

<<精通电脑安全防护技巧600招>>

图书基本信息

书名：<<精通电脑安全防护技巧600招>>

13位ISBN编号：9787115131812

10位ISBN编号：7115131813

出版时间：2005-10

出版时间：人民邮电出版社

作者：张发凌

页数：284

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<精通电脑安全防护技巧600招>>

内容概要

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。

书籍目录

第1章 增强系统安全性 11.1 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 11.2 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 25.3 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 37.1 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 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 573.1 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 643.2 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 774.1 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 894.2 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 995.1 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 1105.2 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 1136.1 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的自防病毒选项 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 1186.2 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 1276.3 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

<<精通电脑安全防护技巧600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 1387.1 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 1497.2 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) 1557.3 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 1628.1 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 1768.2 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 1979.1 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 2129.2 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 2259.3 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 23110.1 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 24110.2 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 26910.3 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 27411.1 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第580招：合理设置工具软件减少病毒危害 27811.2 安全误区 279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 283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

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>