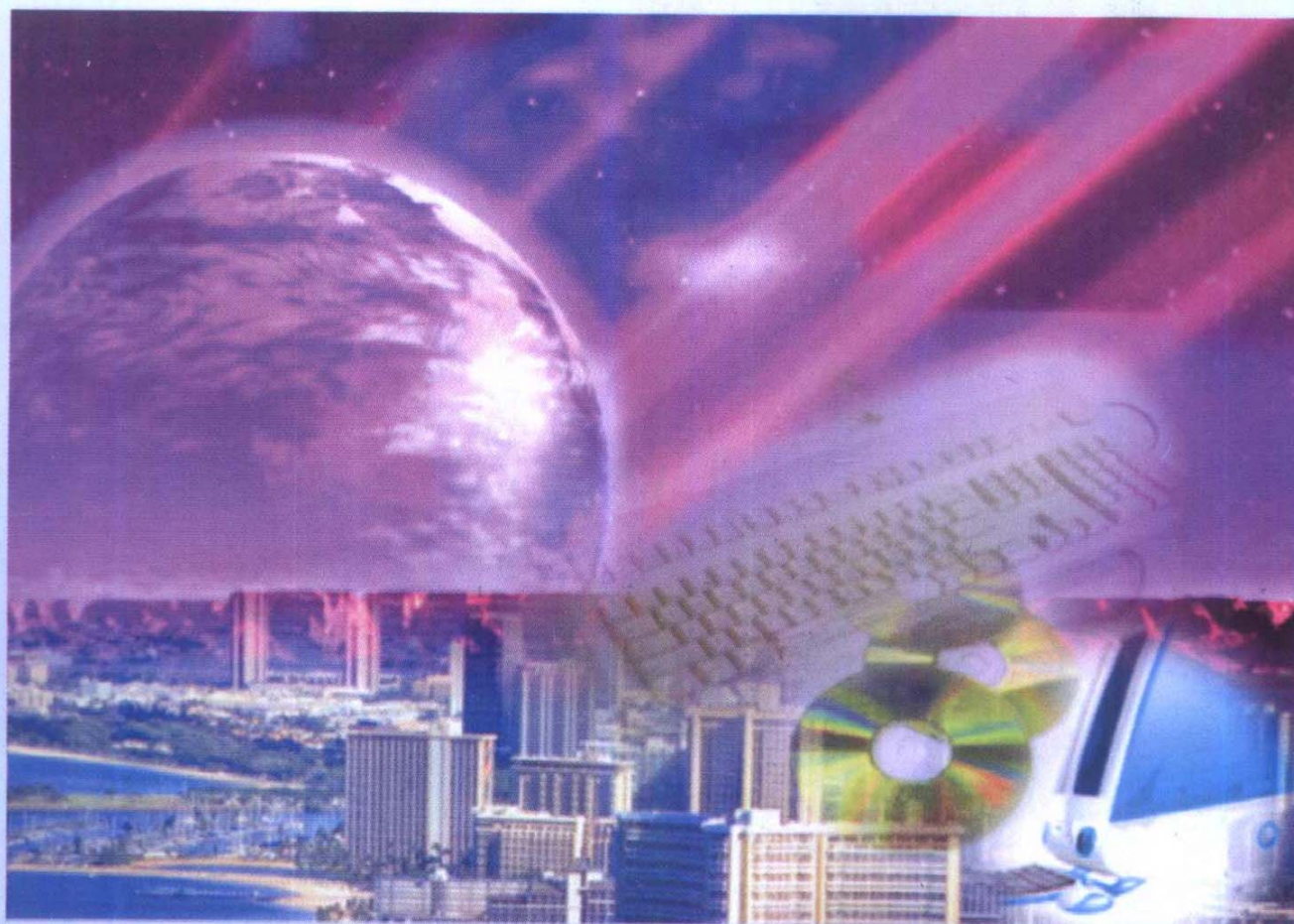




中等职业教育国家规划教材
全国中等职业教育教材审定委员会审定

电子商务 模拟运作

丛凤英 主编



对外经济贸易大学出版社

92

中等职业教育国家规划教材

F-713.36
C87

电子商务模拟运作

主 编	丛凤英	
副 主 编	肖 嘉	张宝顺
责任主审	姚新超	
审 稿	王 健	张战友

对外经济贸易大学出版社

(京)新登字 182 号

图书在版编目(CIP)数据

电子商务模拟运作/丛凤英主编. —北京:对外经济贸易大学出版社, 2002
中职教材
ISBN 7-81078-136-7

I. 国… II. 丛… III. 国际贸易-电子商务-专业学校-教材 IV. F713.36

中国版本图书馆 CIP 数据核字(2002)第 010779 号

© 2002 年 对外经济贸易大学出版社出版发行

版权所有 翻印必究

电子商务模拟运作

丛凤英 主编
责任编辑 李艺

对外经济贸易大学出版社
北京市朝阳区惠新东街 12 号 邮政编码:100029
网址: <http://www.uibep.com>

北京市飞达印刷厂印刷 新华书店北京发行所发行
开本: 787×1092 1/16 11.25 印张 288 千字
2002 年 6 月北京第 1 版 2002 年 6 月第 1 次印刷

ISBN 7-81078-136-7/F·067
印数: 00001—11000 册 定价: 13.50 元

目 录

模块一 网上交易的准备	(1)
操作一 建立企业商务网站.....	(1)
操作二 网站的搜索与推广.....	(8)
操作三 电子商务安全认证	(11)
模块二 网上交易磋商与合同订立	(22)
操作一 网上交易磋商	(22)
操作二 网上电子商务合同的订立	(38)
模块三 出口合同的履行	(50)
操作一 网上审证和改证	(50)
操作二 网上报验与报关	(65)
操作三 网上托运与投保	(82)
操作四 电子商务单证的缮制及结汇	(93)
模块四 进口合同的履行	(107)
操作一 网上开证申请.....	(107)
操作二 网上租船订舱与投保.....	(116)
操作三 网上审单付汇.....	(123)
操作四 网上报验与报关.....	(138)
附加模块一 综合测试	(149)
附加模块二 外贸业务管理及制单软件	(151)
附加模块三 加工贸易计算机联网审批管理系统	(161)
主要参考文献	(171)

模块一

网上交易的准备

【导读】

随着国际互联网的高速发展和广泛应用,企业的经营行为和竞争规则也发生了相应的变化,网上交易目前已经成为企业进行商务活动的重要手段。本模块主要为企业提供开展网上交易所需的网站建立、推广、商务信息搜索以及企业对外联系所需的安全措施等技能的训练,为企业开展电子商务打下基础。

操作一 建立企业商务网站

一、要点提示

1. Web 站点建立方案的选择

Web 站点是企业或个人在 Internet 中展示形象、发布信息的最佳平台。如果企业或个人要参与信息发布,可以根据自己的经济状况、设备条件和技术能力等因素选择一种建立 Web 站点的形式。目前采取的形式主要有两种:一种是自建方式,另一种是委托方式。

(1) 自建方式

如果一个企业有足够的经济实力和技术实力的支持,在必要的情况下可以考虑建立自己独立管理的 Web 站点。

建立自己管理的 Web 站点可以为站点的管理、维护以及信息的及时更新提供极大的灵活性,并通过合理的设计和管理,使站点具有较高的安全性和可靠性。但这种方式资金投入量大,要求有较强技术力量的支持,适用于大中型企业及信息发布商。

(2) 委托方式

如果一个企业的经济实力或技术实力达不到建立自己独立管理的 Web 站点的要求,或暂时还没有建立自己独立管理 Web 站点的需求,可以采取委托管理的方式发布信息。

几种主要的委托方式

1. 虚拟主机

在创建 Web 站点的初期,若不准备做太多的投入,但又急需发布信息,可以选用这种方式。首先企业为自己申请一个域名,然后在 ISP 的信息服务器中租用一定的空间,建立一个虚拟 Web 服务器,以虚拟站点的方式在网上发布信息。站点中 Web 页面的制作和更新可以自己完成,也可以由 ISP 代为完成。

这种方式的特点是:经济实用,无需对软硬件设备进行投资,节省了专线通信费用及构造和维护服务器的软硬件费用,而用户如同拥有自己的 Web 站点一样,只需对自己的信息进行维护即可。此方式对于初次建立网站的企业来说可以节省大量的人力、物力及一系列繁琐的工作,比较适用于中小型信息服务商和一般企业。

2. 主机托管

这种方式与建立自己独立管理的 Web 站点的方式类似,不同的是,企业建立 Web 站点的整套设备托放在 ISP 的机房,所有的设备由 ISP 代为管理和维护,不需要租用数据通信线路。站点中的信息由企业通过远程方式进行维护和更新。这是针对拥有自己独立的域名和服务器,但无力负担高昂的数据通信专线租金的用户而提供的业务。

3. 子域发布

如果一个企业既没有自己的 Web 服务器,也不准备申请自己的域名,但又希望在 Internet 上发布自己企业的信息,那么可以自己制作 Web 页面,或者委托 ISP 企业或类似企业代为制作,并在受托企业的主机上租用一定的空间,把自己的 Web 页面及信息放在受委托企业的主页下发布。这种方式非常经济实用,无需任何软硬件投资,适用于小信息服务、中小企业及个人信息的发布。

2. 建立 Web 站点的准备工作

(1) 接入 Internet

目前通常采用的连接方法是 Web 服务器连接在企业的局域网上,而企业的局域网通过数据通信线路与 ISP 连接,借助 ISP 到 Internet 的链路接入 Internet;其中需要注意的是,必须为 Web 服务器指定一个静态的 IP 地址。

企业的局域网连接到 ISP 的数据通信线路可以从电信公司租用,目前电信公司提供的数据通信线路主要包括 DDN、中继、X.25 等。企业承担的接入费用分为两部分:通信线路租用费和按流量计的信息费用。

(2) 注册域名

使用域名的最初目的是为 Internet 用户提供一种方便记忆的手段。目前,好的 Internet 域名已经远远超出了它的原有功能,就如同企业的商标、品牌一样,成为企业的标志之一。大量的企业为了进入 Internet 或尽早得到一个好的域名,正在快速地注册域名,以便在网上宣传自己的产品和服务。作为有头脑、有远见的企业家,越早行动,越有可能获得符合自己要求的域名。因此,美国在 Internet 上注册域名的公司,从 1995 年初的 25 000 家猛增到目前的 400 000 余家。

Internet 的域名结构由 TCP/IP 协议集中的域名系统(DNS, Domain Name System)进行定义。
域名申请的流程:

- ◆ 确定注册域名;
- ◆ 索取域名注册申请表;
- ◆ 填写域名申请表;
- ◆ 递交域名申请表;
- ◆ 域名注册申请表的受理。

申请域名的注意事项:

- ◆ 中国因特网的申请者必须是法人单位,且只能申请三级域名。
- ◆ 域名的命名规则:A~Z;a~z;0~9;-;未经国家有关部门批准,不得使用“CHINA”、“CHINESE”、“CN”、“NATIONAL”等字样的域名;不得使用其他国家或地区名称、外国地名、国际组织名称;不得使用县级以上行政区划名称;不得使用他人已注册过的名称;不得使用对国家、社会有害的名称。
- ◆ 域名注册须提交的材料:申请表、单位介绍信、承办人身份证复印件、本单位依法登记文件复印件;代理域名注册还须提交代理委托书、代理单位介绍信。
- ◆ 可通过中国网络信息中心的网站 www.cnnic.net.cn、电子邮件 hostmaster@cnnic.net.cn、传真 010-62559892、010-62533515 等获得和填写域名申请表,通过邮寄或面交域名申请表。

(3)域名的分类

DNS 把整个 Internet 划分成多个域,称之为顶级域。顶级域的划分采用了组织模式和地理模式两种划分模式。主要的域名如 .com、.net 等 7 个域对应于组织模式,其余的域对应于地理模式。

NIC 将顶级域的管理权分派给指定的管理机构,各管理机构对其管理的域进行继续划分,即划分成二级域,并将各二级域的管理权授予其下属的管理机构,如此下去,便形成了层次型域名结构。而且最终的域名都能得到 NIC 承认。

资料卡

中国的互联网的域名规定 (顶级域名分配)

顶级域名	分配予
.com	商业组织
.edu	教育机构
.gov	政府部门
.mil	军事部门
.net	主要网络支持中心
.org	上述以外的组织
.int	国际组织

一台主机的主机名应由它所属的各级域的域名与分配给该主机的名字共同构成,顶级域名放在最右面,分配给主机的名字放在最左面,各级名字之间用“.”隔开,如:mail.sina.com.cn。

(4)DNS 的作用

主机名只是为用户提供了一种方便记忆的手段,计算机之间不能直接使用主机名进行通信,仍然要使用 IP 地址来完成数据的传输。要找一个主机名所对应的 IP 地址需借助于域名服务器来完成。Internet 中存在着大量的域名服务器(DNS),每台域名服务器保存着它所管辖区域内的主机名与 IP 地址的对照表。

当 Internet 应用程序接收到一个主机名时,它向本地的域名服务器查询该主机名所对应的 IP 地址,如果本地域名服务器中没有该主机名所对应的 IP 地址,则本地域名服务器向其他域名服务器发出援助信号,由其他域名服务器配合查找,并把查找到的 IP 地址返回给 Internet 应用程序。

(5)获得 IP 地址的方法

对于提供接入服务的 ISP,可向 APNIC(管理亚太地区 IP 地址分配)申请成为会员;向已成为 APNIC 会员的 ISP 申请接入 ISP;加入一个 IP 地址分配联盟,通过此组织向 APNIC 申请 IP 地址。

读一读

网易个人主页空间的申请和注册的方法

1. 进入主页(<http://www.nease.net>),选“共享资源”栏目下的“个人主页 WebPage,加入“登录网页”;
2. 弹出“网页个人主页申请表”,填写申请表,单击“提交”按钮;
3. 若在 3 天内没有收到 Nease 发来的 E-mail,应当重新申请;
4. Nease 发来的 E-mail 包含用户名、口令、地址和一个免费的 E-mail 账号;
5. 为安全起见,应当修改口令。方法是:运行 `telnet://www.nease.net` 或“`telnet://202.96.152.194`”,连入 Nease 主页,然后输入自己的用户名及口令。

CNNIC(中国网络信息中心)以国家 NIC 的身份于 1997 年 1 月正式成为 APNIC 的会员,成立了以 CNNIC 为召集单位的分配联盟,CNNIC 必须将其分配联盟单位的名单及 IP 地址分配情况报告 APNIC。

3. 站点管理

(1)制作网页之前,必须先对网站进行整体规划,可以用树状结构先把每个页面的内容大纲列出来,尤其当要制作一个很大的网站(有很多页面)的时候,特别需要把这个架构规划好,同时也要考虑到以后可能的扩充性,以免做好以后又要一改再改整个网站的架构。

(2)大纲列出来后,还必须考虑每个页面之间的链接关系。是星形、树形,还是网形链接,这也是判别一个网站优劣的重要标志。链接混乱,层次不清的站点会造成浏览困难,影响内容功能的发挥。

(3)为了提高浏览效率,方便资料的寻找,网站的框架基本采用“蒲公英”式,即所有的主要链接都在首页上,每个主链接再分别展开,主链接之间相互链接。

(4)在 FrontPage 中进行站点管理的注意事项:

- ◆ 建立站点后,新建网页都要在“文件夹列表”中点击右键“新建网页”,这样网页才会正确地存入站点,站点浏览或站点上传时才会正常。
- ◆ 所有设计网页时需要的图像先将其复制到 Image 文件夹中,在网页中需要其他地方的图像也要及时地复制到 Image 文件夹中,(一般网页保存时会提醒!)
- ◆ 当建立多个网页或复制多张图片进入文件夹后,FrontPage 会自动在这些文件夹中建立“- private”文件夹。
- ◆ 上传网站时,注意不要将“- private”上传至 Internet 空间中,除非要通过本机直接管理 Internet 上的站点。
- ◆ 当设计窗口中出现“文件夹列表”窗口后,设计界面会变得很小,可以通过“查看”菜单,关闭或显示“文件夹列表”或“视图栏”窗口。

资料卡

好站点的准则

最好的 Web 站点是那些看上去很吸引人,页面简洁,并且不需用户等待很长时间信息就会出现站点。下面是创建一个成功站点的一些准则:

1. 目标明确;
2. 心中时刻想着用户浏览的方便性;
3. 使用下载快的项;
4. 使你的站点在视觉上很吸引人;
5. 不要把所有的东西都放在一页;
6. 用智能方式组织你的内容。

4. 网页的制作

(1) 网页的功能

网页就是 HTML 文件,是一种可以在 WWW 网上传输,并被浏览器认识和翻译成页面显示出来的文件。

网页对于一个企业来说是企业在 Internet 上的主要对外窗口,代表了企业在 Internet 这个虚拟的世界中的形象,同时企业与政府、相关企业以及顾客之间的所有信息交流和服务大多数是通过网页这一载体来完成的。

(2) 网页的组成

一个网页主要由框架、表格、文本、图片、动画、背景颜色、表单、超级链接以及悬停按钮、横幅广告、字幕等动态效果组成。

(3) 网页制作的注意事项

网页应该很吸引人,目标明确,页面简洁,应使重要的信息尽可能地显而易见并易于找到,并且不会让用户等待很长时间信息就会出现在屏幕上。

同时,要考虑网页在不同配置的电脑上显示可能出现的分辨率问题、语言问题等。

(4) 网页制作的总体步骤

- ◆ 选择主题;
- ◆ 规划框架;
- ◆ 资料收集;
- ◆ 具体制作(网页、图片、动画等);
- ◆ 测试链接(特别应该复制所有网页到其他电脑上进行测试并测试网页的实际速度)。

二、基本练习

1. 填空题

- (1) 域名服务器的功能是_____。
- (2) 在文件夹列表中_____新建网页。
- (3) 文本段落设置缩进与行距的方法是_____。
- (4) 可以在图片上添加的热点样式有:_____,_____,_____。
- (5) 表格除了可以作为数据表格外,还可以作为_____使用,这种使用方法一般是将表格设置为_____。
- (6) FrontPage2000 提供了_____种框架模板。
- (7) 改变框架尺寸的最方便的方法是_____。
- (8) 无需服务器支持的几个常用动态效果组件是_____、_____、_____。
- (9) 悬停按钮的效果有以下几种:_____、_____、_____、_____、_____、_____、_____。
- (10) 将向右行走的字幕改为向上行走的字幕方法,是将字幕的 HTML 源代码中 direction = right, 改为_____。

2. 单项选择题

- (1) 超级链接源可以是()。

A. 一个句子	B. 一个图像	C. 一个按钮	D. 一个符号
---------	---------	---------	---------
- (2) 设定加粗文本是使用格式工具栏上的_____按钮。

A. B	B. I	C. U	D. A
------	------	------	------
- (3) 网页中可以设置超级链接的有_____?

A. 文本	B. 图片	C. 表单	D. 表格
-------	-------	-------	-------
- (4) 设定表格的边框样式有_____和_____两种。

A. 亮边框	B. 左边框	C. 上边框	D. 暗边框
--------	--------	--------	--------
- (5) 格式化图片不能完成_____。

A. 调整大小	B. 设置透明色	C. 加边框	D. 替换文本
---------	----------	--------	---------
- (6) 格式化段落操作可以包括以下哪几种? _____

A. 首行缩进	B. 行距大小	C. 段前段后距离	D. 对齐方式
---------	---------	-----------	---------
- (7) 字幕的表现方式有以下几种_____。

A. 滚动条	B. 幻灯片	C. 交替	D. 飞跃
--------	--------	-------	-------
- (8) 常说的网页图片格式扩展名为_____。

- A.GIF B.BMP C.JPG D.PNG
- (9) 文本分行用_____组合快捷键。
- A.Ctrl + Enter B.Shift + Enter C.Enter D.Caps Lock
- (10) 表单的提交目标有_____。
- A. 文件 B. 数据库 C.E - Mail D. 按钮

3. 判断题

- () (1) FrontPage2000 不可以进行站点管理。()
- () (2) 超级链接样式的下划线可以除去。()
- () (3) 表单只能提交到数据库和电子邮件。()
- () (4) 所有浏览器都支持框架。()
- () (5) 网页中不能插入 BMP 图像。()
- () (6) 动态效果均需服务器软件支持。()
- () (7) 字幕动态效果的行走方向只能是向左和向右。()
- () (8) 表格只能作数据表格。()
- () (9) 网页不能随计算机显示器的分辨率而自动调整。()
- () (10) 在 FrontPage2000 中剪裁图像后无法按照图像大小保存图像文件。()

三、网上操作

1. 运行本书配套的教学训练软件；
2. 打开模块一的操作一，阅读“操作要求”并根据提示获取有关信息；
3. 完成操作；
4. 按要求提交操作结果。

四、附加练习

请按下述公司的基本背景，为其设计网页(包括主页面、公司简介、产品介绍等页面)：

汕头茶叶进出口公司是一家以从事茶叶出口贸易为主，多种经营的国有进出口企业，集生产、科研、贸易于一体，自 50 年代创立以来，坚持“重合同、守信用”原则，并以“信誉第一、平等互利”精神，同世界 50 多个国家地区建立贸易关系。

公司现有下属企业 12 家，专业技术人员 100 多人，拥有规模大、卫生条件好、生产能力强、机械设备先进的茶叶加工厂，公司生产的茶叶品种齐全、质量稳定、价格具有竞争性，公司出口的茶叶品种有乌龙茶、普洱茶、花茶、绿茶、饼茶、袋泡茶、健美茶、减肥茶以及各款装潢别致的小包装礼品茶等。在各类茶叶中，凤凰单丛、岭头白叶单丛、石古砵乌龙、岭头奇兰多次被评为全国名优产品，成为四大名茶，深受海内外消费者的欢迎。

操作二 网站的搜索与推广

一、要点提示

1. 网站的搜索

Internet 是一个巨大的信息资源库,每天都有新的主机连接到 Internet 上,每天都有新的信息资源被增加到 Internet 中,使 Internet 中的信息以惊人的速度增长。然而 Internet 中的信息资源分散在无数台主机之中,如果用户想在数百万个网站中快速有效地查找想要得到的信息,就要借助于 Internet 中的搜索引擎。

搜索引擎是 Internet 上的一个网站,它的主要任务是在 Internet 中主动搜索其他 Web 站点中的信息并对其自动索引,其索引内容存储在可供查询的大型数据库中。当用户利用关键字查询时,该网站会告诉用户包含该关键字信息的所有网址,并提供通向该网站的链接。

目前国内用户使用的搜索引擎主要有两类:即英文搜索引擎和中文搜索引擎。常用英文搜索引擎包括 Google、Yahoo!、Infoseek、AltaVista、Lycos 等;常用的中文搜索引擎主要有中文 Yahoo、搜狐、网易、Cseek 等。但是用户并不需要掌握所有搜索引擎的使用方法,只要熟练地掌握二三种搜索引擎即可。

(1) 使用英文 Yahoo!

Yahoo! (<http://www.yahoo.com/>)是目前常用的互联网导航服务网站,以其优秀的分类目录功能著称,它的查询数据库很有限,约 50 万条记录,但基本覆盖了 Internet 中的主要论题及著名的站点。Yahoo! 的使用非常简单,它提供了两种查询方式:按分类目录查询和按关键字查询,用户可以按上面的网址进入 Yahoo! 主页。

资料卡

输入关键字进行搜索的技巧

用户输入关键字时可以使用如表所示的符号,使用这些符号可以对查找的内容做更严格的限制。

符号	功能
关键字	查询完成符合关键字串网站
t:关键字	搜索引擎只查询网页标题
u:关键字	搜索引擎只查询网页中的链接,即 url
+ 关键字	限定关键字串一定要出现在结果中
- 关键字	限定关键字串一定不要出现在结果中
* 关键字	查找所有包含以关键字开头的术语的网站

(2) 使用“搜狐”

搜狐(<http://www.sohu.com>), 也称为 sohu, 是目前在国内比较有影响的一个简体中文互联网导航系统。“搜狐”的较强功能是它的分类目录。“搜狐”的分类目录是专为中国用户设计的, 全部采用人工分类, 符合人们的思维习惯。它把所有精选的中文站点归类, 如娱乐休闲、计算机与互联网、工商经济、科学、艺术、文学、生活服务、科学技术、政治法律等等, 并在每个最初目录下, 都建立全面丰富的目录树系统。可通过初级目录进入到下一级目录。

除分类和关键字搜索功能外, “搜狐”还设立了多个搜索频道, 包括新闻、体育、工商、房地产、影视、游戏等。用户可以通过搜索频道快速找到关于某个方面的热点站点的链接。

2. 推广企业网站的主要方法

一个网站的成功制作, 只是网站开发的第一步。而使网站具有一定知名度及访问量, 让网站的价值得到最大体现, 则需要对网站进行很好的推广。也就是说, 人们如何才能在全球数百万的网址中找到您的网址, 这就需要宣传和推广企业网站。

有效地进行网站推广, 是检验网站功效、完善网站功能、实现网站效益的必然方式。

(1) 网站宣传推广的一般方法

- ◆ 通过“互联网广告发布专家系统(Mr. Post)”发布广告: 可以在较短的时间内自动地、智能地、并发地、高成功率地将自己的广告内容发送到两百多个中文国际经贸站点和 300 多个英文国际经贸站点。
- ◆ 知名网站相互链接: 商务站点可与一些访问量较大的网站进行链接, 以别人的知名度来带动自己站点的知名度, 以提高自己站点的访问量。
- ◆ 通过 BBS 吸引客户: 企业网站中开设 BBS(电子公告板)的主要目的是吸引客户了解市场动向和引导消费市场。
- ◆ 将公司资料加入到世界著名的专业数据库, 如香港贸发局数据库、中国进出口贸易网、广东企业网等。
- ◆ 将公司网址在搜索引擎登记(包括软件自动注册——这类软件很多, 比较易用和具有代表性的是 Submit Wolf PRO, 它可以一次完成 800 个搜索引擎的注册工作; 手工注册——搜索引擎(如 Yahoo)是不支持软件自动注册方式的, 所以必须通过手工注册才能完成)。

(2) 利用著名的搜索引擎

世界上有三大著名商业搜索引擎公司(Yahoo, Excite, Altavista), 是所有买家、卖家寻找新产品和供求信息时必到之处。买家和卖家可以根据行业、国家、地域、具体产品等内容进行查询, 并马上可以得到查询结果——这是企业最有效的网站宣传推广方式, 也是互联网络以其低成本、高效率的优势迅速成为国际贸易主流的主要原因。通过 Internet, 出口企业可以直接找到国外的潜在客户, 进口企业也可以找到所需要的产品和供应商。

(3) 推广企业网站的注意事项

- ◆ 应将网站的宗旨和功能由内而外的推广运用;
- ◆ 根据企业的形象、产品的特点、面对的潜在客户等选择合适的宣传方式。
- ◆ 根据企业的性质和推广的目标, 选择通用的搜索引擎或专业的搜索引擎进行注册;
- ◆ 注册搜索引擎时, 对注册的关键字如行业、地区、产品、特征等内容的填写应全面细致;

◆ 推广成功后应定期模拟客户进行搜索,及时发现并修改错误的搜索结果。

二、基本练习

1. 填空题

(1)搜索引擎包括_____和_____两种方式。

(2)“分类检索”是从搜索首页按照_____型的主题分类逐_____点击来查找所需信息的方法。

(3)“关键词查询”是用所需信息的_____进行查询的方法。

(4)对网站进行多个关键词查询,多个关键词之间一般有_____、_____、_____等三种关系。

(5)注册搜索引擎时所用的联系人_____和联系人_____是日后是否有修改或删除该搜索条目的权限的唯一身份认证。

2. 单项选择题

(1)网站标题搜索时是在关键字前加_____。

A. t B. or C. u D. *

(2)在搜索多个关键词时用“且”,则用_____连接关键词。

A. OR B. NOT C. — D. |

(3)搜索结果是根据与查询要求相匹配的结果的_____来排列相关的分类目录和网站

A. 新旧 B. 大小 C. 质量 D. 字母顺序

(4)注册搜索引擎时一般不用填写_____。

A. 网站名称 B. 网站 URL C. 联系电话 D. 分类名称

3. 判断题

() (1) 注册搜索引擎全部是免费的。

() (2) 注册搜索引擎只能选择一个关键词。

() (3) 搜索“.com”可得到全球所有的网址。

() (4) 一般可以在已搜索的结果中缩小范围重新搜索。

() (5) 已注册的搜索条目不能修改或删除。

三、网上操作

1. 运行本书配套的教学训练软件;

2. 打开模块一的操作二,阅读“操作要求”并根据提示获取有关信息;

3. 完成操作;

4. 按要求提交操作结果。

四、附加练习

搜索与福建安溪制造乌龙茶有关的厂家,不包含“制造工艺”的内容。

操作三 电子商务安全认证

随着 Internet 热潮席卷全球,电子商务日益成为目前最时髦的词汇之一。企业的电子商务系统也包括 Internet,作为一个世界范围内的开放网络,在提供方便的同时,也带来信息安全的问题。网络安全主要考虑涉及隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私,同时也避免其他用户的非授权访问和破坏。本操作主要提供网络信息的安全保密性、完整性、不可否认性等保护措施的训练。

一、要点提示

1. 商务信息的加密

加密技术是电子商务采取的主要安全措施,贸易方可根据需要在信息交换的阶段使用。加密技术指的是将数据进行编码,使它成为一种不可理解的形式,这种不可理解的内容叫密文。加密技术能避免各种存储介质(硬盘、软盘、磁带)上的或通过 Internet 传送的敏感数据被窃取。由于原文加密带有机密性,因而加密技术也适用于检查信息的真实性和完整性。

解密是加密的逆过程,即将密文还原成原来的可理解的形式。

(1)加密的二要素:加密和解密过程中依靠“算法”和“密钥”两个基本元素,缺一不可。其中“算法”是加密或解密的一步一步的过程,“密钥”是这个过程中需要一串串的数字。

算法和密钥在加密和解密过程中缺一不可。在实际过程中,一般来说,加密算法是不变的,加密的算法也是屈指可数的,但是密钥是变化的,其方法也是多种多样的。也就是说,加密技术的关键是密钥。

资料卡

密码技术的历史

密码通信的历史极为久远,其起源可以追溯到几千年前的埃及、巴比伦、古罗马和古希腊。世界上最早的一种密码产生于公元前两世纪。是由一位希腊人提出的,人们称之为棋盘密码,原因为该密码将 26 个字母放在 5×5 的方格里,i,j 放在一个格子里,具体情况如下表所示:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i,j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

这样,每个字母就对应了由两个数构成的字符 $\alpha\beta$, α 是该字母所在行的标号, β 是列标号。如 c 对应 13,s 对应 43 等,如果接收到密文为:

43 15 13 45 42 15 32 15 43 43 11 22 15

则对应的明文即为 secure message(秘密信息)。

密码技术的成果首先被用于战争,下面的例子就是一个明证。1914 年第一次世界大战爆发,德俄相互宣战。在交战过程中,德军破译了俄军第一军给第二军的电文,从中得知,第一军的给养已经中断。

根据这一重要情报,德军在这次战役中取得了全胜。在 20 世纪 20 年代,人们发明各种机械加密设备用来自动处理加密。大多数是基于转轮的概念,机械转轮用线连起来完成通常的密码代替,最著名的是第二次世界大战期间德国的恩尼格马机械密码机。波兰密码小组最早破译了德国的恩尼格马,并告诉了英国人。德国人在战争进行过程中修改了他们的密码。英国人继续对新的方案进行分析,1942 年终于破译德军密码体系。同样,1940 年,美国陆军通信机关破译了日本使用的九七式机械密码,在中途岛海战中,日本海军大将山本五十六的飞机因密码电报被美国截获破译而被击中,进而使战争进程加快结束。

(2) 密钥的长度

密钥的长度是指密钥的位数。一般来说,密钥位数越长,被破译的可能就越小;反之,密钥位数越短,被破译的可能就越大。密文的破译往往是经黑客长时间的测试密钥,破获密钥后,解开密文。例如,一个 4 位的密钥具有 2 的 4 次方(16)种不同的密钥,顺序猜测 16 种密钥就可以将其破译。一个 16 位的密钥具有 2 的 16 次方(65 536)种不同的密钥,顺序猜测 65 536 种密钥对于计算机来说是很容易做到的。如果使用 DES 标准的 56 位密钥,计算机猜测密钥的时间需要好几百年了。因此,密钥的位数越长,加密系统就越牢固。

(3) 加密技术的分类

加密技术的分类目前主要有两种:对称加密和非对称加密。

对称加密是指使用相同的密钥加密和解密,也就是说,一把钥匙开一把锁。发送者和接收者有相同的密钥,这样就解决了信息的保密性问题。使用对称加密方法将简化加密的处理,每个交易方都不必彼此研究和交换专用的加密算法,而是采用相同的加密算法并只交换共享的专用密钥。



议一议

如果交换密钥过程中密钥被窃会出现什么情况?

资料卡

数据加密标准

数据加密标准(DES)是目前广泛采用的对称加密方式之一,是 IBM 公司为保护产品的机密于 1971 年至 1972 年研制成功的,后被美国国家标准局和国家安全局选为数据加密标准,并于 1977 年颁布使用。主要应用于银行业中的电子资金转账(EFT)领域。DES 的密钥长度为 56 位,解密时的过程和加密相似,但密钥的顺序刚好相反。

DES 的保密性仅取决于对密钥的保密,而算法是公开的。DES 内部具有复杂的结构,至今还没有人找到破译的方法。

非对称加密也称为公私密钥(PKI)算法,是指密钥被分解为一对(即一把公开密钥和一把专用密钥或一把加密密钥和一把解密密钥)。这对密钥中的任何一把都可作为公开密钥(加密密钥)通过非保密方式向他人公开,而另一把则作为专用密钥(解密密钥)加以保存。专用密钥只能由生成密钥对的交易方掌握,公开密钥可广泛发布,但它只对应于生成该密钥的交易方。

(3)非对称加密的基本过程

- ◆ 交易方甲生成一对密钥并将其中的一把作为公开密钥向其他交易方公开;
- ◆ 得到该公开密钥的交易方乙使用该密钥对机密信息进行加密后再发送给交易方甲;
- ◆ 交易方甲再用自己保存的另一把专用密钥对加密后的信息进行解密。

因此,网络中的加密普遍采用公私密钥和单钥对称密码相结合的混合加密体制,即加解密时采用单钥密码,密钥传送则采用公私密钥。这样既解决了密钥管理的困难,又解决了加解密速度的问题。

2. 数字证书

数字证书也称为公开密钥证书,在网络通信中标志通信各方身份信息的一系列数据,其作用类似于现实生活中的身份证。它是由一个权威机构发行的,人们可以在交往中用它来识别对方的身份。交易伙伴间可以使用数字证书来交换公开密钥。

资料卡

数字证书的内容

数字证书通常包含以下内容:

1. 证书所有者(即交易方)的名称,命名规则一般采用 X. 500 格式;
2. 标识证书发布者的名称;
3. 证书所有者的公开密钥、有效期;
4. 证书发布者的数字签名;
5. 证书的序列号,每个证书都有唯一的证书序列号;
6. 证书的有效期,通用的证书一般采用 UTC 的时间格式,它的计时范围一般为 1950—2049。

(1)数字证书的标准

国际电信联盟(ITU)制定的标准 X. 509 对数字证书进行了定义,该标准等同于国际标准化组织(ISO)与国际电工委员会(IEC)联合发布的 ISO/IEC 9594—8195 标准。

(2)数字证书的功能

保密性:在发送电子邮件时,使用收件人的数字证书对电子邮件加密。这样,只有收件人才能阅读加密的邮件,在 Internet 上传递的电子邮件信息不会被人窃取,即使发错邮件,收件人也无法看到邮件内容。

认证身份:在 Internet 上传递电子邮件的双方互相不能见面,所以必须用一种确定对方身份的方法,可以利用发件人数字证书在传送前对电子邮件进行数字签名即可确定发件人身份,而不是他人冒充的。