的一般流程

(1) 消费者利用自己的 PC 通过 Internet 选定所要购买的物品，并在计算机上输入订货单，订货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，告诉消费者所填订货单的货物单价、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、电子支票或网络银行账号等，确认订单，签发付款指令。此时 SET (Secure Electronic Transaction, 安全电子交易协议) 开始介入。

(4) 在 SET 中，消费者必须对订单和付款指令进行数字签名。同时利用双重签名技术保证商家看不到消费者的账号信息。

(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，再到电子货币发行公司确认。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号转移到商店账号，或通知发卡银行请求支付。

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

网络支付的基本流程只是对目前各种网络支付结算方式的应用流程的简单归纳，并不表示各种网络支付方式的应用流程与上述的一样。事实上在实际应用中，这些网络支付方式的应用流程由于技术上、资金数量上、管理机制上的不同还有所区别，但大致遵循该流程。不过像信用卡、电子现金、网络银行账号的网络支付结算流程还是有所差别的。

网络支付流程还有一个特点，即实现的是资金的立即支付，它适用于数目众多的较小金额

的电子商务业务,对客户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。这时,传统上采用独立于商务交易环节的金融 EDI 或银行专业 EFT 系统,这是目前比较普遍采用的支付结算方式。



相关链接

中国工商银行网上个人银行支付流程

(1) 登录中国工商银行网站 <http://www.icbc.com.cn/icbc/>, 单击“自助注册”按钮进行注册, 如图 1-4 所示。



图 1-4 工商银行“自助注册”界面

(2) 输入个人准确信息进行注册, 如图 1-5 所示。注册成功后, 系统提示“您已成功注册, 可以登录系统”。

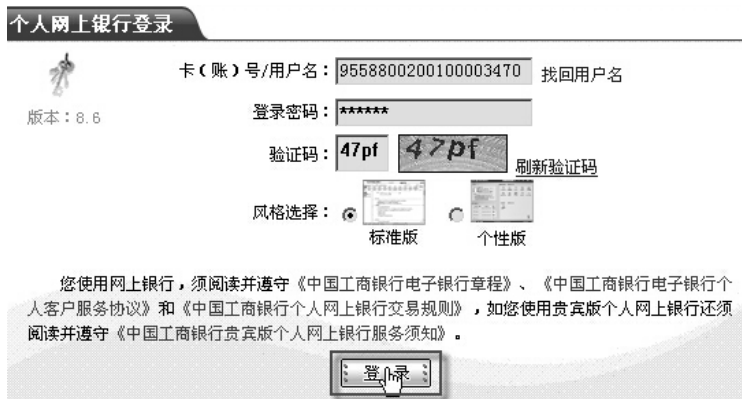


图 1-5 用户自助注册信息

(3) 登录支付宝网站 <http://www.alipay.com/>, 利用手机或 E-mail 进行注册。交易建立后, 在支付宝账户的“交易管理”中单击“付款”按钮, 如图 1-6 所示。



图 1-6 支付宝“交易管理”界面

(4) 选择要使用的网上银行，以上述中国工商银行电子口令用户为例，如图 1-7 所示。

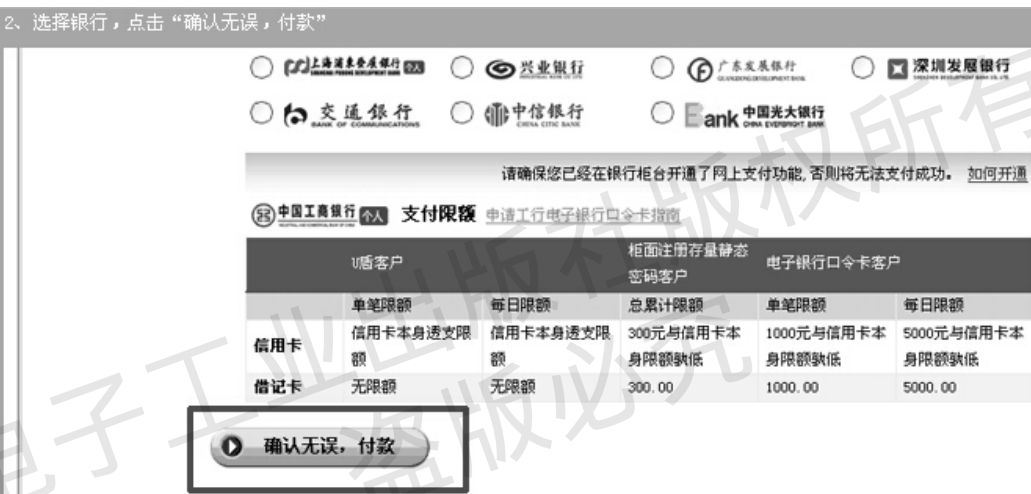


图 1-7 选择工商银行付款

(5) 显示出应付总价及选择的网上银行，单击“去网上银行付款”按钮，如图 1-8 所示。

(6) 输入卡号、验证码，单击“提交”按钮，如图 1-9 所示。



图 1-8 进入工商银行网上银行付款

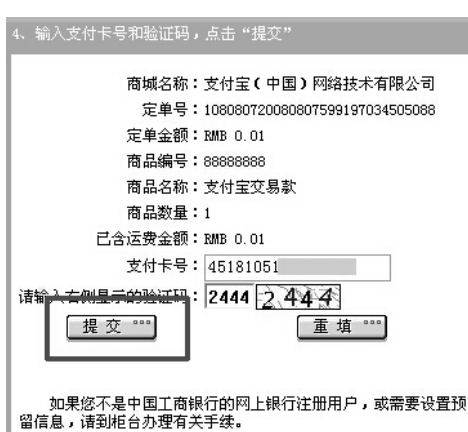


图 1-9 输入卡号和验证码

(7) 确定在工行的预留信息, 单击“确定”按钮, 如图 1-10 所示。

(8) 输入口令密码、网上银行登录密码、验证码, 单击“提交”按钮, 如图 1-11 所示。

5. 确认预留信息, 点击“确定”

您在我行的预留信息如下:

XXX

如上述信息与您在工行实际预留的信息一致, 请点击确认继续交易, 如果信息不一致, 请您立即停止交易, 并尽快与工行客服电话95588联系。

确定 取消

如果您还不是中国工商银行的网上银行注册用户, 请点击[这里](#)申请注册。

图 1-10 确定付款预留信息

6. 输入口令卡密码, 点击“提交”

定单号: 108080720080807599197034505088
定单总金额: RMB 0.01
商品编号: 88888888
商品名称: 支付宝交易款
商品数量: 1
已含运费金额: RMB 0.01
支付卡号: 4518105121636785

请输入如下显示位置的口令卡密码:

***** F3E5 ***** (了解电子银行口令卡)

网银登录密码: *****

请输入右侧显示的验证码: 1360 1360

提交 修改

图 1-11 确认支付信息并提交

(9) 页面显示支付成功, 如图 1-12 所示。

7. 支付成功

付款成功

✓ 支付宝已收到您的付款 0.01 元!

我们已经通知卖家 wl_102@yahoo.cn 发货。
[点此查看本笔交易的详情。](#)

- 返回“等待我付款的交易”;
- 查看我的账户余额;
- 给我的账户充值。

您收到货物时务必确认货物完好和一致性, 如发现表面不一致, 应当直接退货或者要求在签收
详情请参阅《[支付宝争议处理规则](#)》

登录支付宝, 在“交易管理”中进行“确认收货”

图 1-12 支付成功



实践训练

1. 课堂讨论

- (1) 电子支付的产生根源是什么? 电子交易有哪些优点?
- (2) 什么是电子支付? 电子支付具有哪些优势? 存在哪些问题?
- (3) 电子支付的一般流程是什么?

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, 正因为此才造就了中国特色的电子支付业务。

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。网银是第一个因互联网推动而标准化的银行通道能力，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。另一方面，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) 你进行过电子支付吗？下载过收费的彩铃吗？登录 <http://www.12530.com/>，找到你喜欢的彩铃，试着下载一首（收费 2 元）。你是怎么缴费支付的？与到营业厅缴纳手机费相比，你认为这种电子支付有哪些优势？

(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) 对比银行卡和网银支付的异同。

4. 课后拓展

(1) 上网查询你持有的银行卡和该银行网银的支付流程。

(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 2 单元 电子商务安全



情景案例

一个多月支付宝被盗 39 笔

2013 年初，经常淘宝的福州 90 后女生小林，把母亲的两张银行卡绑定在了自己的支付宝上，并申请了“快捷支付”功能。开通“快捷支付”后，小林网购付款时，只需输入支付宝密码，即可从两张银行卡里提取资金，进行消费。而支付宝绑定的是小林的手机号。

过了几个月，小林换了一个手机号，注销了旧号码。2013 年 2 月 27 日，小林收到一封淘宝网的退货邮件。一查淘宝账户才发现，从 1 月中旬开始，有人用她的淘宝账号，进行了 39 笔交易，母亲的两张银行卡先后有 12 000 多元被盗刷。

小林意识到账户被盗，随即报警。警方发现，39 笔交易所留的收货人电话，是小林一年前注销的手机号，收货地点是福州盖山的一家网吧，收货人姓杨，今年 20 岁，是这家网吧的网管。

在证据面前，杨某向警方交代，这个尾数为“7817”的手机号，是他 2012 年 6 月买的。2013 年 1 月 18 日，他打算用这个手机号申请一个支付宝账户，发现这个号码已绑定了一个支

付宝账户。熟悉网购的他,通过“手机号找回密码”的方式,更改了支付宝账户的原密码。

杨某用修改后的密码登录支付宝,发现这个账户开通了“快捷支付”,还关联着两张银行卡。通过“快捷支付”,杨某虽然不知道银行卡的账号、密码,但输入支付宝密码,就买到了价值400元的Q币。随后一个多月间,他用支付宝盗刷12 000多元,大部分用于购买网游装备、计算机等商品。杨某因涉嫌盗窃已被刑拘。



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最大的安全问题。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?如何才能使小林的事件不再重演?



任务分析

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。但许多商业机构对是否采用电子商务仍持观望态度,主要原因是对网上运作的安全问题存有疑虑。美国密执安大学的一个调查机构曾对23 000名因特网用户调查显示: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,使得电子商务的安全性尤其是电子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Internet上时,便会带来许多源于安全方面的问题。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抵赖性,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,致使其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,电子商务安全问题不仅仅是个技术性的问题,不仅仅只涉及技术,更重要的还有管理,而且它还与社会道德、行业管理及人们的行为模式都密切相关。

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、支付等一系列的商务活动;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,这些信息也可能会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。

1. 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着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被泄露,威胁电子商务交易的安全。一般来说电子商务安全中普遍存在着以下几种安全隐患。

(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、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,获取输入的机密信息,或通过对信息流量和流向、通信频度和长度等参数的分析,推出有用信息,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。

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。

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

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假冒信息来欺骗其他用户,主要有以下两种方式。

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,穷尽商家资源,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;伪造用户发大量的电子邮件,窃取商家的商品信息和用户信用,等等。

假冒他人身份,如冒充领导发布命令、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的格式,并可以篡改通过的信息,可以冒充合法用户发送假冒的信息或者主动获取信息,而远端用户通常很难分辨清真伪。

(4)恶意破坏。由于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,甚至可以潜入网络内部,其后果是非常严重的。

(5)交易抵赖。交易抵赖包括多个方面,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;购买者下了订货单不承认;商家卖出的商品因价格差而不承认原有的交易。

此外,各种外界的物理性干扰,例如,通信线路质量较差、地理位置复杂和自然灾害,等等,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

中国互联网络信息中心公布的《2013 年中国网民信息安全状况研究报告》指出,整体上,我国信息安全环境不容乐观,有 74.1%的网民在过去半年内遇到过信息安全问题,总人数达 4.38 亿。

在遭受经济损失的人群中,平均每人损失了 509.2 元,过去半年全国因信息安全遭受的经济损失达到了 196.3 亿元。

过去半年因网上购物发生安全问题的网民数占整体网民的 4.0%,影响人口达 2010.6 万人。因网上购物发生安全事故人群中,发生较多的是遇到欺诈信息,发生比例达 75.0%;其次为假冒网站/诈骗网站,比例为 60.7%;其他方面,个人信息泄露和账号密码被盗分别为 42.9%、23.8%,中病毒或木马的情况为 22.6%。

在因网络支付发生安全事件的人群中,遇到假冒网站/诈骗网站的比例达 57.1%。近年来,假冒的钓鱼网站较为猖獗,已经成为互联网安全的主要危害之一。此外,遇到个人信息泄露的比例为 39.3%,资金被盗、被骗和账号密码被盗的比例达 32.1%。

在智能手机上网用户群中,接收到手机垃圾短信/骚扰短信、骚扰电话的比例分别达 68.6%和 57.2%,在手机上网人群中,除了骚扰电话和垃圾短信外,发生安全事件概率最多的是手机浏览网页,发生比例达 16.8%;其次为手机游戏,发生比例达 13.8%;再次为手机聊天工具和手机下载文件,发生比例在 12%左右;其他方面,手机搜索引擎、手机购物、手机支付等也可能导致安全事件。

2. 电子商务安全要素

电子商务随时面临的威胁导致用户对电子商务安全的迫切需求,真正实现一个安全电子商务系统所要求做到的各个方面,主要包括机密性、完整性、认证性和不可抵赖性等。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,因此,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,以及计算机病毒所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/认证性

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;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,要使交易成功,必须做到:首先要能确认对方的身份,对商家要考虑客户端不能是骗子,而客户也会担心网上的商店是不是一个玩弄欺诈的黑店,所以对个人或企业实体进行身份性确

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，一般都通过证书机构 CA 和证书来实现。

例如，因特网中计算机系统的身份是由其 IP 地址确认的，黑客使用虚假 IP 地址，以达到隐瞒自己身份的目的。另外，在日常电子邮件的使用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，以确保参加交易各方身份的真实有效。

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，因此，对传送的信息要求加密，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，或者数据传输过程中信息的丢失、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。由于因特网的开放体系，只要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，同时还要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一。另外要采取适当的访问控制，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盖章来鉴别贸易伙伴，确定合同、契约和单据的可靠性，以预防抵赖行为的发生，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必须是不可否认的，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。

3. 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，极大地增加了恶意攻击的难度，并增加了审核信息的数量，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, 公钥基础设施)、网络安全技术等内容。实际上安全协议和 PKI 技术都是源于密码技术。

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、签名认证和密钥管理三大技术。

(1) 加密。所谓加密就是使用数学方法来重新组织数据,使得除了合法的接收者外,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。密码算法利用秘密密钥 (Secret Keys) 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进行解密,从而获取敏感信息并保证了网络数据的机密性。

(2) 密钥管理技术。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。在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 (Digital Signature) 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。通过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抵赖性。数字签名机制提供了一种鉴别方法,保证了网络数据的完整性和真实性。普遍用于银行、电子贸易等,以解决伪造、抵赖、冒充、篡改等问题。

(4) 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所采用的协议主要包括以下四方面。

一是电子支付协议。电子支付作为电子商务中最重要的内容,目前已经出现了很多的电子支付协议。根据人们在现实生活中常见的有基于卡的支付协议、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、E-Cash 等。

二是安全 HTTP (S-HTTP) 协议。

三是安全电子邮件协议 (如 PEM、S/MIME 等)。

四是用于公对公交易的 Internet EDI (UN/EDIFACT) 等。

(5) PKI 技术。PKI 是利用公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一整套安全基础平台。

密钥管理是电子商务安全业务中共同存在的问题,为解决在 Internet 上开展电子商务的安全问题,世界各国在经多年研究后,初步形成了一套完整的解决方案。PKI 采用证书管理公钥,即结合 x.509 标准中的鉴别框架来实现密钥管理,通过 CA 把用户的公钥及其他标识信息捆绑在一起,在 Internet 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。

2) 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。网络安全所涉及的方面比较多,如操作系统安全、防火墙技术、VPN (Virtual Private Network, 虚拟专用网) 技术和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 Internet 接入和专用网与公用网之间的安全连接。具体工作原理,在第 6 模块将进行详细叙述。



相关链接

防火墙

防火墙一般有 3 个端口,如图 1-13 所示。其中一个接外网(Internet),一个接内网,一个接 DMZ (Demilitarized Zone 的缩写,中文名称为“隔离区”),在 DMZ 区中有网络服务器。安装防火墙所要达到的效果: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,Internet 和 DMZ 的计算机不能访问内网;Internet 可以访问 DMZ 中的服务器。

VPN 也是一项保证网络安全的技术之一,它是指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在互相之间安全传递信息;同时,企业还可以利用公众信息网的拨号接入设备,让自己的用户拨号到公众信息网上,就可以连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处,是目前和今后企业网络发展的趋势。

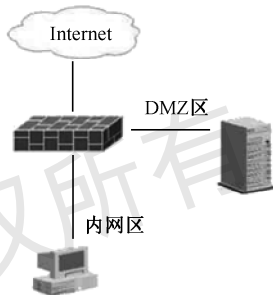


图 1-13 防火墙

4. 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完整,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,实现客户和服务器之间根据规定的安全角色来传递信息。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。所谓公平是指 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。

5. 电子商务安全法律要素

安全的电子商务除了依赖于技术因素外,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。法律法规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与企业之间、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 CA 中心的法律。CA (Certificate Authority, 证书授权中心) 是电子商务中介于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。因而必须由国家法律来规定 CA 中心的合法地位、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来对 CA 中心进行监管,并明确监管的方法及违规后的处罚措施。

(2) 有关保护个人隐私、个人秘密的法律。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,从而吸引更多的人上网进行电子商务活动。

(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。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 CA 中心和收款银行等。其中,CA 中心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。一旦因商家不付货、不按时付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,或取消商家电子支付的账号,或将商家违规情况记入 CA 中心的黑名单,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,必须加快电子商务立法。但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

Android 平台成恶意程序重灾区

2012 年,我国移动用户数量稳步增长,新增智能设备数量跃居世界首位,应用程序商店下载量快速增长。同时,移动互联网恶意程序也在快速繁衍和扩散,危害用户隐私安全,或造成垃圾短信泛滥,给感染用户造成话费损失等。

2012 年,监测到和网络安全企业通报的移动互联网恶意程序样本有 162 981 个,较 2011 年增长了 25 倍,其中约有 82.5% 的样本针对 Android 平台。Android 平台已成为恶意程序的重灾区,这主要是缘于 Android 平台的用户数量快速增长和 Android 平台的开放性。

按照恶意程序的行为属性统计,恶意扣费类的恶意程序数量仍居第一位,占 39.8%,流氓

行为类占 27.7%，资费消耗类占 11.0%，分列第二、三位。



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

针对目前存在的网络支付风险，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。

针对小林支付账号被盗的事件，支付宝采用从终端环境保护、用户认证、隐私保护、安全产品、交易行为监控等完整的链条去保障用户安全。以交易行为监控为例，支付宝开发了一套国内最先进的智能风险实时监控系统，可以实时为用户提供保护。

据支付宝方面统计，2012 年因运营商二次放号带来的账户风险不到 100 笔，占全年快捷支付总笔数的两千五百万分之一。“我们也已经宣布，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。“提升了密码手机重置安全级别，有 20% 的用户因无法找回密码而进行投诉，而这个机制对支付宝案件率的下降也几乎没有作用。”

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

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) 上网查找最近的病毒流行排行，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) 你的计算机受到过安全威胁吗？你是如何处理的？

实训说明

- (1) 本部分实训既可在课堂上进行，也可课后完成实训。
- (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

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。

第3单元 安全电子支付



情景案例

手机用来打电话、发短信人人皆知,但您能否想象,有一天,不用兑换零钱,也不用使用公交 IC 卡,乘坐公交车时只要将手机在车上轻轻一“刷”,就能潇潇洒洒地坐公交车?手机不仅可用来刷卡乘车,还可查询余额和空中充值。这听起来有点“天方夜谭”的事,却已经在湖南郴州实现,郴州市民目前能享受到这种在国内公交行业独一无二的手机支付服务。2012 年 3 月 9 日,湖南移动郴州分公司与市公共汽车公司签署了“移动公交一卡通”项目战略合作协议。

随着业务的不断推进,手机除了能乘坐公交车,还可在超市、便利店等地方进行刷卡购物,同时还可在集团单位内部实现一卡通,真正实现“一机在手,消费随心”。继卡类支付、网络支付后,手机支付俨然成为新宠。

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

消费者在进行电子支付的时候,最担心的就是安全问题。银联手机支付使用了目前国际上最先进、最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,无需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

湖南郴州市民用手机进行支付服务活动,大大地便利了人们的生活,拓展了电子支付的新领域。无论使用信用卡、网银还是移动支付,人们除了关心便捷性以外,最为担心的还是安全问题。那么,电子支付面临哪些安全威胁?其应对措施是什么?安全的电子支付对电子商务的发展和我们的生活有什么意义?

本单元主要阐述安全电子支付的内容,通过本单元的学习,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络支付与结算系统,为电子商务中的网上支付提供了重要的技术手段。

伴随着 2012 年“双十一”支付宝无线业务单日 900 万笔的业绩,可以看到用户对于移动支付的使用潜力。另外,智能终端的普及也给移动支付从硬件上带来了更广阔的可操作性。移动支付产业链各方目前都在积极寻求合作,共同开发抢占市场。为寻求自身利益最大化,银行、运营商、第三方机构各方激烈博弈,分别推出了适于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 手机等, 激烈的多方博弈导致我国之前的移动支付市场处于比较混乱的状态。

可以说 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, 未来肯定会以惊人的速度改变整个支付产业。

继手机的一卡通支付后, 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, 无需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、互联网技术以外, 支付技术和安全技术是其发展最重要的物质基础。相应的法律制度、管理规范是我国电子商务规范、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。湖南郴州率先开通的公交手机支付服务, 必然会在全国普及。电子支付的不断创新, 保障了电子商务的快速发展。但是像福州小林被盗刷资金的事件, 也给消费者的网上支付带来了隐忧。



相关知识

1. 电子支付的安全问题

信息流、商流、资金流、物流是商务活动的四大环节, 资金流又是商务运作模式的核心, 是政府、商家、客户最为关心的对象, 其运作的好坏直接影响到商务处理的效果, 因此政府、企业及家庭个人对解决资金流的运行效率和服务质量的要求也越来越高。

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, 网上金融服务面临着和很多普通互联网服务相同的安全威胁, 电子支付的有效性、真实性、机密性、完整性、认证性和不可抵赖性等安全要求面临危机, 支付的安全性变得尤为重要。

1) 电子支付面临的安全问题

在 2013 年首届中国电子支付发展研讨会上, 公安部网络安全保卫局透露, 2012 年国家网络安全保卫部门刑事犯罪立案数达 10 万多起, 其中有 46.1% 的是网络诈骗案。针对电子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支付行业。

电子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。计算机病毒是编制者在计算机程序中插入的破坏计算机功能或者破坏数据, 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, 可能会导致正常的程序无法运行, 删除计算机内的文件或使其受到不同程度的损坏。通常表现为增、删、改、移。中毒的计算机很有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称为黑客攻击。它的破坏性在于黑客攻击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, 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(CNCERT)的最新数据显示,中国遭受境外网络攻击的情况日趋严重。CNCERT 抽样监测发现,2013年1月1日至2月28日不足60天的时间里,境外6747台木马或僵尸网络控制服务器控制了中国境内190万余台主机;其中位于美国的2194台控制服务器控制了中国境内128.7万台主机。

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,其中位于美国的619台服务器承载了3673个针对境内网站的钓鱼页面,美国服务器承载钓鱼页面数量占全部钓鱼页面数量的73.1%。

(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,系统本身具有的或设置上存在的缺陷。漏洞主要是因为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,从协议规格到设计及物理硬件。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这个漏洞入侵系统,破坏系统的安全性,给电子支付带来巨大的威胁。

2) 电子支付安全问题产生的主要原因

(1) 技术原因。由于受到目前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。电子支付依赖于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”。一些单位和个人由于安全意识不强和防范手段的疏漏,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,加强对信息系统中安全保护,提升安全防范意识尤为重要,养成良好上网习惯,尽可能不在网吧等公共场合进行网上支付。

(3) 法律因素。现有的法律法规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。目前的《计算机信息网络国际联网安全保护管理办法》中规定制造和传播病毒是违法的,但是对于木马、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,每一环节都不违法,但是如果应用到窃取账号等行为时,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,但操作上还是有些困难,包括收集证据、赔偿的标准和计算方法,目前我国立法上缺少统一的规定。

(4) 安全管理滞后。由于我国电子支付方面的法律相对滞后,对电子支付市场特别是非金融机构支付监管不够,目前存在的商业银行和非金融机构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被泄露。

(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。美国建立起其完善的信用体系，足足用了一百年的时间。

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。进行电子支付时，交易双方本能地相互不信任，都害怕对方会不守信，担心自己的利益会受到侵害，因此，宁愿自己先失信，也不愿等到另一方失信后损失自己的利益。

电子商务能够促进交易的发生，降低交易的成本。但在电子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。尽快建立起一个健全的社会信用评价体系是解决我国电子支付信用问题的当务之急。

2. 安全电子支付的途径

(1) 技术保障。技术保障是指实现电子商务所需要的设备、技术等能够稳定、安全地提供所需的功能，其中主要包括实体的安全和网络安全。通过提高设备和网络安全性能，保证电子支付信息传递的完整性和可靠性。利用加密技术保证电子支付的机密性，通过验证技术保证电子支付的真实性和完整性，通过防火墙、杀毒软件等，保证计算机系统不受侵害，提高安全协议、认证技术，保证电子支付的安全性。

(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，保证电子支付安全的顺利进行。

(3) 建立健全法律法规。尽快完善电子商务、电子交易和电子支付方面的法律法规，通过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，建立一个良好的电子商务法制环境来约束人们的支付行为。

具体内容将在模块 5~9 进行详细学习。

3. 安全电子支付的意义

电子支付的广泛应用，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络支付与结算方式，这也是学习、研发、推广应用网络支付与结算方式的必要性所在。

电子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重大影响。这些影响主要表现在以下几方面。

(1) 安全的电子支付发展能够提高电子商务和金融运行效率，节约交易成本，促进经济发展。

(2) 安全的电子支付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) 安全的电子支付突破时空的限制，丰富了支付手段，促进金融创新改革和发展。

(4) 安全的电子支付方便了日常生活支付需要，有利于培养健康文明的支付习惯。

(5) 安全的电子支付将对货币政策，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影响。

(6) 安全的电子支付工具特别是信用卡的使用将促进消费信贷发展，培育社会信用体系建设。



相关链接

24 秒就被转走 10 多万元

安徽省的陈女士,在 2013 年进行网购时,被骗子诱导进行了“超级网银”授权支付操作,短短 5 分钟内,账户中 10 多万元就被洗劫一空。

陈女士在一家购物网站看中一件 200 元的衣服,店家表示需要向厂家订货,再由陈女士来进行支付,并向陈女士提供了一个“代付链接”。(代付操作是一种网购服务,即甲购买商品,但由乙来付款。)

陈女士在代付链接上进行了支付,却无法查到交易记录,于是向店家咨询。店家表示:“由于系统异常,无法正常显示交易订单,请联系客服解冻订单”,并发给陈女士一个 QQ 号。

陈女士没有多想,便与店家提供的客服 QQ 进行了联系。客服 QQ 表示:要解冻订单,需要进行“签约授权”操作,并提供了一个链接。

陈女士点开了上述链接,按照客服 QQ 的提示进行了逐步操作,但随后便发现网银账户的资金出现异常。在之后约 5 分钟时间内,骗子先后分 6 次,从陈女士账户中转走了 108 800 元,其中,前两笔金额各为 5 万元的转账,时间间隔仅为 24 秒。

上述案例是一起典型的钓鱼欺诈。其实是不法分子在正规网站进行低价诱骗顾客下单购买商品,以木马、假链接的形式进行诈骗。



实践训练

1. 课堂讨论

- (1) 电子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,人们不愿意采用电子支付方式的前两大影响因素分别是信用和安全。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,也成为了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,也可在授课后集中完成实训。
- (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) 上机了解网络安全防范手段。
- (5) 从支付和安全两方面分析:电子商务既然有这么多优点,为什么网上交易还不普及?

4. 课后拓展

上网搜集移动支付资料,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,题目可以自拟。

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,而又涉及诸如金融服务、诚信和安全其他层面。信息化、Internet 和电子支付是实现电子商务的基础条件。

电子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 Internet 作为运行平台的网络支付极大地促进了电子商务的发展。

网络支付平台主要由 Internet、支付网关和银行内部专用业务网络三部分组成。电子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,威胁电子商务交易的安全。实现一个安全电子商务系统所要求做到的各个方面,主要包括机密性、完整性、认证性和不可抵赖性等。可以通过密码技术、网络安全技术和法律规范电子商务和支付行为。

资金流处理的支付与结算问题已经成为电子商务发展的瓶颈,电子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,避免遭受利益损失。

练习测试

1. 名词解释

电子交易 电子支付 计算机病毒 黑客攻击 网络安全漏洞

2. 选择题

- (1) 下面哪个不是电子支付的“全能化”的“3A 服务”? ()

A. Anytime B. Anywhere C. Anyhow D. Anyone

(2)()是公钥基础设施的简称。

A. SET

B. PKI

C. EDI

D. Intranet

(3) 电子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) 电子商务系统必须保证具有十分可靠的安全保密技术,必须保证网络安全()。

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. 信息不被他人所接收

B. 信息内容不被指定以外的人所知悉

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,电子支付具有哪些优势?

(3) 电子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) 电子支付面临哪些安全威胁?

4. 论述题

试论述电子支付安全的重要作用。