

网络安全

华师傅资讯 编著

- 安全知识，一网打尽；读者所需，尽在其中
- 摒弃门槛，由易入难；各层读者，皆有所需
- 循序渐进，环环相扣；步步为赢，得心应手
- 优秀团队，十载经验；立足读者，打造精品

铁
道
出
版
社

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

网络安全实用宝典

华师傅资讯 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

许多用户都受着计算机安全问题的困扰,所以本书以计算机安全与防黑技术为主题,从系统设置到网络安全,从数据备份到数据恢复,详细介绍了计算机安全与防黑方面的应用技巧。

全书分为3篇共23章,第1篇(1~8章)介绍了计算机安全方面的内容,包括流氓软件卸载,病毒及木马防护,个人防火墙选用,注册表及组策略安全策略,系统维护等本机的安全应用。第2篇(9~15章)介绍了网络安全方面的内容,包括网络漏洞检查,反黑客实战,网络游戏,网页浏览,邮件处理,互动聊天,购物安全等诸多基于网络应用的安全策略。第3篇(16~23章)介绍了数据安全方面的内容,包括文件、隐私的保护,电子文档的安全,磁盘故障与数据恢复,移动存储数据的维护,办公文档的数据恢复,系统备份与恢复,应用软件备份与恢复等数据维护方法与技巧。

本书适用于各类非计算机专业人员,尤其适合计算机家庭用户和办公用户阅读参考。

图书在版编目(CIP)数据

网络安全实用宝典/华师傅资讯编著. —北京:中国铁道出版社, 2007. 8

ISBN 978-7-113-08195-9

I. 网… II. 华… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆CIP数据核字(2007)第123182号

书 名: 网络安全实用宝典

作 者: 华师傅资讯

出版发行: 中国铁道出版社(100054,北京市宣武区右安门西街8号)

策划编辑: 严晓舟 魏 春

责任编辑: 荆 波 辛 杰

封面设计: 高 洋

封面制作: 白 雪

责任校对: 徐盼欣

印 刷: 北京鑫正大印刷有限公司

开 本: 787×1092 1/16 印张: 35 字数: 817千

版 本: 2007年9月第1版 2007年9月第1次印刷

印 数: 1~5 000册

书 号: ISBN 978-7-113-08195-9/TP·2524

定 价: 52.00元

版权所有 侵权必究

凡购买铁道版的图书,如有缺页、倒页、脱页者,请与本社计算机图书批销部调换。

前言

计算机及网络带给人们的方便是有目共睹的，然而随之而来的种种安全问题却令人始料不及。你的 PC 被攻击过吗？你的数据丢失过吗？估计有 80% 用户的回答是肯定的！或许你的计算机正在用杀毒软件杀毒；或许你正在为恢复数据祈祷，而且很有成就感，看到那么多的病毒、木马、广告程序被清除，那么多丢失的文件被恢复，心里还暗自庆幸。就这样慢慢地，杀毒、恢复数据成为了生活中的一部分！我们不禁会问：“你愿意这样永无止境地杀毒吗？”换句话说，PC 是用来提高自己工作效率的伙伴，不是成为杀毒和恢复数据的机器！

在使用计算机进行操作或上网时，我们经常遇到的入侵方式及“灾难”包括以下几种：

- (1) 被他人盗取密码；
- (2) 系统被木马攻击；
- (3) 浏览网页时被恶意的 java script 程序攻击；
- (4) QQ 被攻击或泄漏信息；
- (5) 病毒或流氓软件感染；
- (6) 系统存在漏洞使他人攻击自己；
- (7) 黑客的恶意攻击；
- (8) 游戏账号 ID、装备被盗；
- (9) 磁盘数据丢失；
- (10) 系统瘫痪或文件（档）损坏/丢失。

我们应想办法尽最大的努力为我们的计算机构建坚固的保护罩，这样才是明智之举！为了我们的工作、生活，还有一份好的心情，Let's go!

本书的读者对象

本书充分考虑了广大初、中级计算机用户 in 安全方面的根本需求，主要面对日常使用计算机的办公人员，以及具有一定计算机应用技能的读者。对于广大的计算机用户来说，实际上对计算机安全、网络安全、数据安全等并不精通，但又不可能花费太多精力去研习。因此，如何在最短时间内，花费较小的精力，让上述读者学到最实用的计算机安全、网络安全、数据安全方面的知识，以保证办公计算机、个人电脑日常的使用，是急需解决的问题。本书就是针对此问题而专门设计、编写的。

本书的特点

本书内容丰富、深入浅出，适合各个层次的读者学习。全书以操作为主，提供了尽可能详细的操作步骤和分解图片，使所有操作一目了然。书中所涉及到的各个方面的安全问题都是用户经常碰到的，并且是困扰用户的常见问题。通过本书的学习，用户可以联系自己的实际问题，逐步深入地学习计算机及其网络安全方面的基本知识、方法和技巧。

本书的内容结构

本书共分3篇23章，第1篇（1~8章）介绍了电脑安全方面的内容；第2篇（9~15章）介绍了网络安全方面的内容；第3篇（16~23章）介绍了数据安全方面的内容。

第1章 开门安全七件事。从计算机开机开始，介绍需要关注的几大安全设置，引起读者对计算机安全的重要性的感知。

第2章 阻击流氓软件。本书特色章节，介绍时下热门的流氓软件阻击、卸载操作。

第3章 病毒防护。从讲解病毒知识及查杀，谈到防病毒软件的使用和升级。

第4章 木马防护。介绍常见木马的查杀方法及木马专杀工具。

第5章 选用个人防火墙。介绍如何选购个人防火墙及天网/诺顿个人安全防火墙的使用。

第6章 注册表安全策略。介绍通过注册表编辑器的设置实现系统、网络安全的方法与策略。

第7章 组策略安全策略。介绍通过组策略工具的设置实现系统、网络安全的方法与策略。

第8章 系统维护宝鉴。介绍计算机常规维护，防止死机、断电和系统蓝屏的方法。

第9章 网络漏洞与端口检查。介绍系统网络服务、系统漏洞、服务端口的扫描及检查方法。

第10章 反黑客实战。介绍黑客常用的扫描程序、口令攻击程序、嗅探器的防御措施。

第11章 网络游戏安全。介绍时下流行的网络游戏密码保护措施及其硬件设备使用方法。

第12章 网页浏览安全。介绍网页浏览安全、浏览器安全防范方面的知识以及浏览器出现问题后的修复方法。

第13章 网络邮件安全。介绍电子邮件的安全问题、Web邮件的安全设置，并以实际操作为例介绍 Outlook Express 和 Foxmail 的安全设置方法。

第14章 网络聊天安全。介绍即时通讯工具 QQ、MSN 的安全防范方法，以及如何防范计算机的 IP 地址被探测。

第15章 网络购物安全。介绍网络购物的流程，并对网络购物的安全问题作全方位的阐述。

第16章 文件、隐私保护。介绍如何清除系统操作痕迹、加密解密文件与文件夹、驱动器隐藏、文件隐身等，以达到文件、隐私的安全保护。

第17章 电子文档安全。介绍 Word 文档、Excel 电子表格、Access 数据库、压缩文件、PDF 文件权限设置等办公、私人文档的安全。

第18章 磁盘数据的恢复。介绍数据丢失的原因、数据恢复前的准备工作、数据恢复软件，对各种情况下的数据丢失提供修复方法，全面掌握数据恢复的实战技能，并详细解析如何预防数据丢失。

第19章 磁盘故障诊断与排除。内容涵盖硬盘基础知识、硬盘故障判定与排除、磁盘坏道的修复和硬盘的日常管理与维护等方面的知识与技能。

第 20 章 移动存储数据的维护。从光盘保护技术开始，全面讲解光盘加密、加密光盘的复制及 U 盘、移动硬盘的内容加密保护等知识技能。

第 21 章 办公文档的数据修复。介绍 Word 和 Excel 文档的数据修复方法，以及使用软件修复工具 FinaDATA 和 EasyRecovery 修复文档的操作技巧，并对 Office 密码破解工具的使用方法作全面的讲解。

第 22 章 系统备份与恢复。从系统还原的重要性开始，讲述如何使用系统备份工具对系统进行备份和恢复。

第 23 章 应用程序的备份与恢复。本章主要讲述如何备份和恢复计算机系统中一些重要的数据，比如：系统配置、注册表、IE 数据、OE、邮箱数据、聊天资料、应用软件等。

本书由专业资讯工作室华师傅资讯编著，张华、张思成、李俊峰、赵永磊、滨海欧承担了主要的编写工作，另外，蒲银廷、牛晓燕、蔡景荣、冯越、万雷、田园、姚新军、徐健、杨明、李树成、谢春雷、李玲、路文彬、黄成利、高山、胡磊、李洪贵、王新亮、姜金元、李恒亮、苏义、孔宪伟、孙名古、张超等老师也参与了本书的编写工作，在此一并感谢。由于编者水平有限，加上时间仓促，欢迎广大读者对书中不足之处批评指正。

华师傅资讯

2007 年 6 月

目 录

第 1 篇 电脑安全篇

第 1 章 开门安全七件事	3
1.1 设置 BIOS 开机密码	3
1.1.1 设置进入 CMOS 的密码	4
1.1.2 设置开机密码	4
1.2 设置系统登录密码	4
1.2.1 创建账户	4
1.2.2 设置密码	5
1.3 设置系统启动密码	6
1.3.1 系统启动密码的设置	6
1.3.2 系统启动密码的应用	6
1.3.3 制作钥匙盘	7
1.4 设置屏幕保护密码	7
1.4.1 Windows 98/Me 屏幕保护密码设置	7
1.4.2 Windows 2000/XP 屏幕保护密码设置	7
1.5 快速锁定系统	8
1.5.1 快捷方式法	8
1.5.2 Windows+L 键法	9
1.5.3 使用待机功能	9
1.6 更改默认账号设置	10
1.6.1 Administrator 账号	10
1.6.2 Guest 账号	12
1.6.3 为用户设置合适的身份	13
1.7 禁止/关闭/删除未使用和不需要的服务及进程	15
1.7.1 禁止 Windows 中不必要的服务	15
1.7.2 管理自启动程序	18
第 2 章 阻击流氓软件	21
2.1 认识流氓软件	21
2.1.1 流氓软件概述	21
2.1.2 流氓软件的来源	23
2.2 手动卸载流氓软件	24
2.3 利用工具软件卸载流氓软件	25
2.3.1 完美卸载软件	25

2.3.2	超级兔子	27
2.3.3	优化大师	31
2.3.4	360 安全卫士	32
2.4	卸载顽固的流氓软件	36
2.4.1	卸载 3721	36
2.4.2	卸载 DuDu 加速器	38
第 3 章	病毒防护	39
3.1	病毒概述	39
3.1.1	病毒的定义	39
3.1.2	计算机病毒的分类	40
3.1.3	病毒发展趋势	42
3.2	病毒的防治	43
3.2.1	判断计算机是否感染病毒	43
3.2.2	典型病毒及其防治	44
3.3	防病毒软件的使用	47
3.3.1	瑞星杀毒软件	48
3.3.2	江民杀毒软件	50
3.3.3	金山毒霸	56
3.4	防病毒软件的升级	59
3.4.1	病毒库更新	59
3.4.2	病毒隔离	60
第 4 章	木马防护	61
4.1	木马概述	61
4.1.1	木马特性	61
4.1.2	木马类型	62
4.1.3	感染木马病毒后出现的状况	63
4.2	发现木马	64
4.2.1	木马常用端口	64
4.2.2	木马过滤器	66
4.2.3	木马运行机制	66
4.3	常见木马的检查方案	68
4.3.1	木马隐身方法	68
4.3.2	手动查杀木马	69
4.4	木马专杀	72
4.4.1	木马防线	72
4.4.2	木马清道夫	75
第 5 章	选用个人防火墙	78
5.1	防火墙简介	78
5.1.1	什么是防火墙	78

5.1.2	防火墙的分类.....	78
5.1.3	防火墙的主要功能.....	83
5.2	如何选购个人防火墙	84
5.2.1	个人防火墙推荐.....	84
5.2.2	免费的个人防火墙	86
5.3	天网防火墙个人版的使用	87
5.3.1	天网防火墙	87
5.3.2	设置天网防火墙的安全规则	87
5.3.3	网络访问监控功能.....	91
5.3.4	日志查看	91
5.3.5	在线检测服务.....	92
5.4	诺顿个人安全防火墙	92
5.4.1	软件简介	92
5.4.2	设置个人防火墙选项	93
5.4.3	使用 LiveUpdate 进行更新	94
5.4.4	执行全面系统扫描.....	94
5.4.5	防护设置	95
5.4.6	安全漏洞扫描.....	96
5.4.7	响应安全问题.....	97
第 6 章	注册表安全策略	99
6.1	注册表综述.....	99
6.1.1	注册表的由来.....	99
6.1.2	注册表的功能.....	100
6.1.3	注册表的编辑.....	102
6.1.4	注册表的备份.....	107
6.2	安全登录.....	110
6.2.1	显示登录窗口选项 	110
6.2.2	指定密码的最小长度 	110
6.2.3	禁止显示前一个登录者的名称 	110
6.2.4	将 Windows 网络登录口令不保存为 PWL 文件 	111
6.2.5	开机自动进入屏幕保护 	111
6.2.6	在“登录”对话框中隐藏“关机”按钮 	111
6.2.7	Windows NT 有效密码的设置 	112
6.2.8	从“开始”菜单中删除“网上邻居”图标 	112
6.2.9	从“开始”菜单的设置中删除任务栏 	113
6.2.10	禁止去除“开始”菜单中的“注销”菜单项 	113
6.2.11	隐藏“开始”菜单中的“文档”菜单项 	114
6.2.12	屏蔽“开始”菜单中的“运行”等功能 	114
6.2.13	在退出 Windows 时清除“文档”中的历史记录 	115

6.2.14	从“开始”菜单中删除用户文件夹	115
6.2.15	设置从睡眠或挂起状态恢复时是否需要输入密码	116
6.2.16	桌面安全限制	116
6.2.17	禁用活动桌面所有设置项目	116
6.2.18	阻止欢迎屏幕显示未读邮件消息	117
6.3	限制系统功能	117
6.3.1	从“我的电脑”菜单中删除“属性”菜单项	117
6.3.2	禁止在桌面及资源管理器中右击时弹出快捷菜单	118
6.3.3	禁止用户运行某些程序	118
6.3.4	通过注册表删除各种历史记录	118
6.3.5	屏蔽“网上邻居”中的一些功能	118
6.3.6	禁用 MS-DOS 方式	119
6.3.7	阻止访问命令提示符和批处理文件	119
6.3.8	从 Windows 资源管理器删除“安全”选项卡	120
6.3.9	禁止使用 REG 文件	120
6.3.10	禁止使用 INF 文件	120
6.3.11	隐藏“控制面板”中的程序选项	120
6.3.12	禁用“控制面板”中的“用户”和“密码”设置项	121
6.3.13	禁止在“控制面板”中使用“网络”属性	121
6.3.14	禁用控制面板	121
6.3.15	隐藏“控制面板”的“显示”设置项中的各个选项卡	122
6.3.16	屏蔽“控制面板”所有设置项目	123
6.3.17	隐藏“控制面板”中的项目和文件夹	123
6.3.18	屏蔽系统属性菜单的各子项	124
6.3.19	禁止普通用户查看事件记录	125
6.3.20	删除“显示”选项中的“主题”设置页	125
6.3.21	禁用屏幕保护程序设置	126
6.3.22	禁止屏幕保护程序的密码被更改	127
6.3.23	屏蔽“添加/删除”项中的“更改或删除程序”选项	128
6.3.24	屏蔽“添加/删除”项中的“添加新程序”选项	128
6.3.25	屏蔽“添加新程序”中的“从 CD-ROM 或软盘安装程序”	128
6.3.26	隐藏“添加/删除 Windows 组件”	129
6.3.27	删除“添加/删除程序”程序	129
6.3.28	隐藏“从网络中添加程序”选项	130
6.4	加强网络安全	130
6.4.1	清除恶意修改	130
6.4.2	开机自动弹出的网页	131
6.4.3	系统启动时的弹出对话框	131
6.4.4	IE 标题栏被修改	132
6.4.5	IE 默认连接首页被修改	132

6.4.6	篡改 IE 的默认页	133
6.4.7	修复被锁定的注册表	133
6.4.8	IE 浏览器默认主页被修改, 设置项被锁定	134
6.4.9	IE 右键快捷菜单被修改	134
6.4.10	查看“源文件”菜单被禁用	134
6.4.11	IE 中鼠标右键失效	134
6.4.12	IE 默认搜索引擎被修改	135
6.4.13	在 IE 地址栏中多出了文字	135
6.4.14	操作系统被修改	135
6.4.15	IE 窗口定时弹出	136
6.4.16	IE 工具栏被添加网站链接	136
6.4.17	网络连接限制 	136
6.4.18	删除网络共享 	136
6.4.19	防范远程用户非法入侵 	137
6.4.20	禁止允许未认证的用户进入网络列举域内用户  	137
6.4.21	清除访问“网络邻居”后留下的字句信息 	137
6.4.22	隐藏“控制面板”中网络标识页的部分项目 	137
6.4.23	隐藏“控制面板”中网络访问控制页 	138
6.4.24	从“网上邻居”中屏蔽“工作组”   	138
6.4.25	隐藏“网上邻居” 	138
6.5	加强文件/文件夹安全	139
6.5.1	修改系统文件夹的保护属性  	139
6.5.2	隐藏资源管理器中的磁盘驱动器   	139
6.5.3	从 Windows 资源管理器中删除“文件”菜单 	140
6.5.4	彻底隐藏文件夹下的内容 	141
6.5.5	禁止用户使用“我的电脑”访问所选驱动器的内容  	141
6.5.6	禁止资源管理器自动加密文件 	142
6.5.7	不显示“共享文档”文件夹 	142
6.5.8	禁用调整桌面工具栏 	143
6.5.9	锁定我的文档   	143
6.5.10	锁定回收站   	143
6.5.11	从“我的文档”上下文菜单中删除“属性”菜单项 	144
第 7 章	组策略安全策略	145
7.1	组策略综述	145
7.1.1	组策略与注册表	145
7.1.2	在 Windows 98 中应用组策略	145
7.1.3	Windows 2000/XP/2003 组策略控制台	148
7.1.4	组策略中的管理模板	149
7.2	“桌面”安全设置	150

7.2.1	隐藏桌面的系统图标	150
7.2.2	不要将最近打开的文档的共享添加到网上邻居	151
7.2.3	禁止用户更改“我的文档”路径	151
7.2.4	禁止添加、拖、放和关闭任务栏的工具栏	152
7.2.5	退出时不保存桌面设置	152
7.2.6	屏蔽“清理桌面向导”功能	152
7.2.7	禁用“活动桌面”	152
7.3	“任务栏”和“开始”安全设置	153
7.3.1	禁止“注销”和“关机” 	153
7.3.2	给“开始”菜单减肥 	153
7.3.3	保护“任务栏”和“开始”菜单的设置 	154
7.3.4	利用组策略保护个人文档隐私 	154
7.4	IE 安全设置	154
7.4.1	禁用“在新窗口中打开”菜单项 	154
7.4.2	限制使用 IE 浏览器的保存功能 	155
7.4.3	禁用“Internet 选项”控制面板 	156
7.4.4	给工具栏减肥 	156
7.4.5	禁止修改 IE 浏览器的主页 	157
7.4.6	自定义 IE 工具栏 	157
7.5	用策略增强系统安全防护	158
7.5.1	隐藏“我的电脑”中指定的驱动器	158
7.5.2	防止从“我的电脑”访问驱动器 	159
7.5.3	禁止使用命令提示符 	159
7.5.4	禁止更改显示属性 	160
7.5.5	禁用注册表编辑器 	160
7.5.6	禁止访问“控制面板” 	161
7.5.7	禁止建立新的拨号连接 	161
7.5.8	禁用“添加/删除程序” 	161
7.5.9	限制使用应用程序 	162
7.6	网络与网络安全管理	162
7.6.1	启用“事件日志记录级别”	162
7.6.2	禁用 TCP/IP 高级设置	163
7.6.3	自定义 URL	163
7.6.4	禁止使用 DNS 域网络中的 Internet 连接共享	164
7.6.5	Authenticode 安全设置	164
7.6.6	安全区域和内容的分级管理	165
7.6.7	禁止在 DNS 域网络上使用 Internet 连接防火墙	166
7.6.8	禁止用户更改局域网中的连接属性	166
7.6.9	删除所有用户远程访问连接	166
7.6.10	禁止添加/删除局域网连接或远程访问连接的网络组件	166

第 8 章 系统维护宝鉴	168
8.1 预防死机与突然断电	168
8.1.1 预防死机	168
8.1.2 预防断电	172
8.2 系统蓝屏的原因及解决办法	172
8.2.1 Windows 98 蓝屏怎么办	172
8.2.2 排除 Windows 2000 蓝屏故障	174
8.2.3 排除 Windows XP 蓝屏故障	177
8.3 Windows 优化大师全能维护	178
8.3.1 用 Windows 优化大师系统检测	178
8.3.2 用 Windows 优化大师优化系统	180
8.3.3 用 Windows 优化大师清理维护	187

第 2 篇 网络安全篇

第 9 章 安全漏洞与端口检查	195
9.1 安全漏洞概述	195
9.1.1 安全漏洞的产生	195
9.1.2 安全漏洞的分类	195
9.1.3 漏洞等级评定	197
9.2 系统网络服务检查	197
9.2.1 系统网络服务解析	197
9.2.2 禁止不安全的网络服务	202
9.3 服务端口检查	207
9.3.1 计算机端口概述	207
9.3.2 监视计算机端口	208
9.3.3 在线检测计算机端口	209
9.4 系统安全漏洞扫描	213
9.4.1 使用 SSS 软件检测安全漏洞	213
9.4.2 使用 MBSA 检查计算机系统安全	216
9.4.3 使用 NMap 扫描系统安全漏洞	219
第 10 章 反黑客实战	224
10.1 黑客常用攻击手段及防御	224
10.1.1 黑客攻击网络的一般过程	224
10.1.2 协议欺骗攻击及其防范措施	225
10.1.3 拒绝服务攻击及预防措施	226
10.1.4 其他网络攻击行为的防范措施	226
10.2 扫描程序的防御	228
10.2.1 扫描程序的工作方式	228

10.2.2	常见扫描程序介绍	229
10.2.3	针对扫描程序的防御方法	230
10.3	口令攻击程序的防御	230
10.3.1	口令攻击原理	230
10.3.2	常见口令攻击程序	231
10.3.3	口令攻击的防御	232
10.4	嗅探器的防御	234
10.4.1	嗅探器的攻击原理	234
10.4.2	怎样发现嗅探器	235
10.4.3	常见嗅探器简介	236
10.4.4	防御嗅探器的攻击	236
第 11 章	网络游戏安全	239
11.1	网络游戏安全概述	239
11.2	使用“盛大密宝”保护网络游戏	240
11.2.1	启用密宝	241
11.2.2	绑定密宝	242
11.2.3	开通游戏应用	242
11.2.4	登录游戏	242
11.2.5	密宝挂失/更换	243
11.3	使用网易将军令保护网络游戏	245
11.3.1	启用“将军令”	246
11.3.2	绑定“将军令”	247
11.3.3	“将军令”挂失	248
11.3.4	“将军令”停用/更换	248
11.4	使用游戏之星网游防盗号卡保护网络游戏	249
11.4.1	绑定当前卡	250
11.4.2	绑定备用卡	251
11.4.3	备用卡转当前卡	252
11.4.4	登录游戏	253
11.5	使用密码保护卡保护魔兽世界	254
11.5.1	账号绑定	254
11.5.2	服务开通	255
11.5.3	登录游戏	256
11.5.4	更换密保卡	257
第 12 章	网页浏览安全	258
12.1	网页浏览安全概述	258
12.1.1	网络广告	258
12.1.2	恶意网站	259
12.1.3	网络偷窥	260

12.2	浏览器安全防范	261
12.2.1	IE 选项安全设置	261
12.2.2	Cookies 问题	263
12.2.3	浏览器设置	264
12.2.4	网页脚本	267
12.2.5	使用第三方浏览器	268
12.3	浏览器修复	272
12.3.1	修复首页更改	272
12.3.2	修复标题栏更改	273
12.3.3	修复工具栏	274
12.3.4	修复右键快捷菜单	275
第 13 章	网络邮件安全	276
13.1	电子邮件的安全问题	276
13.1.1	申请免费电子信箱	276
13.1.2	申请电子信箱的不安全因素	277
13.1.3	收发电子邮件	279
13.1.4	密码和账户	282
13.1.5	垃圾邮件	284
13.1.6	邮件病毒	285
13.2	Web 邮件的安全设置	286
13.2.1	反垃圾邮件设置	286
13.2.2	反病毒设置	288
13.3	Outlook Express 的安全设置	288
13.3.1	Outlook Express 账户设置	288
13.3.2	使用 Outlook Express 收发邮件	291
13.3.3	用 Outlook Express 发送加密电子邮件	292
13.3.4	Outlook Express 安全性设定	299
13.3.5	将垃圾邮件拒之门外	300
13.3.6	给 Outlook Express 加锁	301
13.4	Foxmail 的安全设置	302
13.4.1	设置 Foxmail 中的账号口令	302
13.4.2	在 Foxmail 中设置垃圾邮件过滤	304
13.4.3	清除遗忘的密码	308
13.4.4	防范 Foxmail 账户被破解	309
第 14 章	网络聊天安全	310
14.1	保护 QQ 密码	310
14.1.1	QQ 密码保护	310
14.1.2	设置安全的 QQ 密码	312
14.1.3	删除 QQ 登录号码	313

14.2	防范 IP 地址被探测	314
14.3	防范 QQ 木马程序及病毒	315
14.3.1	防范 QQ 木马的一般措施	316
14.3.2	防范 QQ 连发器	317
14.3.3	防范 GOP 木马盗号	318
14.3.4	防范 QQ 狩猎者	320
14.3.5	QQ 女友 Worm.LovGate.v.QQ	322
14.3.6	QQ 代码炸弹	323
14.3.7	QQ 尾巴病毒	323
14.3.8	QQ 恶意代码专杀	324
14.4	MSN Messenger 安全防范	325
14.4.1	如何安全使用 MSN	325
14.4.2	如何防护 MSN 病毒	327
14.4.3	即时了解 MSN 最新更新信息	328
第 15 章	网络购物安全	329
15.1	网络购物概述	329
15.2	网络购物的一般流程	329
15.2.1	注册网站用户	329
15.2.2	注册网上银行	330
15.2.3	在线购物	332
15.2.4	在线支付	333
15.2.5	收取货物	333
15.3	网上购物的安全隐患	333
15.3.1	虚假信息	333
15.3.2	支付安全	334
15.3.3	钓鱼式陷阱	334
15.4	安全交易措施	335
15.4.1	详细了解商品	335
15.4.2	了解商家信誉	335
15.4.3	货到付款	336
15.4.4	维护正当利益	336
15.5	选择安全的支付手段	336
15.5.1	工商银行安全支付	336
15.5.2	招商银行安全支付	337
15.5.3	建设银行安全支付	338
15.5.4	农业银行安全支付	339
15.6	网上个人信息的保密	339
15.6.1	设置 IE 防止 Cookie 泄露个人资料	339
15.6.2	修改注册表防止 Cookie 泄露个人资料	340

15.6.3 使用 KV2006 保护网络隐私	340
15.7 用户账号、密码的保密和保管	342
15.7.1 删除保存用户上网登录账号和密码的临时文件	342
15.7.2 使用修改文件名的方法保护密码	343

第 3 篇 数据安全篇

第 16 章 文件、隐私保护	347
16.1 清除系统操作痕迹	347
16.1.1 清除文档操作痕迹	347
16.1.2 清除程序运行痕迹	348
16.1.3 清除网络浏览痕迹	350
16.1.4 利用工具软件清除系统的操作痕迹	352
16.2 加密解密文件与文件夹	353
16.2.1 用类标识符加密文件夹	353
16.2.2 使用 NTFS 特性加密	357
16.2.3 导出与保存加密证书	359
16.2.4 使用 E-钻文件夹加密大师加密文件夹	361
16.3 隐藏驱动器	361
16.3.1 修改注册表隐藏驱动器	361
16.3.2 修改组策略隐藏驱动器	362
16.3.3 使用软件隐藏驱动器	363
16.4 文件隐身术	363
16.4.1 用 Txt2bmp 隐藏文本到图片中	363
16.4.2 用 Txt2bmp 从图像中分离文本	364
16.4.3 用“超级文件隐形家”隐藏或恢复文件	364
16.4.4 用“超级文件隐形家”伪装文件目录	364
16.4.5 使用“文件夹隐藏大师”保护个人隐私	365
第 17 章 电子文档安全	368
17.1 Word 文档安全	368
17.1.1 隐藏文档记录	368
17.1.2 躲开他人视线	369
17.1.3 给文档设置密码	369
17.1.4 加密后的小措施	370
17.1.5 保护文档	371
17.1.6 设置文档的局部保护功能	372
17.1.7 突发事件下的文档保护	372
17.1.8 宏病毒的防范	373
17.2 Excel 电子表格安全	373