中国科学出版集团
新世纪书局

一学就懂的实用知识 + 一看即会的操作讲解 = 一本速通的完全学习手册

一看即会

◎ 细致教学 ◎ 经验分享 ◎ 技术指南 ◎ 应用为王

新手学电脑安全与黑客攻防

杰创文化 编著

CD

图书 + 光盘 + 附赠 = 绝对超值的学习套餐

高品质的图书
全面的功能讲解、详尽的操作步骤、实用的案例演练，三大要素完美融合

+

丰富的光盘资源
129个重点操作实例的视频教学录像，播放时间长达192分钟

+

买一送一超值附赠
畅销图书《新手学系统安装和重装》的全部视频教程

科学出版社

一看即会

新手学电脑安全与黑客攻防

杰创文化　编著

科学出版社

内 容 简 介

电脑和网络在促进经济发展、推动社会进步和提高人们的生活品质等方面发挥着越来越突出的作用，然而与此同时，网络的安全问题也变得日趋严重，各种病毒、木马和黑客攻击不断出现、花样还时时翻新，威胁着我们的电脑安全，需要引起每一个用户的重视。

本书的编写目的就是帮助新手学习电脑安全及黑客攻防的相关知识，通过简单、实用的系统安全设置、修复系统漏洞等操作，常见的黑客入侵手段介绍，以及利用 QQ 攻防、电子邮箱攻防等具体的实例演练，让读者快速掌握电脑安全设置以及防范黑客入侵电脑的方法。

全书共 15 章。第 1 章介绍电脑安全的基本知识，即为什么要注意电脑安全、电脑安全简介和常见的电脑安全技术等知识。第 2 章介绍如何为电脑设置密码，内容包括为电脑设置 BIOS 密码、账户密码，开启/关闭屏幕保护密码和电源管理密码，并且介绍了一些常用的密码设置技巧。第 3～7 章介绍了桌面、账户的安全设置，使用防火墙、修复系统漏洞，文件/文件夹及一些常用的软件的安全设置，备份与还原系统中的重要数据以及系统、上网过程中的一些安全操作等知识。第 8 章介绍在使用网上银行时应注意的一些问题以及安全操作等知识。第 9 章介绍关于病毒的基本知识，分别使用瑞星、金山毒霸和诺顿三种较为著名的杀毒软件查杀病毒及其相关设置等知识。第 10 章介绍黑客的基本知识，IP 地址和端口的基本知识及分类，黑客常用的一些 DOS 命令及手段等知识。第 11～15 章介绍黑客常用的嗅探攻击以及怎样防范嗅探攻击，远程控制，QQ 攻防、木马攻防以及电子邮箱攻防等知识。

光盘中包含播放时间长达 192 分钟的 129 个重点操作实例的视频教学录像，同时附赠了畅销图书《新手学系统安装和重装》的全部视频教程。

本书适合电脑初学者快速掌握维护电脑安全与防范黑客攻击的能力，也适合广大电脑爱好者以及各行各业需要学习电脑防御技术的人员使用，还可作为各类电脑培训学校、大中专院校的教学辅导用书。

图书在版编目（CIP）数据

新手学电脑安全与黑客攻防/杰创文化编著.—北京：科学出版社，2010.4
（一看即会）
ISBN 978-7-03-026948-5

Ⅰ.①新… Ⅱ.①杰… Ⅲ.①电子计算机－安全技术 ②计算机网络－安全技术 Ⅳ.①TP309②TP393.08

中国版本图书馆 CIP 数据核字（2010）第 039612 号

责任编辑：杨 倩 李 莉 / 责任校对：杨慧芳
责任印刷：新世纪书局 / 封面设计：锋尚影艺

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学出版集团新世纪书局策划
北京彩和坊印刷有限公司印刷
中国科学出版集团新世纪书局发行 各地新华书店经销
*
2010 年 5 月 第 一 版 开本：16 开
2010 年 5 月第一次印刷 印张：16
印数：1—5 000 字数：389 000

定价：29.80 元（含 1CD 价格）
（如有印装质量问题，我社负责调换）

前言 Preface

随着互联网技术的不断发展，信息交流更加高效、便捷，各种新的网络功能也不断涌现，网络在促进经济发展、推动社会进步和提高人们的生活质量等方面发挥着越来越重要的作用。然而与此同时，网络的安全问题也变得日趋严重，各种病毒、木马不断出现、花样还时时翻新，威胁着我们的电脑安全，需要引起每一个用户的重视。

此外，在网络中有一群被称为“黑客”的神秘人物。最早黑客是指热心于计算机技术、水平高超的电脑专家，尤指程序设计人员。但到了今天，黑客已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。作为一个有一定操作经验的电脑用户，读者有必要了解一些黑客的知识，通过模拟黑客的行为准则以及入侵网络的方式、方法，反过来发现自身存在的问题，做好防范工作，从而最终保证自己的数据信息和网络财产的安全。

本书就是为读者量身打造的快速掌握电脑安全与黑客攻防技能的实用大全，全书共15章。第1章介绍电脑安全的基本知识，即为什么要注意电脑安全、电脑安全简介和常见的电脑安全技术等知识。第2章介绍如何为电脑设置密码，内容包括为电脑设置BIOS密码、账户密码，开启/关闭屏幕保护密码和电源管理密码，并且介绍了一些常用的密码设置技巧。第3~7章介绍了桌面、账户的安全设置，使用防火墙、修复系统漏洞，文件/文件夹及一些常用的软件的安全设置，备份与还原系统中的重要数据以及系统、上网过程中的一些安全操作等知识。第8章介绍在使用网上银行时应注意的一些问题以及安全操作等知识。第9章介绍关于病毒的基本知识，分别使用瑞星、金山毒霸和诺顿三种较为著名的杀毒软件查杀病毒及其相关设置等知识。第10章介绍黑客的基本知识，IP地址和端口的基本知识及分类，黑客常用的一些DOS命令及手段等知识。第11~15章介绍黑客常用的嗅探攻击以及怎样防范嗅探攻击，远程控制，QQ攻防、木马攻防以及电子邮箱攻防等知识。有了这些知识，你就能全面认识电脑的安全隐患和黑客的真实面貌，并掌握防范黑客入侵电脑的方法；就能了解常用的DOS指令以及对应的参数，尝试使用各种DOS指令；就能自己用杀毒软件查杀电脑中的病毒和木马啦。

本书内容系统、全面，采用大量图片配合文字说明的方式对知识点进行介绍，步骤清晰、完备，保证读者一看即会！此外，在介绍操作方法时，尽量选用符合实际需求的实例，便于读者应用于实践。

本书配一张CD多媒体视频教学光盘，具有极高的学习价值和使用价值。光盘中包括播放时间长达192分钟的129个重点操作实例的视频教学录像，同时附赠了畅销图书《新手学系统安装和重装》的全部视频教程，具体使用方法请阅读下页的“多媒体光盘使用说明”。

本书由杰创文化组织编写。如果读者在使用本书时遇到问题，可以通过电子邮件与我们取得联系，邮箱地址为：1149360507@qq.com。此外，也可加本书服务专用QQ：1149360507与我们取得联系。由于作者水平有限，疏漏之处在所难免，恳请广大读者批评指正。

编著者

2010年3月

多媒体光盘使用说明
How to Use the CD-ROM

本书配套多媒体教学光盘内容包括129个重点操作实例的视频录像，对应书中各章节内容，逐步详细讲解了具体的操作步骤。读者可以先阅读图书再浏览光盘，也可以直接通过光盘学习电脑安全的维护与黑客攻防的方法。同时，为了让读者能更快地解决电脑安全问题，特别赠送了畅销图书《新手学系统安装和重装》的全部视频教程。

将配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如图1所示。单击按钮❶可进入目录浏览界面；单击按钮❷可浏览光盘中的文件。

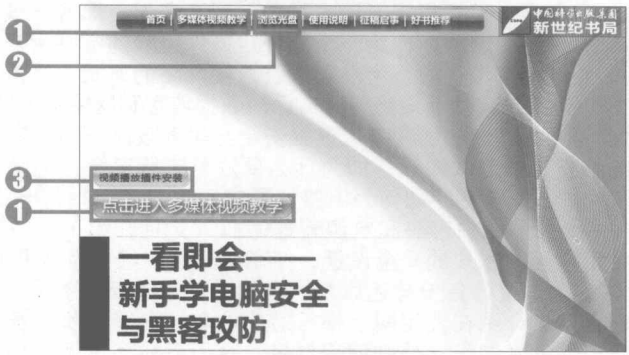


图1 光盘主界面

在目录浏览界面中单击按钮❹可打开下一级目录，包含以节标题命名的视频文件链接；单击要学习的内容，对应的视频文件将在“视频播放区”中播放，如图2所示。如果不能正常播放视频，请单击图1中的按钮❸，以安装视频播放插件。

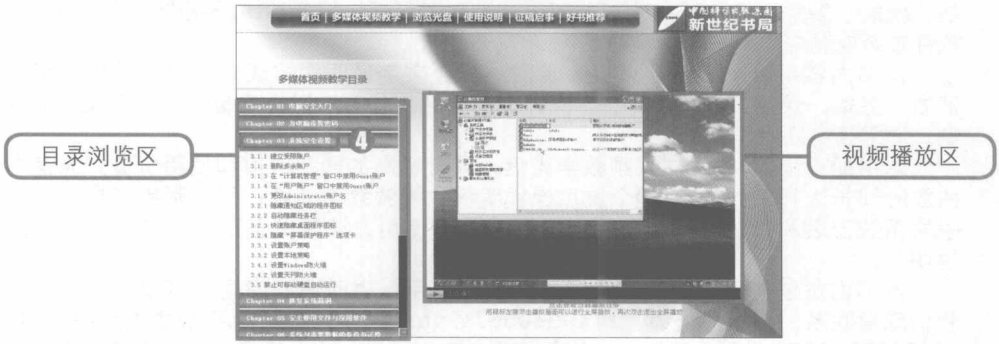


图2 播放界面

提示

如果放入光盘后没有自动运行，则在“我的电脑”中双击光驱盘符进入光盘，然后双击start.exe文件即可。

目录·Contents

Chapter 01

电脑安全入门

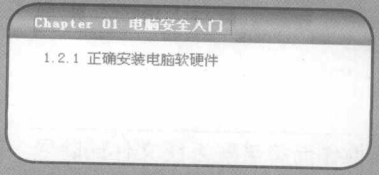
重点知识

1. 为什么要注意电脑安全
2. 电脑安全简介
3. 常见的电脑安全技术

随着科学技术的发展，电脑已经在社会生活的各个角落发挥了不同的作用，特别是互联网的推广与应用，使得人们的生活、工作、学习和交流环境逐渐发生改变，但是改变也有好有坏，好的会带来巨大的社会和经济效益，坏的则会使电脑存在危险性和脆弱性。为了能更好地使用和维护电脑，用户需首先了解电脑安全的基础知识以及常见的电脑安全技术。

视频文件

参见随书光盘：视频教程\Chapter 01



1.1 为什么要注意电脑安全

当用户使用电脑一段时间之后，许多安全问题就会不断地出现，常常出现的电脑安全问题包括误删除某些重要文件、黑客、电脑病毒和木马等。

电脑由硬件系统和软件系统组成，其中软件系统是相关的技术人员根据用户的需求进行编写的，所以在系统分析、系统设计等开发阶段中不可避免地会出现一些考虑不周的地方，对于某些大型的软件系统则很可能会出现一些软件漏洞，从而被黑客抓住漏洞进行攻击，造成电脑安全的问题，而有些电脑安全问题则是用户自己操作不当造成的，例如误删除某些重要文件而导致系统无法正常启动。下面介绍造成电脑安全问题的常见原因。

1 黑客

黑客，原意是指热心于电脑技术，水平很高的电脑专家，特别是程序设计人员，但是到了今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的人。黑客通常利用操作系统或者某些软件的漏洞来入侵和控制电脑，以偷窥他人隐私、远程控制电脑、盗取他人的资料和账户密码等重要信息。所以用户应该及时修复系统漏洞并使用最新版本的应用软件。在修复系统漏洞时可开启电脑中的“自动更新”功能，或者登录微软官方网站手动下载并安装升级补丁。

“红客”一词来源于黑客，红色在中国有着特定的价值含义，即正义、道德、进步、强大，等等。红客是一种热爱祖国、坚持正义、开拓进取的精神，因此只要具备这种精神并热爱着电脑技术的人都可称为红客。

骇客同样来源于黑客，但是这类人专门使用恶意攻击、植入木马和病毒等一系列的破坏手段来破坏他人的系统，盗取他人的账号密码或者导致其他电脑系统彻底崩溃而丢失重要数据。

2 电脑病毒

电脑病毒是指编制或者在电脑程序中植入具有破坏功能或者毁坏数据，影响电脑使用，并能够自我复制的一组计算机指令或者程序代码。由于电脑病毒具有隐蔽性和突发性，当病毒入侵至电脑中时，一般会潜伏很长一段时间，一旦时机成熟就会对系统造成破坏，严重地影响电脑的安全。因此用户可以在电脑中安装杀毒软件，而病毒的种类在不断地增加，故用户需要及时升级杀毒软件并设置开机时启动实时保护。

3 木马

木马和病毒一样，也是一段电脑程序。但是木马和病毒有着不同的地方，木马是被用来盗取其他用户的个人信息或者诱导目标用户执行该程序以达到盗取密码等各种数据资料等目的。用户可使用杀毒软件扫描并查杀电脑中存在的木马。

4 误删除某些重要文件

普通用户一般对电脑中的某些重要文件不太认识，常常由于误操作而将某些系统文件删除导致无法启动系统，例如，有些用户为了方便，常常将应用软件安装到系统分区中，当需要手动删

除某些应用程序时，一不小心就很有可能将系统分区中的某些重要文件删除。为此，用户可将应用软件安装在除系统分区外的其他分区中。

1.2 电脑安全简介

电脑安全主要包括硬件和软件两方面的安全，安装电脑硬件时需要掌握正确的安装方法，安装软件也同样需要注意选择安装的路径和安装的附件。随着互联网的推广及应用，大量的电脑病毒、木马及黑客利用系统的漏洞或者用户的疏忽进入电脑并对电脑造成不同程度的损失，因此用户应了解电脑安全方面的知识，以阻止电脑病毒和黑客的入侵。

1.2.1 正确安装电脑软硬件

电脑硬件是用户使用电脑的基础，在正确安装之前需要了解电脑可以正常运行的环境。通常电脑要放置在一个干净、通风性比较好的办公环境中，而且要满足其运行所适宜的温度、湿度和电压等要求，以保证电脑硬件能够正常、高效地运行。除此之外，应该让电脑良好的接地，即接好家里的地线和购买好的插座板或者使用导线将机箱与地相连。当电脑中存放有重要数据时，应该安装屏蔽机房或者电子干扰设备。

1 安装多条内存条

内存是电脑系统运行过程中重要的临时信息场所，它是相对于外存而言的。用户平常使用的程序，如Windows操作系统、打字软件和游戏软件等，一般都是安装在硬盘等外存上的，但如果没有内存它们是无法工作的，必须把它们调入内存中运行才能使用。我们平时输入一段文字或者玩一个游戏，其实都是在内存中进行的，就好比在一个书房里，存放书籍的书架和书柜相当于电脑的外存，而我们工作的办公桌就是内存。通常我们把要永久保存的、大量的数据存储在外存上，而把一些临时的或少量的数据和程序放在内存上，当然，内存的好坏会直接影响电脑的运行速度。

若想要扩大内存容量可通过安装多条内存条来实现，在选购内存条的时候需要注意不同型号的内存条可能会因为速度问题产生一个时间差而导致电脑经常死机，建议用户在选购内存条时最好选择同种型号的内存条。由于内存的插槽在主板上，所以也要考虑到内存条与主板是否兼容的问题。在安装内存条时需要对准内存条的缺口与主板上内存插槽中的凸块，否则会损坏内存条或者内存插槽。

2 安装一个新的硬盘

电脑中的硬盘保存了操作系统、应用软件等重要的数据信息，一旦硬盘遭到破坏，硬盘中的数据将会遭受不同程度的破坏，给用户带来巨大的损失，因此用户必须正确地操作和使用硬盘。硬盘要远离磁场较强的环境，一般情况下硬盘都是固定在主机中，用户若要安装或者拆下硬盘时，要小心，不要摔打硬盘。

当硬盘的容量所剩无几时，用户就考虑到要在电脑中安装第二个硬盘，以IDE硬盘的安装为

例，用户在安装硬盘之前需要确定主机中是否有新增硬盘的安装空间，主机电源是否能满足新增硬盘的电源需求以及是否有空闲的硬盘插头。

满足以上三个条件之后，用户还需要在已安装主机机箱内的硬盘和新购买的硬盘之间选择引导系统的主盘，一般情况下选择已安装在主机机箱内的硬盘为主盘，新购买的硬盘为从盘。接着就可将硬盘连接在主板上对应的IDE接口中，一个IDE接口最多可接两个IDE设备，安装新硬盘之前，机箱主板上的IDE接口分别连接着光驱和安装了操作系统的硬盘，此时可将两个硬盘连接同一个IDE接口，连接之后就可开始设置跳线，跳线有三种设置，即master、slave和cable select，其中master是设置为主盘，slave是设置为从盘，cable select是根据在数据线上的位置自动决定主从盘关系。用户可按照硬盘说明书或者硬盘体上的详细说明进行跳线设置。设置完毕后将硬盘装入主机机箱中，然后连接好设备的数据线与电源线即可。

安装完成之后，两个硬盘很有可能会产生盘符交错的问题。当主硬盘中只有一个分区时便不会出现盘符交错的问题，而如果主硬盘中有至少两个分区时，就很有可能产生盘符交错，即将主硬盘的主分区默认为C盘，而新安装硬盘的主分区设置为D盘，然后依次排列主硬盘和新安装硬盘中的其他分区，这样一来就会导致除C盘以外的其他分区无法正常使用。用户有两种方法来解决该问题，一种方法是对新安装的硬盘进行重新分区，并且在分区的过程中将所有分区都设置成扩展分区；另一种方法是在BIOS设置界面中的“Standard CMOS Features”选项中将第二硬盘的IDE设置为None。

3 正确放置显示器

在使用完电脑之后应当关闭显示器。由于现在大多数的显示器都具有DPMS（显示器电源管理）功能，即在主机关闭之后，显示器能够长时间保持节能方式，但是长时间使显示器处于开启状态会使显示器的消磁电路无法对显示器进行消磁处理，从而使显示器屏幕因长期得不到消磁而造成偏色现象。

在使用显示器时，应尽量让其处在通风性较好的位置并且还要注意防潮。显示器正在运行时不要遮住其通风孔并且不要在上方放置任何东西，否则会因无法散热而造成显示器内温度过高；在放置显示器时应尽量使其保持平衡，不要放在沙发、床等比较软的物体上；若放置显示器的环境比较潮湿，需要做好防潮措施，即在显示器旁放置一个风扇或者食品包装袋中的防潮剂。不能将水或者其他液体滴入显示器内，否则会影响显示器的正常工作或者损坏显示器；不要用带有腐蚀性或者导电性液体的布料品擦拭显示器屏幕，只能用较干的布或者专用的电脑清洗剂来擦拭，并且在擦拭之前一定要确保电脑处于关闭状态，为了安全，建议用户切断电源。

4 正确使用USB可移动设备

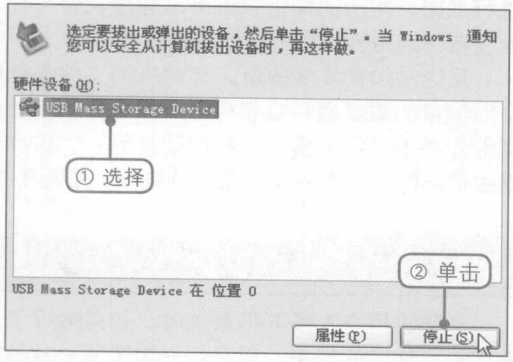
USB的全称是Universal Serial Bus，中文含义是“通用串行总线”。USB是一个外部总线标准，用于规范电脑与外部设备的连接和通信。USB接口支持设备的即插即用和热插拔功能。而USB接口的移动硬盘不仅容量大，而且携带方便，用户在携带或者使用时不要损坏该设备，否则将会导致该移动硬盘内的数据无法读出或者根本无法识别。另外，用户在使用移动硬盘时，直接将其连线与机箱的USB接口相连接即可，系统会自动检测到新硬件并识别。USB接口虽然支持热插拔，但是建议用户在取走移动硬盘时按照如下的步骤进行。

① 单击“安全删除硬件”命令

当用户想要安全取走移动硬盘时，①在桌面上的通知区域中右击图标。②在弹出的菜单中单击“安全删除硬件”命令。

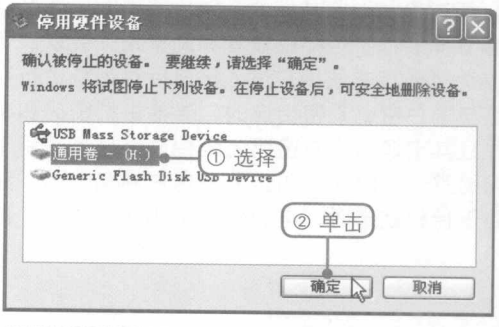
② 选择要拔出的设备

弹出“安全删除硬件”对话框，①在硬件设备中选择USB Mass Storage Device选项。②单击“停止”按钮。



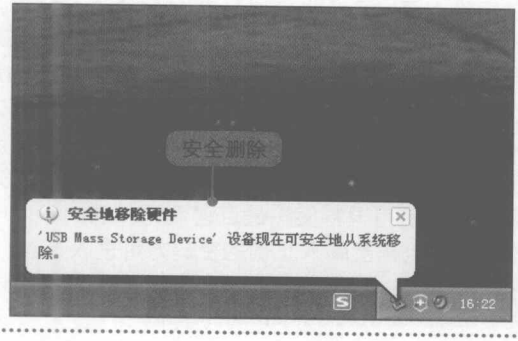
③ 停用硬件设备

弹出“停用硬件设备”对话框，①在列表框中选择“通用卷－（H：）”选项。②单击“确定”按钮。



④ 安全删除

此时在桌面右下角的通知区域中即可看见“安全地移除硬件”提示信息。



5 正确安装应用软件

用户不仅要能正确地安装某些硬件，而且也要掌握安装应用软件的技巧。如果需要在网站上下载安装软件，那么在选择下载网站时，一般都是直接登录该软件对应的官方网站进行下载，若登录其他网站有可能会下载到带有病毒或者木马的安装软件。成功下载安全的安装软件后，在安装时也要注意技巧，有些安装软件会带有一些附加的软件使其一起安装，例如在安装某些应用软件时会询问用户是否安装Google工具栏，若不仔细就直接将其安装至电脑中了，所以在安装软件过程中需要看清楚后再操作，一般建议用户将应用软件安装在除系统分区之外的其他分区中，否则当用户重装系统后系统分区中的应用软件都会被格式化。

1.2.2 对重要数据要多重保护

电脑中的数据一般都存放在硬盘中，其中也包括重要的数据，将重要数据存放到硬盘后，需要对这些数据做好多重保护。可直接在“我的电脑”窗口中将其隐藏；若觉得该种隐藏法不够安全，则可以使用WinRAR压缩软件将重要数据进行加密压缩；也可以使用第三方软件对重要数据进行加密，常用的加密软件有高强度文件夹加密大师和万能加密器。加密之后用户也可使用操作系统自带的备份工具将重要数据进行备份。

无论是加密或者备份，其对应的文件都是放置在硬盘中，但是硬盘并不是完全安全的，可能会因硬盘的磁道损坏或者病毒入侵等原因而造成重要数据的丢失。因此用户可将重要数据存储到其他介质中（如光盘、可移动硬盘等），这样一来就可确保重要数据的安全性，当电脑中的数据发生损坏时，可直接使用备用的数据，不至于造成很大的损失。

1.2.3 保障系统安全

当非法用户入侵电脑系统时，如果做好了系统的安全措施则不会造成很大的损失，否则将会造成不可估计的损失，因此用户需要通过各种措施来保障系统的安全，例如为系统设置不同的密码、对系统的安全进行相关的设置、及时修复系统漏洞等。

1 为系统设置密码

用户可以在系统设置BIOS密码、账户密码、屏幕保护密码和电源管理密码。BIOS密码是用来防止非法用户进入BIOS并肆意篡改其设置的，在BIOS密码中又可分为普通用户密码和超级用户密码，使用普通用户密码进入BIOS设置界面后，只能查看和浏览其相关设置，并不能设置其中的某些重要属性，而使用超级用户密码进入BIOS设置界面后，不但能够查看和浏览相关设置，而且还可以对BIOS的所有属性进行更改；账户密码则是为了防止非法用户进入桌面后对系统进行盗取或者破坏操作；屏幕保护密码和电源管理密码均是与账户密码紧密相连的，屏幕保护密码和电源管理密码只有在设置了账户密码的情况下有效，并且其密码与账户密码完全相同，只是适用于不同的情况，屏幕保护密码适用于用户暂时离开电脑的那一段时间，防止非法用户偷窥电脑，液晶显示器使用屏幕保护是百害而无一利的；当电脑处于待机状态时，电源管理密码即可生效，再次启动时则需要输入正确的密码方可进入桌面。

2 设置系统安全

当一台电脑并非一个人使用时，就需要在操作系统中建立一些除管理员账户外的其他账户，而Windows系统拥有比较完善的系统用户权限管理功能，用户可以以管理员的身份创建各个权限不同的账户，这样其他用户就无法访问系统中一些特定的数据或者文件，从而保证了特定数据的相对安全。用户可在桌面上进行一系列的安全设置，例如隐藏通知区域中的程序图标、自动隐藏任务栏、快速隐藏桌面程序图标或者隐藏“屏幕保护程序”选项卡等。为了进一步的安全，用户可进入本地安全策略中设置账户策略和本地策略，用户还需要开启并配置Windows防火墙或者使用其他防火墙来保护系统，如天网防火墙。

3 修复系统漏洞

当选择了一款操作系统时，该操作系统不可避免地存在一些漏洞，一些黑客往往会利用这些