软硬兼施
电脑丛书

精通

电脑安全防护技巧600招

◆ 张发凌 陶龙明 水一舟 编著

人民邮电出版社
POSTS & TELECOM PRESS

软硬兼施
电脑丛书

精通

电脑安全防护技巧600招

◆ 张发凌 陶龙明 水一舟 编著

人民邮电出版社

图书在版编目（CIP）数据

精通电脑安全防护技巧600招 / 张发凌等编著. —北京：人民邮电出版社，2005.10
（软硬兼施电脑丛书）

ISBN 7-115-13181-3

Ⅰ. 精… Ⅱ. 张… Ⅲ. 电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆CIP数据核字（2005）第115485号

内 容 提 要

本书以电脑安全防护为主题，从系统设置到网络安全，从数据备份到数据恢复，从安全策略到安全误区，介绍了电脑安全方面的600余招应用技巧。全书共分为11章，第1、2章主要介绍增强系统的安全性、系统安全限制和隐私保护等内容；第3章介绍办公文档与文件夹安全防护等内容；第4章介绍病毒、木马查杀和预防等内容；第5、6、7、8章主要介绍网络应用中的安全防护，如Internet安全设置、电子邮件安全设置、即时聊天工具安全设置和防火墙设置等内容；第9章介绍系统、数据备份和还原等内容；第10章介绍系统、数据安全修复；第11章介绍安全管理与安全误区。

本书条理清晰，采用图文并茂的方式进行讲解。通过本书的学习，读者可以掌握大量电脑安全应用技巧，从而让电脑工作在安全状态之下。本书适合于初中级电脑爱好者阅读。

软硬兼施电脑丛书

精通电脑安全防护技巧600招

◆ 编　　著　张发凌　陶龙明　水一舟
责任编辑　马雪伶

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：18.75
字数：445千字　　2005年10月第1版
印数：1－6 000册　　2005年10月北京第1次印刷

ISBN 7-115-13181-3/TP・4511

定价：26.00元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前　言

“我的电脑中毒了”、“我的 QQ 被盗了”、“我收到了好多垃圾邮件”、“我的系统瘫痪了”……这些都是大家在使用电脑时会遇到的问题，电脑安全问题成为每个电脑用户越来越关心的问题。

一些初级电脑用户可能认为只要经常查杀病毒就可以确保电脑安全了，其实“电脑安全”不只是查杀电脑病毒，它还包括增强系统安全性、保护个人隐私及文档的安全等内容。本书对这些内容均做了介绍，例如“揪出隐藏的超级用户”（第 22 招）、“使用在线扫描发现系统漏洞”（第 26 招）、“禁止使用注册表编辑器”（第 78 招）、“清除网吧上网信息”（第 120 招）、“设置 Word 文档的编辑权限”（第 141 招）、“关闭蠕虫病毒可利用的 135 端口”（第 398 招）、“封杀木马发送邮件的 25 端口”（第 404 招）、“阻止黑客和病毒对系统服务端口的扫描”（第 406 招）、“利用防火墙防止别人用 Ping 命令探测”（第 416 招）……

针对读者对电脑安全认识不全面、安全防护无从下手的情况，我们编写了本书。本书从安全管理的一般原则出发，从系统设置到网络安全，从数据备份到数据恢复，从安全策略到安全误区，把安全应用的方方面面落实到一招一式，招招实用，可以全面提高读者的电脑安全应用水平，规范电脑安全管理。

本书由张发凌策划，张发凌、陶龙明、水一舟编写。吴祖珍、管文蔚、王丽莉、马立涛、郭本兵、邓建钟、刘芳等人参加了书稿的校对及整理工作，在此对他们表示深深的谢意！

由于作者水平有限，书中难免存在一些疏漏，望读者不吝赐教。在阅读本书的过程中，读者如果遇到问题，或者有什么意见和建议，可以和我们联系，我们的联系方式：maxueling@ptpress.com.cn 或 witren@sohu.com。

编　者

2005 年 10 月

目　录

第 1 章　增强系统安全性 ····· 1

1.1　系统登录与退出安全设置 ····· 1

第 1 招：通过 BIOS 设置开机密码 ····· 1

第 2 招：让 Windows 98 必须输入密码才能登录 ····· 1

第 3 招：禁止将网络登录密码保存在 PWL 文件中 ····· 1

第 4 招：禁止系统启动时使用 F8 启动功能键 ····· 2

第 5 招：让系统开机即运行屏保程序 ····· 2

第 6 招：为系统设置强健的登录密码 ····· 2

第 7 招：设置超强的 Windows XP 启动密码 ····· 3

第 8 招：让 Windows XP 系统需要“密匙盘”才能登录 ····· 3

第 9 招：禁止从软盘和 CD-ROM 启动系统 ····· 4

第 10 招：设置组策略加强系统密码安全 ····· 4

第 11 招：设置组策略启用账户锁定策略 ····· 5

第 12 招：设置组策略不处理只运行一次列表 ··· 6

第 13 招：用批处理文件在每次启动时删除默认共享 ····· 6

第 14 招：从休眠/挂起恢复时提示输入密码 ·· 7

第 15 招：让系统登录时不显示上次登录的用户名 ····· 7

第 16 招：将 Administrator 账号改名 ····· 7

第 17 招：禁用来宾账户 ····· 8

第 18 招：安装 Windows XP 时务必给管理员设置密码 ····· 8

第 19 招：创建另一个拥有管理员权限的账户 ····· 8

第 20 招：不以管理员的身份来运行程序 ···· 10

第 21 招：注意系统账号的增减 ····· 10

第 22 招：揪出隐藏的超级用户 ····· 10

第 23 招：当用户离开时快速锁定桌面 ····· 11

第 24 招：退出时自动清除页面文件 ····· 11

1.2　系统漏洞扫描与补丁升级 ····· 12

第 25 招：使用扫描器检查系统漏洞 ····· 12

第 26 招：使用在线扫描发现系统漏洞 ····· 13

第 27 招：使用共享扫描工具扫描开放共享 ·· 13

第 28 招：微软安全检测工具 MBSA 的妙用 ·· 14

第 29 招：使用 Hot Fix 让系统安全更无忧 ·· 16

第 30 招：瑞星系统漏洞扫描工具使用技巧 ···· 16

第 31 招：金山毒霸漏洞扫描工具使用技巧 ····· 16

第 32 招：让系统一开始就获得最新的免疫力 ····· 17

第 33 招：Windows 98 上网升级安全补丁 ·· 17

第 34 招：给 Windows 98 安装 IE 6.0 最新版以保护个人隐私 ····· 19

第 35 招：给 Windows 2000 安装 SP4 补丁 ··· 19

第 36 招：给 Windows XP 安装 SP2 补丁 ·· 19

第 37 招：Windows XP 手动上网升级补丁 ···· 20

第 38 招：开启自动升级功能 ····· 22

第 39 招：从“添加或删除程序”中查看自动更新情况 ····· 22

第 40 招：下载安装 ADODB.Stream 漏洞防范工具 ····· 22

第 41 招：下载安装 CIH 免疫程序 ····· 23

第 42 招：下载安装 Funlove 病毒免疫程序 ····· 23

第 43 招：下载安装欢乐时光 Happytime 免疫程序 ····· 24

第 44 招：下载安装冲击波/震荡波疫苗程序 ··· 24

第 45 招：下载安装 JPEG 文件漏洞的防毒疫苗 ····· 25

1.3　Windows XP SP2 新安全设置 ····· 25

第 46 招：启用 Windows XP SP2 防火墙 ··· 25

第 47 招：添加安全的例外程序通过防火墙 ···· 25

第 48 招：限制例外程序仅适用于内网 ····· 26

第49招：在命令行下收集防火墙配置信息…26
第50招：管理Internet加载项……27
第51招：设置IE阻止弹出窗口……27
第52招：阻止来自特定发布者的下载内容…28
第53招：发现可能有破坏性的下载文件……28
第54招：手动配置数据执行保护 ……29
第55招：使用Boot.ini停用整个系统的DEP…30
第56招：限制窗口覆盖屏幕 ……30
第57招：启用Windows防火墙的IPSec验证允许来自指定系统的主动传入消息……30
第58招：启用防火墙保护所有网络连接…31
第59招：指定Windows防火墙阻止所有未经请求的传入消息……31
第60招：限制Internet通信……32
第61招：定制Windows可访问Internet的项目……32
第62招：对“脱机文件”缓存进行加密…33
第63招：抵御可疑的电子邮件附件……33
第64招：解决OE无法下载图片问题 ……33
第65招：解决无法设置Cookie的问题 ……34
第66招：解决安全中心找不到杀毒软件问题……34
第67招：解决网站验证码无法正常显示问题……34
第68招：解决降低IE安全级别报错问题……35
第69招：解决IE不允许安装使用无效签名的对象问题 ……35
第70招：解决一些应用程序无法在SP2中运行问题 ……35
第71招：解决下载文件时以纯文本方式打开问题 ……36
第72招：取消SP2安全中心的提示窗口 …36

第2章 系统安全限制与隐私保护……37

2.1 系统安全限制……37
第73招：禁止更改桌面设置 ……37
第74招：禁止用户利用“注销”功能来切换登录用户名 ……38
第75招：禁止使用“网上邻居”访问共享资源……39
第76招：禁用“添加/删除程序”操作…… 39
第77招：防止用户从可移动媒体安装程序……40
第78招：禁止使用注册表编辑器…… 40
第79招：禁止远程编辑注册表…… 41
第80招：禁止用户使用.reg文件…… 41
第81招：禁止查看指定磁盘驱动器的内容……41
第82招：防止用户在计划任务文件夹中添加删除任务 …… 41
第83招：禁止改变计划任务属性…… 42
第84招：禁止手动控制计划任务…… 42
第85招：禁止运行指定的程序…… 42
第86招：禁用“开始→运行”菜单…… 42
第87招：锁定“我的文档” …… 42
第88招：锁定“我的电脑” …… 43
第89招：禁止控制面板中的所有设置项目…43
第90招：禁止使用INF脚本文件 …… 43
第91招：禁止使用LanMan Hash…… 44
第92招：禁止打印机共享 …… 44
第93招：禁止加载登录屏幕保护程序…… 44
第94招：禁止改变“启动”菜单…… 44
第95招：禁止非法用户访问远程桌面…… 44
第96招：禁止他人通过拨号访问自己的计算机 …… 45

2.2 系统隐私保护…… 45
第97招：清除“我最近的文档”记录…… 45
第98招：清除“运行”记录 …… 45
第99招：清除“查找”记录 …… 45
第100招：清除计划任务记录…… 46
第101招：清除Temp文件夹记录…… 46
第102招：清除剪贴板内容 …… 46
第103招：清除回收站中的内容…… 47
第104招：清除Word记录…… 47
第105招：清除Excel记录 …… 47
第106招：清除WPS记录 …… 47
第107招：清除Office “回收站”记录… 47
第108招：清除非法操作产生的“被挽救的文档”记录…… 48
第109招：清除Windows的日志记录…… 48
第110招：清除防火墙安全日志记录…… 48
第111招：清除FTP连接日志记录 …… 48

第 112 招：清除“写字板”中的记录……49
第 113 招：删除输入法自动记忆的信息……49
第 114 招：清除曾访问的网页 ……49
第 115 招：清除浏览过的地址 ……50
第 116 招：清除 Cookies 文件夹记录……50
第 117 招：清除“收藏夹”记录 ……50
第 118 招：清除 IE 浏览历史记录……51
第 119 招：用脚本和批处理清除计算机中的记录……51
第 120 招：清除网吧上网信息 ……52
第 121 招：清除 QQ 交流记录 ……52
第 122 招：清除 MSN 交流记录……52
第 123 招：清除网易 POPO 交流记录 ……53
第 124 招：清除 YAHOO 交流记录……53
第 125 招：清除网络蚂蚁下载记录列表……54
第 126 招：清除网际快车下载记录列表……54
第 127 招：清除影音传送带下载记录列表…54
第 128 招：清除 WinZip 历史文件夹内容…55
第 129 招：清除 WinZip“文件”菜单中的历史文件……55
第 130 招：清除 WinRAR 访问的历史记录…55
第 131 招：清除 Windows Media Player 播放记录……55
第 132 招：清除 Real Player 文件记录……56
第 133 招：让 ACDSee 自动清除历史记录……56

第 3 章　办公文档与文件夹安全……57

3.1　Office 文档安全设置……57
第 134 招：防止他人偷窥文档内容 ……57
第 135 招：防止文档信息暴露隐私 ……57
第 136 招：设置文档保护……58
第 137 招：禁止多用户同时编辑 Word 文档…58
第 138 招：设置格式限制……58
第 139 招：设置窗体保护……59
第 140 招：保护文档的局部内容 ……59
第 141 招：设置 Word 文档的编辑权限……59
第 142 招：防范宏病毒……60
第 143 招：保存文档的同时保留备份……60
第 144 招：防止突发事件导致文档丢失……61
第 145 招：利用密码保护 Word 文档……61
第 146 招：利用密码保护工作表……61
第 147 招：利用密码保护工作簿……62
第 148 招：设置 Excel 表格特定的区域为可编辑区域 ……62
第 149 招：隐藏 Excel 工作表中重要的数据部分 ……63
第 150 招：隐藏重要的行、列数据……63
第 151 招：利用密码保护 Access 数据库…63
第 152 招：设置用户编辑数据库的权限 …64
第 153 招：将 Outlook 的通讯记录保存起来 ……64
第 154 招：强制 Outlook 以纯文本方式读邮件 ……64
第 155 招：自动删除含特定名称的病毒 …64

3.2　文件、文件夹安全设置……65
第 156 招：使用“编辑文件夹的 HTML 模板”加密文件夹……65
第 157 招：将 FAT32 文件系统转换为 NTFS 文件系统……66
第 158 招：将文件夹设为专用文件夹……66
第 159 招：让 Windows XP NTFS 分区也显示安全标签……67
第 160 招：共享驱动器或文件夹的安全设置 ……67
第 161 招：将重要文件隐藏起来……67
第 162 招：让其他用户看不到系统文件 …68
第 163 招：让系统文件彻底不显示……68
第 164 招：隐藏文件的扩展名……68
第 165 招：修改文件的扩展名……68
第 166 招：隐藏重要文件的创建日期……69
第 167 招：将文件夹图标改变系统图标 …69
第 168 招：利用 NTFS 文件系统来加密文件 ……69
第 169 招：利用 Desktop.ini 文件来加密文件 ……69
第 170 招：在 DOS 下利用 COPY 命令来合并隐藏文件……70
第 171 招：利用 WinZIP 来加密文件 ……70
第 172 招：利用文件加密机（ABI-Coder）来加密文件 ……70

第173招：对文件进行伪装加密（Hide In Picture）……71
第174招：对图像文件进行加密（PhotoEncrypt）……72
第175招：禁止修改文件属性……72
第176招：用更为安全的方法来共享文件夹……72
第177招：在Windows XP中设置共享文件夹的访问权限……72
第178招：在Windows 98中设置共享文件夹的密码……73
第179招：隐藏Windows XP中的“共享文档”……73
第180招：利用类标识符“隐藏”文件夹…73
第181招：Cookie数据记录的安全管理…74
第182招：利用“文件签名策略”来保护数据安全……75
第183招：设置Control.ini文件来保护系统……75
第184招：防范几个危险文件……76
第4章 病毒、木马查杀和预防……77
4.1 病毒查杀和预防……77
第185招：防范病毒的常识……77
第186招：判断电脑是否感染了病毒……77
第187招：利用BIOS设置防毒……77
第188招：根据进程名查杀病毒……78
第189招：根据进程号查杀病毒……78
第190招：防毒十二策……79
第191招：防止ActiveX控件绕过IE……79
第192招：图片病毒的防范……80
第193招：两招彻底杜绝JPEG图片病毒……80
第194招：ActiveX漏洞防范方法……80
第195招：利用批处理文件防范病毒……80
第196招：快速查杀计算机病毒……81
第197招：用抓包工具揪出电脑病毒……81
第198招：设置注册表权限防病毒启动……81
第199招：防范移动存储设备传播病毒……82
第200招：碰上最新病毒怎么办……82
第201招：因病毒破坏而无法启动Windows时怎么办……82
第202招：禁止信使服务以防骚扰……83
第203招：彻底清除主引导区病毒……83
第204招：防御脚本病毒……84
第205招：防止病毒发作后的自动复制…84
第206招：防止病毒发作后利用CDO传播…84
第207招：防止病毒发作后利用OOM传播……85
第208招：防止SYN洪水攻击……85
第209招：防止网页脚本病毒执行……86
第210招：防止Word文档的宏病毒……86
第211招：防止ICMP重定向报文的攻击…86
第212招：利用专杀工具查杀病毒……87
第213招：巧用Windows 系统控制台删除病毒文件……87
第214招：让病毒自动还原被恶意修改键值……88
第215招：使用在线病毒检测……89
4.2 木马查杀和预防……89
第216招：利用进程标识符查杀木马……89
第217招：搜查木马藏身之地……90
第218招：查看系统中是否有简单木马…90
第219招：搜查隐藏在注册表非启动项下的木马……91
第220招：搜查“组策略”中的木马……91
第221招：怎样彻底查杀Trojan.SyncroAd.d木马……91
第222招：用Longhorn的“任务管理器”查找木马……92
第223招：防范利用Word文档执行木马…92
第224招：防范传奇木马……92
第225招：禁止硬盘AutoRun功能预防木马运行……93
第226招：防范恶意碎片文件引起的攻击…93
第227招：查杀反弹端口型木马……93
第228招：防范反弹端口型木马……94
第229招：巧妙分离带木马文件……94
第230招：防止利用TTL值来鉴别操作系统类型……95
第231招：手工清除嵌入式DLL木马……95

第 232 招：防范 PHP 木马攻击……95
第 233 招：防范利用 Guest 账户的入侵 ……96
第 234 招：防范利用 Windows 2000 输入法漏洞入侵 ……96
第 235 招：快速查杀木马技巧 ……97
第 236 招：微软反间谍软件应用技巧……97
第 237 招：利用 Windows 命令检查电脑是否感染木马 ……98

第 5 章　Internet 安全设置与策略……99

5.1　Internet 安全设置……99
第 238 招：禁止使用“Internet 选项”对话框……99
第 239 招：快速查看网页是否安全 ……99
第 240 招：设置 Cookie 访问权限……99
第 241 招：禁用或限制使用 Java 程序及 ActiveX 控件……100
第 242 招：防止上网浏览时所填写的信息被泄露……100
第 243 招：让 IE 自动清除浏览记录……100
第 244 招：隐藏 IE 地址栏 ……101
第 245 招：锁定 IE 工具栏来限制其他用户随意添加按钮 ……101
第 246 招：禁止在 IE 中使用“文件→另存为”命令……102
第 247 招：禁止在浏览时查看网页源文件…102
第 248 招：启动分级审查功能来限制浏览…102
第 249 招：解除 IE 的分级审查口令……102
第 250 招：禁止 IE 自动安装不安全组件……103
第 251 招：禁止 IE 访问某些站点……103
第 252 招：禁止用户更改添加到安全站点中的网站……103
第 253 招：禁止用户更改安全级别 ……104
第 254 招：禁止 IE 下载文件功能……105
第 255 招：启用 IE 对 Windows 安装脚本的安全提示……105
第 256 招：禁用缓存自动代理脚本 ……105
第 257 招：在 IE 中禁止使用鼠标右键……105
第 258 招：禁止 IE 自动播放动画……106
第 259 招：禁止导入或导出收藏夹链接…106
第 260 招：禁止更改浏览器主页…… 106
第 261 招：取消 IE 自动保存密码功能 …… 106
第 262 招：禁止更改 IE 代理服务器设置…… 107
第 263 招：禁止更改邮件发送程序…… 107
第 264 招：禁止更改临时文件的设置…… 107
第 265 招：禁止更改分级审查设置…… 107
第 266 招：禁用“重置 Web 设置”功能…… 107
第 267 招：禁用编辑和创建计划组…… 108
第 268 招：禁止用户使用标识…… 108
第 269 招：禁用“常规”选项卡…… 108
第 270 招：禁用“安全”选项卡…… 109
第 271 招：禁用“内容”选项卡…… 109
第 272 招：禁用“程序”选项卡…… 109
第 273 招：禁用“高级”选项卡…… 109
第 274 招：禁用“连接”选项卡…… 109
第 275 招：禁止缓存自动带理脚本…… 109
第 276 招：在安全和非安全模式之间切换时发出警告 ……110
第 277 招：解除网页文字无法复制……110
5.2　Internet 安全策略……110
第 278 招：在线交易操作需反复确认……110
第 279 招：网络钓鱼攻击的防范……111
第 280 招：上网浏览时使用代理服务器…111
第 281 招：巧输密码防止被盗……111
第 282 招：网吧上网后的清理工作……112
第 283 招：识破假冒网上银行技巧……112

第 6 章　电子邮件安全设置…… 113

6.1　Outlook Express 6.0……113
第 284 招：自动谢绝垃圾邮件……113
第 285 招：自动谢绝邮件炸弹……113
第 286 招：禁止其他程序暗中发送邮件…114
第 287 招：启动 Outlook Express 的自防毒选项……114
第 288 招：对邮件进行加密和签名保护…114
第 289 招：利用数字标识强化信息安全…115
第 290 招：保护私人的 Outlook Express 收件箱……116
第 291 招：让 Outlook Express 自动清理垃圾邮件 ……117

第 292 招：不让 Outlook Express 记住账户口令……117
第 293 招：隐藏邮件来保护邮件的安全性…117
第 294 招：让发送的邮件只为纯文本格式…118
第 295 招：将邮件存放文件夹移到安全的目录中……118
6.2 Microsoft Office Outlook 2003……119
第 296 招：为 Office Outlook 2003 设置密码保护……119
第 297 招：自动删除含特定名称的病毒…119
第 298 招：自动删除符合过滤条件的垃圾邮件……120
第 299 招：使用规则过滤未知来源邮件…120
第 300 招：禁用 Outlook 的邮件自动预览功能……120
第 301 招：取消自动记忆邮箱口令 ……121
第 302 招：让 Outlook 只接收安全收件人的邮件……122
第 303 招：巧妙收取安全的.exe 附件 ……122
第 304 招：让 Outlook 自动分拣邮件 ……122
第 305 招：为重要邮件设置自动标记功能…123
第 306 招：在回复邮件时不包含邮件原件…123
第 307 招：有选择地发送和接收邮件……124
第 308 招：自动删除已发送的邮件 ……124
第 309 招：更改电子邮件和附件至安全保存位置……125
第 310 招：安全阅读电子邮件 ……126
第 311 招：防止 Outlook 自动将病毒邮件寄出……126
第 312 招：删除不安全的附件 ……126
第 313 招：设置 Outlook 中的安全区域…127
第 314 招：安全解除 Outlook 的附件限制…127
6.3 Foxmail 5.0……128
第 315 招：设置个人账户密码保护 ……128
第 316 招：防御 Foxmail 中文域名解析漏洞……128
第 317 招：防止用冒名账号发送邮件……129
第 318 招：单独删除邮件的有害附件……129
第 319 招：以纯文本方式显示可疑的 HTML 邮件……130
第 320 招：消除 Foxmail 地址自动记忆能力 …… 130
第 321 招：禁止 Foxmail 日志文件再次记录操作信息 …… 131
第 322 招：遗忘账户密码怎么办…… 131
第 323 招：恢复误删除的 Foxmail 邮件… 131
第 324 招：将恶意邮件发送人添加到黑名单中 …… 132
第 325 招：防御地址簿信息泄露…… 132
第 326 招：为接收的不同用户邮件分别打上不同标记 …… 133
第 327 招：让 Foxmail 自动过滤垃圾邮件 133
第 328 招：将邮件账户存储到安全的盘符中 …… 134
第 329 招：加密 Foxmail 文件夹防止其他用户修改 …… 134
第 330 招：在接收邮件之前将垃圾邮件清理 …… 135
第 331 招：安全地将发件人添加到地址簿中 136
第 332 招：退出 Foxmail 时自动清理废件箱 …… 136
第 333 招：给电子邮件进行加密和签名保护 …… 136
第 7 章 即时聊天工具安全设置 …… 138
7.1 QQ……138
第 334 招：隐身登录 QQ …… 138
第 335 招：拒绝陌生人发来的消息…… 138
第 336 招：清除 QQ 登录窗口中的 QQ 号码列表 …… 139
第 337 招：将接收的文件保存在特定文件夹中 …… 139
第 338 招：通过问题提示过滤陌生人的消息 …… 139
第 339 招：巧妙避开木马对 QQ 密码的监视 …… 140
第 340 招：防止他人登录 QQ…… 140
第 341 招：使用代理服务器避免暴露真实 IP 地址…… 140
第 342 招：使用错位输入防止木马记录正

确密码……141
第 343 招：使用中文密码防木马盗号……141
第 344 招：给 QQ 再加一道本地密码保护…142
第 345 招：将 QQ 彻底隐藏 ……142
第 346 招：使用 QQ 病毒专杀工具……142
第 347 招：在线查杀 QQ 病毒 ……142
第 348 招：网吧上网后清理 QQ 登录记录…143
第 349 招：隐藏自己的摄像头 ……144
第 350 招：在 Windows XP 中拒绝接收 QQ 广告……144
第 351 招：清除“QQ 尾巴”病毒……145
第 352 招：清除 QQ“缘”病毒……145
第 353 招：清除“武汉男生”病毒 ……145
第 354 招：清除“QQ 女友”病毒……146
第 355 招：清除“QQ 狩猎者”病毒……146
第 356 招：清除“爱情森林”病毒 ……147
第 357 招：妙招应对“飘叶 OICQ 千夫指”…148
第 358 招：谨防 QQ 骗术 ……148
第 359 招：从源头杜绝木马 ……149
7.2 MSN……151
第 360 招：撤销 MSN 自动登录……151
第 361 招：防止聊天记录曝光 ……151
第 362 招：让杀毒软件自动扫描接收文件…152
第 363 招：阻止不受欢迎的客人 ……153
第 364 招：防止邮件内容曝光 ……153
第 365 招：禁止将 MSN 联系人名单存储在共享计算机上 ……154
第 366 招：防止他人未经授权访问个人信息……154
第 367 招：认识和清除“MSN 密码窃贼”……154
第 368 招：认识和清除“MSN 小尾巴” ….155
第 369 招：清除“MSN 性感鸡”（MSN.DropBot.b）……155
7.3 其他即时聊天工具…… 156
第 370 招：让网易 POPO 拒绝陌生人消息…156
第 371 招：设定权限避免被干扰 ……156
第 372 招：为共享文件夹设置访问密码…156
第 373 招：让网易 POPO 获取密码保护…157
第 374 招：ICQ 账号等私人信息的防盗措施…… 157
第 375 招：堵住 ICQ 中的“后门” …… 158
第 376 招：忽略特定用户发来的消息…… 158
第 377 招：控制垃圾邮件 …… 159
第 378 招：新浪 UC 安全设置 …… 159
第 379 招：申请新浪 UC 密码保护 …… 160
第 380 招：在 UC 中防止垃圾邮件 …… 161
第 381 招：在雅虎通设置屏蔽某人发来的消息…… 161
第 382 招：自动查杀接收到的文件…… 161
第 8 章　黑客安全与防火墙设置 …… 162
8.1 端口与服务安全设置……162
第 383 招：利用 netstat 命令查看本机开放端口 …… 162
第 384 招：找出打开可疑端口的恶意程序… 162
第 385 招：在 Windows XP 中用 netstat 命令直接查看端口与程序…… 163
第 386 招：利用 Fport 查看开放端口对应的程序 …… 163
第 387 招：用 Active Ports 查看本级活动端口和连接 …… 163
第 388 招：简单屏蔽 Windows XP 的 3389 端口 …… 164
第 389 招：修改 Windows XP 的远程管理默认端口 …… 164
第 390 招：停用系统远程终端服务…… 166
第 391 招：用 Port Reporter 全程跟踪端口活动状态 …… 166
第 392 招：设置地址转换保护上网安全…167
第 393 招：改变 FTP 服务器默认端口 …… 167
第 394 招：禁用不必要的服务…… 168
第 395 招：一次性关闭 137、138、139 和 445 端口 …… 169
第 396 招：关闭 1900 端口 …… 169
第 397 招：关闭蠕虫病毒可利用的 123 端口 …… 170
第 398 招：关闭蠕虫病毒可利用的 135 端口 …… 170
第 399 招：关闭可被病毒利用的 445 端口…170

第400招：关闭系统的文件共享服务的139端口……171
第401招：简单更改Windows 2000的Telnet端口……171
第402招：用批处理查看开放端口和对应的进程……171
第403招：防范利用4899端口远程控制……172
第404招：封杀木马发送邮件的25端口……172
第405招：应用TCP/IP端口筛选管理开放端口……172
第406招：阻止黑客和病毒对系统服务端口的扫描……173
第407招：使用端口碰撞技术让开放端口更安全……173
第408招：禁止远程协助……174
第409招：关闭Messenger服务……174
第410招：关闭Windows 系统默认的Telnet服务……174
第411招：设置FTP服务器“只允许匿名连接”……175
第412招：关闭Windows 2000/XP系统IIS开启的FTP服务……175
第413招：关闭Windows 2000/XP系统IIS开启的Web服务……176
第414招：关闭Windows 2000/XP系统IIS开启的SMTP服务……176
8.2 黑客入侵与防火墙策略……176
第415招：创建IP策略防Ping命令探测系统……176
第416招：利用防火墙防止别人用Ping命令探测……180
第417招：利用“路由和远程访问”组件防Ping命令探测……180
第418招：应用IP策略反制Telnet登录……181
第419招：捆绑MAC地址防止IP地址被盗……182
第420招：监视MAC地址追踪IP盗贼……182
第421招：设置代理服务器隐藏IP地址……183
第422招：用SocksCap32代理隐身IP……184
第423招：彻底隐藏上网IP……185
第424招：实行网络24小时自动监测……185
第425招：配置注册表防止DDOS攻击……186
第426招：综合应用防范DDOS攻击……186
第427招：访问ADSL防火墙管理页面……187
第428招：设置ADSL Modem防火墙限制连接数目……187
第429招：启用ADSL Modem防火墙攻击防御……188
第430招：设置ADSL Modem防火墙过滤IP地址……188
第431招：用ADSL Modem防火墙黑名单追查攻击者……189
第432招：设置ADSL Modem防火墙自动发送攻击通知……189
第433招：更改ADSL Modem管理密码……189
第434招：更改Web/Telnet管理端口……190
第435招：把攻击映射到不存在的端口……190
第436招：启用ICF使系统获得基本的安全保障……191
第437招：启用ICF阻止IP欺骗……191
第438招：改变ICF常规服务端口躲避攻击……192
第439招：设置ICF允许在特殊需要时Ping本机……192
第440招：启用ICF安全日志保存被攻击的证据……193
第441招：自定义防火墙IP规则……193
第442招：自定义IP规则防范震荡波……194
第443招：自定义规则关闭TCP 139端口……194
第444招：自定义规则开放FTP服务……195
第445招：设置IP规则允许局域网共享……195
第446招：对防火墙进行系统测试……195
第447招：防止渗透防火墙……196
第448招：使用主板上的防火墙……196
第9章 系统、数据备份和还原……197
9.1 系统备份与还原……197
第449招：Windows 98系统文件的备份……197
第450招：Windows XP系统文件的备份……197
第451招：手工备份Windows 98驱动程序……198

第 452 招：手工还原 Windows 98 驱动程序…199
第 453 招：备份 Windows 2000/XP/2003 配置文件……199
第 454 招：还原 Windows 2000/XP/2003 配置文件……199
第 455 招：利用第三方工具备份 Windows 驱动程序……200
第 456 招：利用第三方工具还原 Windows 驱动程序……201
第 457 招：备份和还原系统字体……201
第 458 招：创建 Windows 2000/XP/2003 系统还原点……201
第 459 招：利用系统还原点恢复 Windows 2000/XP/2003 系统……202
第 460 招：进入“安全模式”修复 Windows XP……203
第 461 招：利用 Windows XP 自动系统恢复功能备份系统……203
第 462 招：利用 Windows XP 自动系统恢复功能还原系统……203
第 463 招：安装故障恢复控制台……203
第 464 招：运行故障恢复控制台修复 Windows XP 系统……204
第 465 招：利用 Ghost 备份 Windows 系统…204
第 466 招：利用 Ghost 还原 Windows 系统…206
第 467 招：利用 Ghost 实现硬盘系统相互备份……207
第 468 招：利用 Ghost 9.0 的增量备份让备份文件自动更新……208
第 469 招：用 Power Quest Drive Image 备份系统……209
第 470 招：用 Power Quest Drive Image 还原系统……210
第 471 招：备份和还原 Windows XP 激活文件……211
第 472 招：备份 Windows XP 用户口令…211
第 473 招：备份和还原 Internet 信息服务配置信息……212
9.2　数据备份与还原……212
第 474 招：将“我的文档”文件夹转移到非系统分区……212
第 475 招：使用文件和设置转移向导创建备份……213
第 476 招：使用文件和设置转移向导恢复备份……214
第 477 招：备份和恢复 Word 模板文件…214
第 478 招：让 Word 自动备份文档……215
第 479 招：利用 Office 2003 设置保存向导备份 Office 设置……215
第 480 招：利用 Office 2003 设置保存向导还原 Office 设置……216
第 481 招：利用 Office 2003 应用程序恢复工具恢复文档……216
第 482 招：备份和还原 WPS Office 2003 的自定义设置……217
第 483 招：完全备份 Foxmail……217
第 484 招：备份和还原 Foxmail 账户……217
第 485 招：备份和还原 Foxmail 地址簿…218
第 486 招：备份 Outlook Express 中的邮件…218
第 487 招：备份和还原 Outlook Express 中的通讯簿……218
第 488 招：备份和还原 OE 中的账户……219
第 489 招：备份 OE 中的邮件规则……219
第 490 招：还原 OE 中的邮件规则……219
第 491 招：备份 Outlook 2003 个人目录…220
第 492 招：备份和还原 IE 收藏夹……221
第 493 招：备份和还原输入法自定义词组…221
第 494 招：备份 QQ 聊天记录……221
第 495 招：备份 QQ 好友名单……222
第 496 招：备份 QQ 语音聊天记录……222
第 497 招：备份和还原 Media Player 许可证文件……222
第 498 招：备份和恢复 WinRAR 设置……223
第 499 招：备份硬盘分区表……223
第 500 招：备份 C 盘主引导区信息……224
第 501 招：备份 C 盘系统引导区信息……224
第 502 招：备份 D 盘的主引导区信息……225
第 503 招：备份 D 盘的系统引导区信息……225
9.3　注册表备份与还原……226
第 504 招：什么情况下备份注册表……226

第505招：在DOS下备份Windows 98注册表……226
第506招：在Windows 98系统中备份注册表……227
第507招：在Windows 2000/XP/2003系统中手工备份注册表……227
第508招：利用注册表编辑器备份整个注册表……227
第509招：用第三方“备份”工具备份注册表……228
第510招：在DOS下恢复注册表……228
第511招：在Windows 98系统中恢复注册表……228
第512招：利用系统自带备份工具备份注册表……228
第513招：利用系统自带备份工具还原注册表……229
第514招：利用系统安装光盘恢复注册表…230
第515招：利用紧急修复盘恢复注册表…230

第10章 系统、数据安全修复……231

10.1 系统安全修复……231
第516招：系统文件被病毒感染后的修复…231
第517招：系统文件Ntfs.sys丢失的修复…232
第518招：系统文件NTLDR丢失的修复…233
第519招：Rundll32.exe文件损坏的修复…234
第520招：hal.dll文件丢失的修复……234
第521招：误删除SAM文件的恢复……234
第522招：误删除Boot.ini文件的恢复…235
第523招：nwlink.vxd文件丢失的修复…235
第524招：回收站内文件的恢复……236
第525招：多操作系统启动菜单的修复…237
第526招：多操作系统下的Windows XP无法启动的修复……238
第527招：注册表被恶意代码禁用后的恢复……239
第528招：“运行”功能被恶意代码禁用后的恢复……241

10.2 数据安全修复……242
第529招：Word文档损坏后的修复……242
第530招：Normal.dot模板损坏而导致Word文档损坏的修复……244
第531招：编辑Word文档中被保护的重要区域……244
第532招：忘记Word文件的加密密码后的恢复……245
第533招：忘记Access文件的加密密码后的恢复……246
第534招：编辑Excel中被保护的工作表…246
第535招：EXE文件的打开方式被病毒更改后的修复……247
第536招：RAR和ZIP压缩包损坏的修复…247
第537招：视频文件播放时无法拖动的修复……248
第538招：硬盘数据丢失的修复……249
第539招：误格式化硬盘后数据丢失的修复……250
第540招：在DOS下误删除数据的修复…252
第541招：误删除数码相机照片的修复…253
第542招：病毒破坏数据的修复……254
第543招：硬盘主引导区损坏的修复……254
第544招：硬盘分区表损坏的修复……256
第545招：硬盘0磁道损坏的修复……256
第546招：硬盘坏道的修复……262
第547招：硬盘中了逻辑锁的修复……263
第548招：硬盘碎片过多后的修复……264
第549招：误克隆数据的修复……267
第550招：PM转换分区失败的数据的修复…268
第551招：从光盘操作系统恢复数据……268
第552招：无法读取的光盘数据的修复…268
第553招：无法读取的软盘数据的修复…269

10.3 IE浏览器安全修复……270
第554招：IE首页被恶意代码更改后的修复……270
第555招：IE标题栏被恶意代码更改后的修复……270
第556招：IE默认微软主页被恶意代码更改后的修复……271
第557招：IE搜索引擎被恶意代码更改后的修复……271

第 558 招：Outlook 标题栏被添加非法信息后的修复 ……271
第 559 招：鼠标右键菜单被添加非法网站链接后的修复 ……271
第 560 招：利用 IE 浏览网页时无法使用右键的修复 ……272
第 561 招：IE 地址栏的下拉菜单被禁用后的修复 ……272
第 562 招：系统启动时自动弹出恶意提示窗口的修复 ……272
第 563 招：IE“查看”菜单下的“源文件”项被禁用的修复 ……272
第 564 招：IE 收藏夹被强行添加非法网站的地址链接后的修复 ……273
第 565 招：IE 工具栏中非法添加按钮后的修复 ……273
第 566 招：利用 IE 浏览器打开网站出现乱码后的修复 ……273

第 11 章　安全管理与安全误区 ……274

11.1　安全管理 ……274
第 567 招：选择更安全的操作系统 ……274
第 568 招：对系统进行安全评估 ……274
第 569 招：使用自动下载安装所有重要补丁 ……274
第 570 招：关闭或删除不需要的系统默认设置和服务 ……275
第 571 招：定期检查敏感文件 ……275
第 572 招：尽量从官方网站下载软件 ……275
第 573 招：每天访问安全信息网站 ……276
第 574 招：迅速隔离受感染的计算机 ……276
第 575 招：不到处张贴敏感信息标签 ……276
第 576 招：不轻易在网上泄露个人真实信息 ……277
第 577 招：严防祸从口出 ……277
第 578 招：安装网络防火墙 ……277
第 579 招：科学配置、使用防火墙产品 ……278

11.2　安全误区 ……278
第 580 招：合理设置工具软件减少病毒危害 ……278
第 581 招：计算机在局域网内所以很安全 ……279
第 582 招：拨号上网因无固定 IP 地址，所以很安全 ……279
第 583 招：电脑里没有重要东西不必担心安全问题 ……279
第 584 招：危险总是来自网络外部 ……280
第 585 招：有了杀毒软件单机版就不需要安装网络版了 ……280
第 586 招：局域网有防火墙所以单机上就不需要再装防火墙 ……280
第 587 招：不需要对 UNIX 和 Linux 系统采取严格的病毒防范措施 ……281
第 588 招：使用 Macintosh 电脑不必担心受到攻击 ……281
第 589 招：浏览器补丁更新以后系统就安全了 ……281
第 590 招：病毒防护工具可以阻止各种恶意程序侵入系统 ……281
第 591 招：对付电脑病毒的关键是“杀” 282
第 592 招：每月更新一次病毒库系统就会安全 ……282
第 593 招：在内部网上共享的文件是安全的 ……282
第 594 招：安全评估就是安全扫描 ……282
第 595 招：安全扫描就是针对系统和软件漏洞的扫描 ……282
第 596 招：杀毒软件不能实现防火墙的功能 ……283
第 597 招：防火墙多装几个更有安全保障 ……283
第 598 招：封闭端口不是保障网络安全的惟一办法 ……283
第 599 招：在线检测没问题就行了 ……284
第 600 招：安全等级越高越好 ……284

第1章　增强系统安全性

1.1　系统登录与退出安全设置

第1招：通过BIOS设置开机密码

BIOS开机密码是进入系统的第一道防线，这道防线虽然不是不可逾越的，但设置开机密码对于一般水平的攻击者还是有一定作用的。以Phoenix-Award BIOS为例，开机密码的设置方法如下。

（1）开机时按住“Del”键不放即可进入BIOS设置程序。

（2）移动光标到“SUPERVISOR PASSWORD”菜单并回车，出现设置密码对话框。输入密码后回车，再输入一次相同的密码并确认，完成密码设置。

（3）移动光标到“Advance BIOS Features”菜单并回车，再移动光标到“SECURITY OPION”菜单回车，选择“SYSTEM”选项，按“Esc”键退出。

注意：此处必须选择SYSTEM才代表设置的是系统开机密码，SETUP代表的是BIOS设置密码。

（4）选择SAVE&EXIT SETUP菜单并按回车，出现提示后按“Y”键，保存并退出BIOS设置。

这样设置后，以后每次开机都会弹出对话框，要求输入开机密码，否则无法进入系统。

提示：如果要取消密码设置，进入密码设置，两次输入密码为空即可。

第2招：让Windows 98必须输入密码才能登录

大家都知道给Windows 98设置密码完全是一个摆设，任何人都可以单击登录对话框的“取消”按钮正常进入系统并操作，因此Windows 98登录密码毫无安全性可言。但通过注册表设置，可以强制用户登录时必须输入密码，否则不允许登录。这在一定程度上提高了Windows 98的登录安全性。具体设置方法如下。

单击“开始→运行”，在“运行”对话框中输入“regedit”并回车，打开注册表编辑器。展开[HKEY_LOCAL_MACHINE\Network\Logon]分支，新建或选中名为“MustBeValidated”（REG_DWORD类型）的键值项，将其键值设置为“1”即可。

提示：①将“MustBeValidated”的键值设置为“0”表示允许单击“取消”登录。

②通过修改注册表更改系统属性，在设置完成后需要重新启动系统才能生效。

第3招：禁止将网络登录密码保存在PWL文件中

通常情况下，Windows 98系统口令及网络口令都保存在.pwl文件中，例如，如果登录用

户为 MS，则密码文件为 MS.PWL。这使解密高手有机可乘，通过如下操作可以将口令不保存为*. pwl 文件。

单击“开始→运行”，在“运行”对话框中输入“regedit”并回车，打开注册表编辑器。展开[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Lanman]分支，新建或选中名为“DisablePwdCaching”（REG_BINARY 类型）的键值项，将其键值设置为“01 00 00 00”即可。

第 4 招：禁止系统启动时使用 F8 启动功能键

Windows 98 启动时按住“F8”键可打开系统功能菜单，进入 DOS 或安全模式，这样就能绕过前面设置的登录密码，直接进入系统。为防止此安全漏洞，可以编辑 Windows 98 的 MSDOS.SYS 文件，在其中加入如下修改。

BootDelay=0：开机时不显示“Starting Windows 98”，省略延迟；

BootGUI=1：直接进入 Windows 98 图形界面，而不是 DOS 状态；

BootKeys=0：禁止 F4、F5 和 F8 等开机功能键；

BootMenu=0：不显示开机菜单；

BootMulti=0：不允许双引导；

BootWin=1：直接启动 Windows 98，而不进入 DOS 环境。

这样就达到了禁止使用功能键进入 DOS 状态或安全模式的目的，从而保证了系统安全。

此外，为防止其他用户在系统启动时按“Ctrl+Alt+Del”组合键使计算机重新启动后直接进入安全模式，还须在 MSDOS.SYS 文件中加入一条：BootFailSafe=0（禁止安全模式），这样就完全确保了系统登录密码的有效性。

提示：要恢复安全模式登录，设置 BootFailSafe=1 即可。

第 5 招：让系统开机即运行屏保程序

让计算机开机后自动进入加密的屏幕保护程序可防止非法用户使用系统。如果只是把屏幕保护程序拖到“开始→程序→启动”中是不行的，因为在计算机启动时只要按住“Ctrl“或“Shift”键就能跳过“启动”。而经过如下设置之后，用户就可以高枕无忧了。

单击“开始→运行”，在“运行”对话框中输入“regedit”并回车，打开注册表编辑器。展开[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]分支，新建或选中名为“PingBao”（REG_SZ 类型）的键值项，将其键值设置为某加密屏幕保护程序名及其路径，如“C:\Windows\System\三维文字.scr”。

提示：如需取消开机即进入屏保设置，删除此键值项即可。

第 6 招：为系统设置强健的登录密码

一些用户习惯于把系统登录密码设置得很简单，容易记忆；但是简单的密码也容易被破解，比如以个人姓名的拼音作为密码，或者使用和自己有关系的一组数字，如生日、电话号