

电脑软、硬件自己动手DIY系列

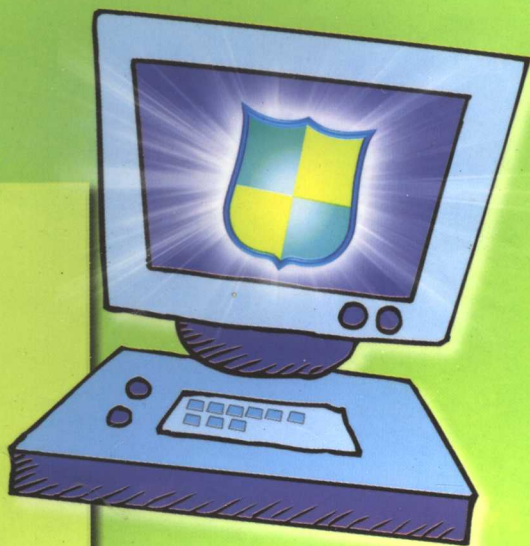
打造我的 安全电脑



北京希望电子出版社 总策划
张 强 张志楠 编 著

你想知道吗：

- ❖ 缺乏安全使用电脑的基本知识造成的损失将是什么？
- ❖ 如何设置Windows的用户密码与各种安全设置？
- ❖ 如何给Windows 98/2000/XP打补丁和升级？
- ❖ 如何使用SSH软件保证远程安全登录？
- ❖ 如何检测电脑端口与电脑系统漏洞？
- ❖ 如何给压缩软件加密？
- ❖ 如何防范恶意网页？
- ❖ 如何设置CMOS密码？
- ❖ 如何进行加密技术和数字签名？
- ❖ 如何使用QQ密码防盗专家保护QQ密码？
- ❖ 如何从表现形式和传播途径发现并防止电脑病毒？
- ❖ 如何删除电脑中保存用户上网登录账户和密码的临时文件？



中国林业出版社
China Forestry Publishing House
www.cfph.com.cn



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

电脑软、硬件自己动手DIY系列

打造我的 安全电脑

北京希望电子出版社 总策划
张 强 张志楠 编 著

你想知道吗：

- ⊙ 缺乏安全使用电脑的基本知识造成的损失将是什么？
- ⊙ 如何设置Windows的用户密码与各种安全设置？
- ⊙ 如何给Windows 98/ 2000/XP打补丁和升级？
- ⊙ 如何使用SSH软件保证远程安全登录？
- ⊙ 如何检测电脑端口与电脑系统漏洞？
- ⊙ 如何给压缩软件加密？
- ⊙ 如何防范恶意网页？
- ⊙ 如何设置CMOS密码？
- ⊙ 如何进行加密技术和数字签名？
- ⊙ 如何使用QQ密码防盗专家保护QQ密码？
- ⊙ 如何从表现形式和传播途径发现并防止电脑病毒？
- ⊙ 如何删除电脑中保存用户上网登录账户和密码的临时文件？



中国林业出版社
China Forestry Publishing House
www.cfph.com.cn



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内容简介

本书是一本介绍如何保护自己的电脑以及网络系统中的数据不被破坏和丢失,如何保证数据在传输过程中的安全,如何避免数据被篡改,如何在系统和文件遭到破坏后能够恢复还原,如何保护网上交易的安全,保证网络游戏安全,如何保证电子邮件的安全的书。

全书共分为 7 个部分,15 个章节,详细介绍了电脑安全概述、电脑操作系统安全、软件安全与文件保护、上网安全、硬件安全与病毒防范、数据备份与恢复、黑客防范与防火墙使用。

本书结构清晰,深入浅出,重视实践,立足于解决实际问题,以操作为主,每个步骤都配有相应的图片,使所有操作一目了然,方便读者阅读和学习,使读者真正能够 step by step (一步一步)地掌握本书所提供的各种保护电脑的实用安全方法。

本书不仅适合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

打造我的安全电脑/张强、张志楠编著.—北京:中国林业出版社,2006.1

ISBN 7-5038-4093-5

I. 打... II. ①张... ②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 106614 号

出版:中国林业出版社(100009 北京市西城区刘海胡同 7 号 010-66184477)

北京希望电子出版社(100085 北京市海淀区上地 3 街 9 号金隅嘉华大厦 C 座 611)

网址:www.bhp.com.cn 电话:010-82702660(发行) 010-62541992(门市)

印刷:北京媛明印刷厂

发行:全国新华书店经销

版次:2006 年 1 月第 1 版

印次:2006 年 1 月第 1 次

开本:787×1092mm 1/16

印张:19

字数:436 千字

印数:0001~5000 册

定价:25.00 元

前 言

足球比赛中,进攻是最好的防御。但在计算机安全领域不是这样!作为普通用户最需要的是维护计算机正常使用,保护自己的信息不受损失。基于以上考虑,设计一本从解决实际问题出发、重在防护、让读者学会方法而不是依样画葫芦的图书就是极有价值的事情了。

同时,纵观当前图书领域,计算机安全、网络安全和黑客等相关书籍并不少见,但真正适合读者的却不多见。一些是属于教程类的安全理论,对普通用户根本无法起到解决安全问题的实际作用;一些书籍过于重视讲述安全方面的技术性问题,普通用户实在难以理解;另外一些书籍则是主要介绍黑客相关技术,这些并不符合普通用户需要。对普通用户需要的是安全使用计算机,并不是去当黑客。

◎ 本书的读者对象

本书主要面对日常使用计算机的办公人员,各类非计算机专业人员。对于最广大的计算机用户来说,实际上对网络安全、计算机安全等并不精通,但又不可能花费太多精力去研习。因此,如何在最短的时间内,花费不大的精力,让上述读者学到最实用的计算机安全、网络安全知识,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专门设计、编写。

本书的讲解深入浅出,并且提供了尽可能详细的操作步骤和分解图片,可以使你毫无困难地学习。对于经常使用计算机的用户,阅读本书将不会有任何障碍。对于计算机基础较薄弱的用户,也不用担心学习困难,只要知道如何启动计算机,如何区分鼠标左右键,什么是单击和双击,则阅读本书就不会有障碍了,并能通过本书的学习获得巨大收获。

本书代表了网络和系统安全实用技术的发展方向,充分考虑了广大初、中级计算机用户在安全方面的根本需求。

◎ 本书的特点

本书内容丰富、讲解详尽、由浅入深,适合各个层次的读者学习。全书以操作为主,每个步骤都配有相应的图片,使所有操作一目了然。全书以专题为主线分为七个部分:电脑安全概述、电脑操作系统安全、软件安全与文件保护、上网安全、硬件安全与病毒防范、数据备份与恢复、黑客防范与防火墙使用。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,用户可以联系自己的实际问题,逐步深入地学习到计算机及其网络安全方面的基本知识、方法和技巧,成为维护电脑系统安全的“门内汉”。

◎ 本书的内容结构

第一部分 电脑安全概述

第1章 为什么要掌握基本的电脑安全知识。通过实际案例说明掌握电脑系统的安全知识的重要性和必要性。

第二部分 电脑操作系统安全

第2章 电脑操作系统安全。操作系统的安全是电脑系统的核心,本章介绍Windows 98/2000/XP中用户账户、密码设置的相关知识和方法。

第3章 电脑端口和电脑漏洞检测。介绍电脑端口基本知识，以及检测电脑漏洞的软件和方法。

第三部分 软件安全与文件保护

第4章 应用软件安全。介绍保证 Office 文档和 PDF 文档安全的基本方法。

第5章 使用加密保护文件。介绍加密的基本知识，PGP 软件的使用，压缩文件的加密方法。

第四部分 上网安全

第6章 电子邮件与网上聊天安全。介绍如何安全使用 OE、FoxMail，如何安全使用 QQ 和 MSN 上网聊天。

第7章 IE 浏览器安全。介绍保证 IE 安全的基本方法。

第8章 电子商务安全。介绍如何安全地在网上购物，如何保护用户账户和密码。

第五部分 硬件安全与病毒防范

第9章 硬件安全-CMOS 密码设置与破解。介绍 CMOS 各种密码的设置及其常用破解软件和破解方法。

第10章 电脑病毒与防护。介绍电脑病毒的基本知识、常用防护和检查方法。

第六部分 数据备份与恢复

第11章 分区表和系统的备份与恢复。介绍如何对分区表和系统进行备份与恢复。

第12章 分区和文件的备份与恢复。介绍如何对硬盘分区进行备份与恢复。

第七部分 黑客防范与防火墙使用

第13章 黑客攻击防范。介绍防范黑客攻击的基本方法。

第14章 网络游戏安全。介绍如何保护网络游戏中的用户账户和密码的安全。

第15章 防火墙的使用。介绍几种常用防火墙的设置和使用方法。

◎ 致谢

本书由张强、张志楠编写。张强从事计算机教学多年，对网络安全、数据安全教学有很深刻的认识，非常了解读者的学习特性；张志楠从事网站管理多年，具有丰富的网络维护，精通计算机的软、硬件问题处理。同时参加本书编写与整理的还有赵密广、蔡朝晖、徐勤、孙立文、刘强、王俊宏、孙桂娟、张斌、岳振华、邢爱珍、李辉、赵孝、谭春娥、奚峰等。

作者的 E-mail 地址：zhqang@edatapower.com。

感谢你选择本书，希望本书能够对提高你的处理计算机安全的能力有所帮助，本书如有不当之处，希望你不吝指正。

编者

目 录

前言

第一部分 电脑安全概述

第 1 章 为什么要掌握基本的电脑安全知识.....1

- 1.1 缺乏电脑安全知识造成损失的案例.....1
 - 1.1.1 案例 1-疏忽大意造成损失.....2
 - 1.1.2 案例 2-由于用户缺乏必要的安全知识造成的损失.....2
 - 1.1.3 案例-3 黑客攻击造成的损失.....2
- 1.2 电脑及网络安全概述.....3
 - 1.2.1 电脑硬件安全.....3
 - 1.2.2 电脑信息安全.....6
 - 1.2.3 电脑网络安全.....7
- 1.3 电脑安全的基本技术.....8
 - 1.3.1 物理安全技术.....8
 - 1.3.2 访问控制.....9
 - 1.3.3 数据完整性检验.....9
 - 1.3.4 数据机密性保护.....9
 - 1.3.5 防病毒技术.....9
 - 1.3.6 防火墙技术.....9
 - 1.3.7 数据备份与恢复技术.....9
- 本章小结.....9

第二部分 电脑操作系统安全

第 2 章 Windows 系统安全.....10

- 2.1 Windows 安全概述.....10
- 2.2 Windows 98 的密码和安全设置.....11
 - 2.2.1 如何设置 Windows 98 用户密码.....11
 - 2.2.2 如何设置 Windows 98 启动密码.....12
 - 2.2.3 如何设置屏保密码.....13
 - 2.2.4 如何破解屏保密码.....14
 - 2.2.5 如何在 Windows 98 中隐藏文件夹.....14

- 2.2.6 如何在 Windows 98 中显示隐藏文件夹.....15

2.3 Windows 2000/XP 密码和账户设置.....15

- 2.3.1 Windows 2000/XP 的登录过程简介.....15
- 2.3.2 如何设置 Windows 2000/XP 启动密码.....16
- 2.3.3 如何停用 Windows 2000/XP 启动密码.....17
- 2.3.4 如何制作 Windows 2000/XP 密码恢复盘.....18
- 2.3.5 如何设置 Windows XP 安全登录或注销.....20
- 2.3.6 如何设置 Windows 2000/XP 的用户账号.....21
- 2.3.7 如何设置 Windows XP 用户密码...22
- 2.3.8 如何更改 Windows 2000/XP 用户密码.....23
- 2.3.9 如何在添加用户的同时设置 Windows XP 用户密码.....23
- 2.3.10 如何恢复丢失的 Windows XP 密码.....24

2.4 Windows 文件安全设置.....25

- 2.4.1 使用 NTFS 文件系统保证系统安全.....25
- 2.4.2 如何设置 Windows XP 文件夹的本地共享与安全管理.....25
- 2.4.3 如何设置 Windows XP 文件夹的网络共享与安全管理.....26
- 2.4.4 如何实现 Windows XP 文件夹的隐藏和加密.....26
- 2.4.5 如何设置 NTFS “文件/文件夹”权限.....27
- 2.4.6 如何恢复文件/文件夹的默认访问权限.....28

2.5 如何给 Windows 98/2000/XP 打补丁

和升级	30	4.1.3 如何用数字签名保护文档	54
2.5.1 如何给 Windows 98 打补丁 和升级	30	4.2 Excel 电子表格安全	56
2.5.2 如何在局域网里给 Windows 2000/XP 打补丁和升级	30	4.2.1 如何设置 Excel 密码	56
2.5.3 如何从微软的网站上给 Windows XP 打补丁和升级	31	4.2.2 如何保护 Excel 工作簿	57
2.5.4 如何给 Windows 2000 打补丁 和升级	33	4.2.3 如何设置工作表保护	57
2.5.5 如何在 Windows 2000/XP 中 安装数字认证书	34	4.2.4 如何设置单元格保护	58
本章小结	37	4.2.5 如何撤销工作簿保护和撤销 工作表保护	59
第 3 章 电脑端口与系统漏洞检测	38	4.2.6 如何为 Excel 添加数字签名	59
3.1 电脑系统安全漏洞检测	38	4.3 Access 数据库安全	61
3.1.1 什么是电脑系统安全漏洞	38	4.3.1 Access 数据库加密的作用与实现 ..	61
3.1.2 如何使用 Nessus 扫描软件 检测安全漏洞	38	4.3.2 如何设置数据库密码	62
3.1.3 如何使用 SSS 软件检测 安全漏洞	42	4.3.3 什么是 MDE 和 ADE 文件 如何将 MDB 格式文件转换 MDE 格式文件	63
3.1.4 如何使用 MBSA 检查电脑 系统安全	44	4.3.4 用户与组账户有何作用	64
3.1.5 网络侦听功能简述	45	4.3.5 如何新建用户	64
3.1.6 如何使用 ARPKILLER 软件 查找网络嗅探器 (sniffer)	46	4.3.6 如何新建组	65
3.1.7 如何使用 SSH 软件保证远程 安全登录	46	4.3.7 如何设置用户隶属组	65
3.2 电脑端口检查	47	4.3.8 如何设置用户登录密码	66
3.2.1 什么是电脑端口	47	4.3.9 如何设置用户和组的权限	66
3.2.2 如何监视电脑端口	47	4.4 Office 文件的恢复	66
3.2.3 如何在线检测电脑端口	49	4.4.1 恢复没有响应的程序	66
本章小结	51	4.4.2 如何恢复 Office 文档	67
第三部分 软件安全与文件保护		4.4.3 如何使用 Easerecovery 修复 Office 文档	67
第 4 章 应用软件安全	52	4.5 Acrobat Professional 6.0 的安全性	69
4.1 Word 文档安全	52	4.5.1 如何为 PDF 文档设置权限密码	69
4.1.1 如何隐藏文档记录	52	4.5.2 Acrobat 的数字签名及其使用	70
4.1.2 如何设置 Word 权限	53	4.5.3 如何进行自签名数字证书加密 PDF 文档	73
		4.5.4 如何在 PDF 文档上进行自签名 数字证书	75
		本章小结	79
		第 5 章 使用加密保护文件	80
		5.1 加密技术和数字签名简介	80
		5.1.1 什么是加密技术	80
		5.1.2 单钥加密法	81

5.1.3	公钥加密法	82
5.1.4	什么是数字签名	82
5.2	PGP 加密软件的使用	83
5.2.1	如何安装 PGP	84
5.2.2	如何生成 PGP 的密钥	86
5.2.3	如何管理 PGP 密钥	87
5.2.4	如何用 PGP 加密文件	93
5.2.5	如何用公钥加密文件	96
5.2.6	如何用私钥签名文件	97
5.2.7	如何用 PGP 永久性删除文件	98
5.3	压缩软件的加密	100
5.3.1	如何用 WinZip 8.0 对 ZIP 压缩文档加密	100
5.3.2	如何用 WinRAR 3.0 对 RAR 压缩文档的加密	101
	本章小结	102

第四部分 上网安全

第 6 章	电子邮件与网上聊天安全	103
6.1	E-mail 安全防范	103
6.1.1	如何安全使用 Outlook Express 6 ..	103
6.1.2	如何安全使用 Foxmail 5.0	109
6.1.3	使用 PGP 签名和加密 E-mail	111
6.1.4	Web 信箱的安全问题	112
6.2	QQ 安全防范	114
6.2.1	如何申请保护 QQ 密码	114
6.2.2	使用 QQ 密码防盗专家保护 QQ 密码	115
6.2.3	QQ 常见漏洞	117
6.2.4	QQ 病毒查杀与专杀	117
6.2.5	如何防护 QQ 消息炸弹	118
6.2.6	如何防护 QQ 变异“炸弹”	120
6.3	MSN 安全防范	121
6.3.1	如何安全使用 MSN	121
6.3.2	如何防护 MSN 病毒	123
6.3.3	即时了解 MSN 最新更新信息	124
	本章小结	124

第 7 章	IE 浏览器安全	125
7.1	IE 的安全设置	125
7.1.1	如何防范恶意网页	125
7.1.2	如何设置分级审查	126
7.1.3	如何设置匿名浏览	127
7.1.4	如何清除 Cookie 记录	128
7.1.5	如何清除历史记录	128
7.1.6	如何清除密码记录	129
7.1.7	如何删除 IE 临时文件	129
7.2	修复 IE	129
7.2.1	如何给 IE 打补丁	129
7.2.2	如何在线检测浏览器漏洞	130
7.2.3	如何使用“上网助手”修复 IE ...	131
	本章小结	133
第 8 章	电子商务安全	134
8.1	在线电子商务应注意的事项	134
8.1.1	在线电子商务的类型	134
8.1.2	在商家自己的网站购物	135
8.1.3	要找有知名度的大网站交易	135
8.1.4	了解安全购物规则	135
8.1.5	注意商家信息是否真实完整	135
8.1.6	了解商家的信誉度	136
8.1.7	对比价格，价格过于便宜的 商品要小心	136
8.1.8	警惕欺骗性电子邮件	136
8.1.9	欺骗性电子邮件的主要特征	137
8.1.10	如何防范假冒网站	138
8.1.11	如何保护个人银行账号	138
8.1.12	注意注册和通过实名 认证的时间	139
8.2	网上购物安全支付方式	139
8.2.1	使用货到付款	139
8.2.2	使用安全付款服务	139
8.2.3	申请个人证书	140
8.2.4	在线支付最好使用一个 单独的银行卡	140
8.2.5	在线支付密码输入后， 窗口要及时关闭	140

8.2.6	不要在网吧进行网上支付	140
8.3	网上个人信息的保密	140
8.3.1	如何设置 IE 防止 Cookie 泄漏个人资料	140
8.3.2	如何修改注册表防止 Cookie 泄漏个人资料	140
8.3.3	如何使用 KV2005/2004 保护网络隐私	141
8.4	用户账号、密码的保密和保管	143
8.4.1	删除保存用户上网登录账户和 密码的临时文件	143
8.4.2	如何使用修改文件名的方法 保护密码	144
8.4.3	使用 Password 2000 软件 保护密码	144
	本章小结	147

第五部分 硬件安全与病毒防范

第 9 章	硬件安全—CMOS 密码设置与破解	148
9.1	什么是 BIOS 和 CMOS	148
9.2	如何进入 BIOS 设置环境	149
9.3	如何设置 CMOS 密码	150
9.3.1	如何设置高级管理员的密码	150
9.3.2	如何设置普通用户密码	151
9.3.3	如何设置启动密码	152
9.4	如何破解 CMOS 密码	153
9.4.1	如何使用 CMOSPWD.EXE 破解软件	153
9.4.2	如何利用 DEGUG 去除 CMOS 密码	155
9.4.3	如何建立自己的破解文件	155
9.4.4	如何使用 C 语言编写 CMOS 密码清除程序	156
9.4.5	如何使用 CMOS 放电清除密码	156
9.4.6	如何使用跳线放电清除密码	157
9.4.7	如何通过升级 BIOS 破解密码	158
	本章小结	158

第 10 章	电脑病毒与防护	159
10.1	电脑病毒概述	159
10.1.1	电脑病毒定义	160
10.1.2	电脑病毒的特征	161
10.1.3	电脑病毒破坏的表现	163
10.2	电脑病毒的表现	163
10.2.1	病毒发作前的表现现象	164
10.2.2	电脑病毒发作时的表现现象	165
10.2.3	电脑病毒发作后的表现现象	166
10.2.4	如何从表现形式和传播途径 发现电脑病毒	168
10.3	电脑病毒的工作过程	168
10.4	电脑病毒的防治	169
10.4.1	认识电脑病毒的传播途径	169
10.4.2	电脑病毒的预防	169
10.4.3	查杀病毒时的注意事项	171
10.4.4	病毒发生后如何处理	171
10.5	典型病毒的防范与杀除	174
10.5.1	如何识别宏病毒及进行防范	174
10.5.2	如何进行宏病毒的预防与删除	175
10.5.3	如何清除冲击波病毒	176
10.5.4	振荡波等蠕虫病毒的攻击 目标及危害	178
10.5.5	如何清除冲击波病毒	178
10.6	常用杀毒软件简介	179
10.7	KV2005 杀毒软件的使用	180
10.7.1	KV2005 安装	180
10.7.2	KV2005 工作界面	182
10.7.3	如何升级 KV2005	183
10.7.4	KV2005 系统设置	183
10.7.5	如何制作 DOS 杀毒盘	185
10.7.6	如何使用 DOS 杀毒盘杀毒	185
10.7.7	如何制作硬盘修复王	186
10.7.8	如何备份与恢复 KV2005	186
10.8	金山毒霸 2005 杀毒软件的使用	187
10.8.1	金山毒霸 2005 的安装与注册	187
10.8.2	工作界面	187
10.8.3	查杀病毒	188

10.8.4	杀毒设置	189
10.8.5	创建应急盘	192
10.8.6	防毒设置	193
10.9	卡巴斯基 5.0 杀毒软件使用	197
10.9.1	卡巴斯基的安装与注册	198
10.9.2	工作界面	198
10.9.3	扫描病毒	198
10.9.4	现在更新	200
10.9.5	查看隔离区	200
10.9.6	查看报告	201
10.9.7	查看备份	202
10.9.8	配置实时监控	202
10.9.9	配置手动扫描	204
10.9.10	定制全面扫描计划	205
10.9.11	配置更新	205
10.10	Norton AntiVirus 杀毒软件的使用	206
10.10.1	如何在尚未安装 NAV 的情况下 杀除计算机中的病毒	206
10.10.2	NAV 2004 的安装与注册	208
10.10.3	工作界面	208
10.10.4	扫描病毒	209
10.10.5	计划扫描设置	211
10.10.6	升级病毒库	212
	本章小结	213

第六部分 数据备份与恢复

第 11 章	分区表和系统的备份与恢复	214
11.1	数据备份的概述	214
11.2	硬盘分区表备份与修复	215
11.2.1	如何使用 Diskgen 软件 备份分区表	215
11.2.2	如何使用 Diskgen 软件 恢复硬盘分区表	216
11.2.3	如何使用 Diskgen 重建 硬盘分区表	217
11.2.4	如何使用 KV 硬盘修复王 备份和修复分区表	217
11.3	系统文件的备份与恢复	218

11.3.1	如何备份硬件配置文件	218
11.3.2	如何备份和恢复 Windows 注册表	220
11.4	Windows 系统备份与恢复	221
11.4.1	如何恢复 Windows 98 系统	221
11.4.2	如何备份和恢复 Windows 2000 系统	222
11.4.3	如何备份和恢复 Windows XP 系统	225
11.5	驱动程序备份与恢复	227
11.5.1	如何使用驱动精灵备份 驱动程序	228
11.5.2	如何使用驱动精灵恢复 驱动程序	230
11.5.3	如何使用驱动精灵备份数据	230
11.5.4	如何使用驱动精灵备份 IE 收藏夹	231
11.5.5	如何使用驱动精灵恢复数据	231
	本章小结	231

第 12 章 磁盘分区和文件的备份与恢复

12.1	Norton Ghost 备份工具的使用	232
12.1.1	如何使用 Norton Ghost 2003 进行分区备份	232
12.1.2	使用 Norton 恢复分区	237
12.1.3	如何创建 DOS 启动盘	239
12.1.4	如何使用 Ghost 启动盘 备份分区	240
12.1.5	如何使用 Ghost 启动盘 恢复分区	242
12.2	Ghost Explore 备份工具的使用	243
12.2.1	如何在 Windows 下修改 备份映像文件	243
12.2.2	如何使用 Ghost Explore 恢复文件和文件夹	244
12.2.3	如何使用 Ghost Explore 添加文件和文件夹	244
12.3	如何使用 EasyRecovery 恢复文件	245
12.3.1	如何恢复文件和文件夹	245

12.3.2	如何恢复被删除的文件	247
12.3.3	如何从一个格式化分区中 恢复文件	248
12.4	Power Image 备份工具的使用	249
12.4.1	如何使用 Power Image 备份分区	249
12.4.2	如何使用 PQDI 恢复分区	250
12.5	百诺备份专家的使用	252
12.5.1	如何设置百诺备份专家	252
12.5.2	如何使用百诺备份专家 备份分区	252
12.5.3	如何使用百诺备份专家 恢复分区	254
	本章小结	254

第七部分 黑客防范与防火墙使用

第 13 章	黑客攻击防范	255
13.1	因特网和通信协议简述	255
13.1.1	什么是 TCP/IP 协议	255
13.1.2	什么是 IP 地址	255
13.1.3	IP 地址是怎样分类的	256
13.1.4	TCP/IP 提供哪些常见服务	257
13.1.5	TCP/IP 有什么安全缺陷	257
13.2	黑客攻击手段	258
13.2.1	黑客概述	258
13.2.2	黑客有哪些攻击手段	258
13.2.3	黑客攻击的基本步骤	260
13.2.4	防范黑客攻击的对策	261
13.2.5	如何封死黑客的“后门”	263
13.2.6	如何做好 IE 的安全设置	266
13.3	防范木马	267
13.3.1	木马特性	267
13.3.2	木马的工作原理	268
13.3.3	如何使用木马分析专家 检测木马	268
13.3.4	如何使用反间谍专家检测木马	270
13.3.5	如何使用反黑精英查杀木马	273
13.4	江民黑客防火墙的使用	276

13.4.1	如何进行规则设置	276
13.4.2	如何设置江民黑客防火墙	277
13.4.3	如何进行程序审核	278
13.4.4	如何显示当前连接	279
13.4.5	如何显示系统信息	279
	本章小结	280

第 14 章 网络游戏安全

14.1	网络游戏安全概述	281
14.2	如何保护网络游戏的密码和隐私	282
14.2.1	如何使用 KV2004/2005 保护隐私信息	282
14.2.2	如何使用金山网镖防盗取 网络游戏密码	284
14.2.3	如何彻底防御网络游戏外挂木马	284
14.3	如何使用防盗卡保护网络游戏	285
14.3.1	如何绑定矩阵防盗卡	286
14.3.2	如何绑定备用卡	286
14.3.3	如何把备用卡转成当前卡	287
14.3.4	如何使用防盗卡登录游戏	288
	本章小结	288

第 15 章 防火墙的使用

15.1	防火墙技术简介	289
15.1.1	防火墙的工作原理	289
15.1.2	防火墙的类型	290
15.1.3	包过滤技术及防火墙的 主要功能	290
15.2	Windows XP ICF 防火墙的使用	291
15.2.1	如何启用 ICF 防火墙	291
15.2.2	如何设置 ICF 防火墙	292
15.3	Windows XP SP2 防火墙设置	293
15.3.1	如何启动 SP2 安全中心	294
15.3.2	如何进行 SP2 防火墙常规设置	294
15.3.3	如何处理 Windows 安全警报	294
15.3.4	如何进行 SP2 防火墙例外设置	295
15.3.5	如何进行 SP2 防火墙高级设置	296
15.4	Symantec 防火墙的安装和使用	298
15.4.1	网络安全特警的安装	298

15.4.2	如何在第一次启动时 设置防火墙	300	15.5.1	安装天网防火墙个人版	311
15.4.3	如何对 Norton 网络安全 特警进行升级	305	15.5.2	天网防火墙系统设置	313
15.4.4	如何设置防火墙的原则	305	15.5.3	自定义 IP 规则	314
15.4.5	如何使用 Symantec 在线 安全检测	309	15.6	金山网镖 6	316
15.5	天网防火墙个人版	310	15.6.1	安装金山网镖 6	316
			15.6.2	如何使用 IP 规则编辑器	318
			15.6.3	如何进行系统漏洞检测	319
				本章小结	320

第一部分 电脑安全概述

第 1 章 为什么要掌握基本的电脑安全知识

本章重点：

当代社会，人们越来越依靠电脑，电脑给人们带来巨大的效益的同时，也带来潜在的巨大风险。实际上，电脑病毒的泛滥，黑客的横行已经给人们带来了数以亿计的巨大损失。

所以，为了在享受电脑带来巨大效益的同时减少其所造成的损失，我们就必须掌握必要的电脑安全知识。

知识要点：

缺乏安全使用电脑的基本知识造成损失的案例

电脑及其网络安全概述

电脑安全的基本技术

1.1 缺乏电脑安全知识造成损失的案例

随着社会信息化进程的飞速发展和计算机硬件价格的不断下跌，电脑的使用已经非常普及了。在很多办公室中，人手一台电脑已经十分普遍；在家庭中，拥有两台以上的电脑已不鲜见，具有多台电脑的家庭还有的组建了家庭网络。电脑作为人们日常办公的工具、网上冲浪的舢板，已经成为现代社会中人们生活的必需品。在各种政治、经济、社会活动中，人们使用电脑来处理日益增长的各种各样的巨量信息，设想在现代社会，如果电脑停止运行 1 个小时，将会出现什么样的后果呢？将给人们带来巨大的损失。

任何事物都具有两面性，电脑在给人们带来巨大好处的同时，也给人类社会带来了巨大的风险。巨量的各种商业信息、经济信息、个人信息 24 小时在网上穿梭，并且长期保存在电脑的硬盘中，无论哪个环节一旦出现意外，而事先没有采取预防措施，那么造成的损失将是极其巨大的。

电脑病毒的泛滥，黑客的横行已经给人们带来了数以亿计的损失。曾几何时，电脑病毒的泛滥使人闻毒色变，黑客横行令人痛恨但又无可奈何，由于缺乏安全知识，用户个人的疏忽大意造成硬盘数据的丢失，令人痛不欲生，是很多人都经历过的事情。



1.1.1 案例 1 疏忽大意造成损失

某公司办公室人员王某，由于硬盘上保存的历史文件过多，造成 D 盘剩余空间太少，因此决定对 D 盘进行清理，把一些已经没用的文件彻底删除掉，即不把删除的文件放到回收站内，而直接进行彻底删除。但是在操作过程中，不小心把几份重要的文件也同时删除掉了，当时并没有发现。第二天上班时发现这些重要文件被删除了，由于当时没有做过文件备份，因此无法恢复，王某十分着急。虽说后来采用了补救措施，但是耽误了很多时间、精力，也影响了公司的业务。事后因为此事，王某被公司老板严重批评。

1.1.2 案例 2 由于用户缺乏必要的安全知识造成的损失

北京某高校教师李某，一天突然发现自己的电脑不能启动了，赶紧求助于学校的计算机教师，经过检查发现电脑中了病毒，分区表和文件分配表遭到破坏。该教师十分着急，因为该计算机的硬盘中保存着刚刚撰写完成的书稿和上课的讲义。据该教师讲，以前从来没有发生过这样的事情，因此没有进行备份。尽管使用工具软件恢复了硬盘的分区表和文件分配表，但是还仍然有一些文件没有完全恢复，对于个人而言损失巨大。

对于电脑中病毒，该教师感到很奇怪，电脑已经安装过杀毒软件，怎么还会感染病毒呢？当询问他杀毒软件是否经常升级，回答说没有升过级，因不知道需要升级，也不知道怎么升级。显然这是一起很典型的由于用户缺乏杀毒软件需要定期升级的基本知识所造成的损失。

1.1.3 案例 3 黑客攻击造成的损失

在 2002 年 7 月，新加坡发展银行查获，一名电脑黑客侵入 21 个线上银行账号，盗取了 200~4999 新加坡元不等的金额，给被盗用户带来严重的经济损失。

罪犯是通过网络非法侵入某些客户的个人电脑，利用黑客手段，窃取了用户电脑用户账号和密码，然后实施网上盗窃的。事后调查，这些被盗的用户缺乏必要的防黑客的知识，在电脑上，没有安装防黑软件或是把防黑软件关闭了，从而造成了巨大的经济损失。

图 1-1 表现的正是黑客攻击著名网站，更改网站主页。

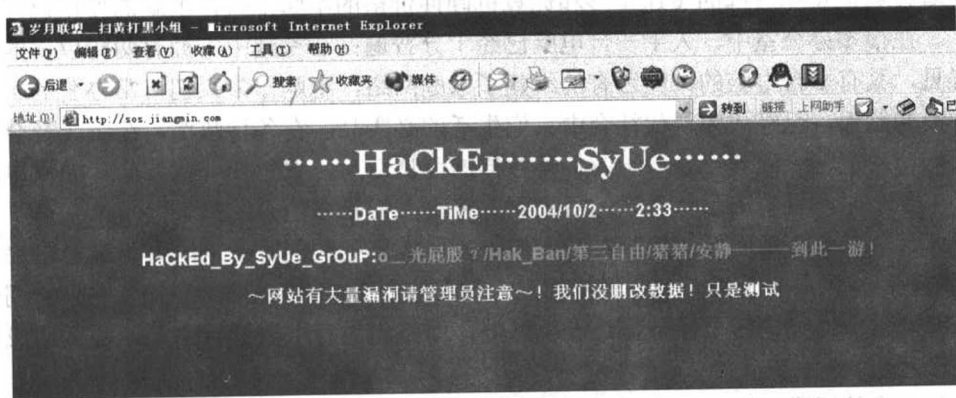


图 1-1 黑客攻击著名网站，更改网站主页

以上案例不胜枚举，那么如何防止和解决电脑不安全的问题，正是本书的宗旨。

1.2 电脑及网络安全概述

电脑安全也称为计算机安全。随着电脑使用的普及,电脑出现数据丢失、黑客入侵、病毒感染的案例大量涌现,使得电脑及网络安全日益成为人们讨论的重要话题。在 Internet 日益扩展和普及的今天,人们对电脑系统、网络系统安全的要求更高,所涉及的面更广了。本章将简单介绍电脑系统安全的相关知识,使广大读者对电脑系统安全、网络安全的有关知识和有关技术有一个概括的了解。

电脑系统是由硬件和软件组成的。如果说硬件是电脑的躯体,那么软件就是电脑的灵魂。电脑完成的一步步操作都需要由电脑软件来控制,离开软件,电脑就是一堆废铁,可见电脑软件在电脑系统的作用是多么重要。

电脑和网络软件是由专门的技术人员按照实际需求编写的,在软件开发阶段的各个环节中,出现一些考虑不周的问题是在所难免的,通常人们把这些软件设计中考虑不周全的地方称为软件漏洞。对于一些由几百万行代码组成的大型软件系统更是如此,或多或少总会出现一些软件漏洞,这些漏洞就造成了电脑和网络系统的安全问题。

在电脑开始使用的早期,电脑系统的安全就引起了人们的重视。到了 20 世纪 80 年代后,随着电脑的普及,特别是到了 20 世纪 90 年代 Internet 的发展,使得独立的电脑系统通过网络连接起来,在全世界的范围内,开始相互通信和共享信息。电脑系统和网络系统在处理、存储、传输和使用上存在着先天的问题,因此电脑中和网络上的数据很容易被干扰、泄露、窃取、篡改、冒充和破坏。各种病毒不断涌现和黑客攻击手段的不断发展,电脑和网络系统安全问题日益受到了人们越来越多的重视。

根据电脑和网络系统的构成,可以把电脑和网络系统的安全分为电脑硬件安全、电脑信息安全和电脑网络安全。

1.2.1 电脑硬件安全

电脑硬件的安全是软件可靠、稳定运行的保证,是信息可靠保存的保证,是构成电脑安全的基本要素。

电脑运行环境安全是指保证电脑系统运行在一个安全的工作环境中。这个工作环境可以是机房、办公室和家庭的卧室等,要求工作环境清洁、通风良好,满足电脑系统所需要的温度、湿度和电源功率。对于重要部门的电脑系统还要求设置屏蔽机房或电子干扰设备,以防重要信息的泄露。

(1) 电脑降温设备安全运行

在使用电脑时,应注意使 CPU 风扇、显卡风扇、电源风扇等散热设备良好工作,否则会由于 CPU、显卡、主板等硬件温度过高而造成电脑系统的死机或损坏。在炎热的夏季,由于连续使用电脑,且电脑的降温部件不能完全正常工作,从而导致温度过高,造成电脑烧毁的情况是屡见不鲜的。

电脑内的这些降温设备,在长期工作过程中会吸附很多灰尘,这将极大地影响降温效果。风扇的轴承内会因为缺少润滑油而不能正常工作,因此需要定期维护。

尤其是在每年进入夏季之前,应该对 CPU、显示卡以及电源的降温风扇进行除尘,并



向风扇的轴承添加润滑油。在进行这些操作时，需要用螺丝刀，把这些风扇从电脑内拆下，然后进行维护，使用毛刷清洁风扇扇页上的灰尘。

①揭开风扇上的不干胶封口纸，如图 1-2。

②向风扇轴承添加润滑油。向风扇的轴承滴 1~2 滴缝纫机油，然后把封口纸重新粘好。

③取下 CPU 散热片，用潮湿的布，擦掉其上的灰尘，如图 1-3。

④重新安装 CPU 散热片和风扇时，小心操作避免损坏主板周围的电器元件。



提示： 不要使用普通机油。



不干胶封口纸

图 1-2 降温风扇

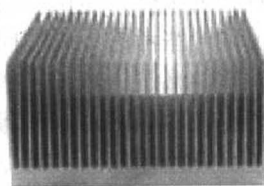


图 1-3 CPU 散热片

(2) 移动硬盘、闪存和 MP3 的安全操作

移动硬盘、闪存和 MP3 是人们使用越来越普遍的移动存储设备。同软盘相比，这些移动存储可存储更多的信息。移动存储设备是通过 USB（中文含义通用串行总线）接口与电脑相连接。

这些移动存储设备可以在 USB 接口进行热插拔（即带电插拔），使用起来十分方便。但是如果使用不当也会造成移动存储设备上数据的丢失。

在使用移动存储设备之前，首先要确定是否开启了主板上 COMS 中的总线控制器（通常都已被设置成开启），然后把移动存储设备的连线接上，插入到机箱的 USB 接口中，系统会自动监测到新硬件。



注意： 在 DOS 状态下无法使用移动储存设备。如果使用 Windows 98 操作系统，需要安装驱动程序，在 Windows 2000/XP 中不要安装驱动程序直接使用，插入后系统会自动识别，并在“我的电脑”中显示移动存储设备的分区图标。

USB 虽然支持热插拔，但是在拔掉移动存储设备时，最好是在关闭移动存储设备后再把它拔出。尤其是在打开读写数据过程中，绝对更不能直接拔下，否则会引起移动存储设备上的文件出现错误。

安全删除 USB 移动存储设备方法 1，操作步骤如下：

①在系统任务栏中，双击【USB 移动存储设备图标】，如图 1-4。

②在弹出“安全删除 USB Mass Storage Device-驱动器”的提示框后，单击该提示框，

如图 1-5。等到移动存储设备上的指示灯熄灭后，就可以拔掉该移动设备了。

安全删除 USB 移动存储设备方法 2，操作步骤如下：

- ①在系统任务栏中，双击【USB 移动存储设备图标】，如图 1-4。
- ②打开“安全删除硬件”窗口，单击【停止】，如图 1-6。



图 1-4 USB 移动存储设备图标

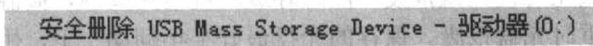


图 1-5 安全删除 USB 移动存储设备

③在弹出的“停用硬件设备”对话框中，选定停用的硬件设备后，单击【确定】，待移动存储设备上的指示灯熄灭后，就可以拔掉该移动设备了，如图 1-7。

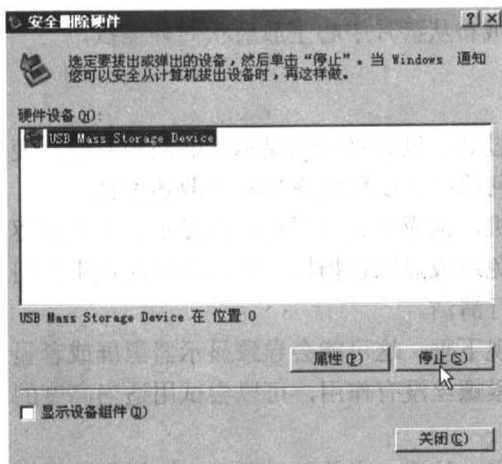


图 1-6 安全删除硬件

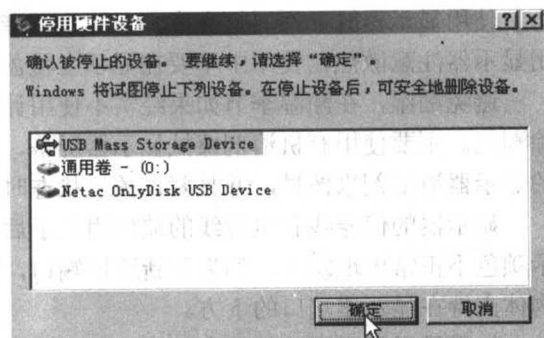


图 1-7 停用硬件设备

(3) 软盘的安全操作

软盘作为一种价格低廉的移动存储设备，在很多场合还在广泛使用。为了保证电脑安全可靠地保存数据，应该正确地使用软盘。

软盘的读写过程中，不能从软驱中取出。软盘保存时要远离磁场、电场、热源。不要用手接触软盘的读写窗口。

(4) 光盘的安全操作

光盘是一种长寿命的存储介质，理论上可以保存数据 100 年，但是很多光盘没有使用多少次就会出现不能读出数据的情况。

出现这些情况除了与光盘自身的质量有关之外，还与用户的操作有关。使用光盘中，不要用手触摸保存数据的一面（没有商标的那一面），手上的油污会造成光盘数据的损坏。不要把光盘的数据面放在任何硬物上，以免划伤数据面造成数据的损坏。

如果自己刻录光盘时，不要把光盘刻满，应该至少留 10% 左右的空间，这样将减少由于光盘边缘的损坏造成无法读写。

保存光盘时，要放在光盘盒或光盘袋中保存，避免光线照射，远离热源。光盘的存放