施　容　等编著

电脑安全靠自己

电脑应用靠自己丛书

机械工业出版社
CHINA MACHINE PRESS

电脑应用靠自己丛书

电脑安全靠自己

施　容　等编著

机械工业出版社

电脑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是令人始料不及的。本书针对具有一定电脑应用技能的读者，系统地介绍了在使用个人电脑时用到的数据恢复、病毒与木马的查杀、防止黑客入侵的方法和技巧。书中通过一些典型实例，指导读者全面应对电脑安全事故，将损失降到最低程度。书中设计了一系列小任务，如“想一想”、“显身手”等，通过这些启发性的活动帮助读者在实践中学习。

如果读者对电脑病毒、黑客、系统崩溃、硬盘数据丢失还不以为然，本书可以为读者敲敲警钟，会使读者从现在做起，牢固树立安全第一的思想；如果读者曾经遇到过一些小的安全事故，但并未对读者的工作造成很大的影响，本书应该是个不错的选择，因为它可以使读者保持清醒头脑，为日后安全使用电脑打好基础；如果读者有过有关电脑安全问题的惨痛教训，那更应该看看本书，或许今后读者就能应用所学到的知识防患于未然，正确处理各种灾难事故。

图书在版编目（CIP）数据

电脑安全靠自己/施容等编著. —北京：机械工业出版社，2003.5
（电脑应用靠自己丛书）
ISBN 7-111-12161-9

Ⅰ. 电… Ⅱ. 施… Ⅲ. 电子计算机—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2003）第 037273 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：车　忱
责任印制：路　琳

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2003 年 6 月第 1 版第 1 次印刷
787mm×1092mm　1/16 · 11.5 印张 · 284 千字
0001－5000 册
定价：18.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、88379646
封面无防伪标均为盗版

出 版 说 明

目前，电脑技术涉及的领域越来越广、内容越来越多、发展越来越快，所以，仅凭一些陈旧的电脑技能很难跟上时代的发展。要适应 IT 的发展，知识更新尤为重要，这也要求每个热衷电脑学习的朋友改变传统的学习方式和方法。

当今的时代是个性化、人性化的时代，学习电脑更是因人而异。那种传统的“言传身教”的学习方式在很大程度上已经不能适应目前的状况。近年来，一种“自助式”的学习思路正呈现出其优越性。它的基本思想表现在两个方面：一是“相关知识的学习”，即自己不断实践，在无数成功和失败中“悟”出一套适合个人的学习方法和技巧；二是“解决问题的能力培养”，即培养实际分析问题、处理问题的能力。

为适应时代需求的变化，我们组织编写了这套“电脑应用靠自己”丛书。本丛书总体遵从循序渐进、经验与技巧相结合的原则，适用于不同层次的读者及同一层次的读者在不同学习阶段的需要。

本套丛书从最基本的常识入手，力求用通俗、浅显、轻松、明快的语言和编写形式帮助读者在其指导下展开自学活动，达到在实际学习和工作中独立分析和解决问题的目标。

对于电脑新手，本套丛书从必备的基础操作和基本常识入手，使得读者能够轻松入门，快速上手；对于有一定基础的朋友，可从中得到有关电脑的最新知识，掌握实用技术和应用技巧。更为重要的是，丛书通过设立一系列启发性栏目引导读者，达到融会贯通、熟练运用的目的。

在信息时代，电脑技术已经是人们生产和生活的必备技能。只要学习方法得当，刻苦勤奋，善于摸索，年龄大小和电脑知识基础的差异都不会成为障碍。有了本套丛书的帮助，相信会有更多的读者在学习电脑知识的过程中体验到快乐。

机械工业出版社

前　言

从本质上讲，电脑是一个十分脆弱的系统，它在进行数据的处理、存储、传输时往往存在安全隐患，数据很容易被干扰、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。自从 Internet 流行以来，电脑安全更是一个必须高度重视的话题。然而，至今仍有很多用户错误地认为“电脑安全就是杀毒”，其实电脑安全涉及的范围正在前所未有地拓展。

国际标准化组织（ISO）将“计算机安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”此概念偏重于静态信息保护。也有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。可见，电脑安全的内容应包括两方面：即物理安全和逻辑安全。物理安全指系统及相关设备受到物理保护，免于破坏、丢失等。逻辑安全包括信息完整性、保密性和可用性。为了让广大用户了解病毒和其他侵害给电脑造成的危害，了解电脑安全的主要内容，逐步普及电脑安全意识，共同推动电脑及网络健康有序地发展，我们结合多年的实践组织编写了本书。

本书以初级读者为主要对象，以“靠自己”为目标。系统介绍了电脑安全常识、电脑病毒及防治、网络安全、系统安全、硬盘数据安全和密码安全等方面的内容。全书共分为 8 章，第 1 章介绍了电脑安全的基本常识，使读者树立最基本的安全意识；第 2 章剖析了电脑病毒的机理和特性，读者可以加深对电脑病毒本质的认识，从系统的高度树立防范和检测病毒的意识；第 3 章通过大量实例详细介绍了电脑病毒的清除方法和技巧，比较深入地介绍了主流杀毒软件的高级应用；第 4 章介绍了上网安全的基础知识，分析了网络入侵的有关问题；第 5 章介绍了防电脑黑客的实用方法和技巧，强调了个人上网用户的安全防范策略；第 6 章介绍了硬盘数据的安全威胁和拯救数据的具体攻略；第 7 章以 Windows 操作系统为例，介绍了系统安全的具体方法和技巧；最后一章介绍了密码设置的技巧和遗忘密码的解决办法。

本书力求以新颖别致的形式使读者轻松而快速地掌握电脑安全设置的基本方法和技巧，正文中穿插了“专题苑”、“小锦囊”、“想一想”、“显身手”、“技能沙龙”等特色栏目，旨在帮助读者扩展视野，借鉴技巧，边学边练。对于一些疑难问题，还采用了“指明灯”栏目予以必要的提示。

本书由眼界资讯组织编写并审定，全书由施容、陈德荣、丰世明、荣璧琼、卢晓佳、阙晓玲、罗光飞、唐明编写。

由于时间仓促、作者水平有限，本书错漏之处在所难免，敬请广大读者批评指正。

编　者

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第1章　电脑安全基本常识

本章导读

普通用户在使用电脑时，往往对病毒、黑客、系统崩溃、硬盘损坏等在思想上认识不足，技术准备也不充分，当出现问题时束手无策。此外，对文档、邮件和一些特殊软件的加密手段十分低劣，一些重要数据、账号的泄密事件时有发生，忘记密码后也毫无办法。本章将面向个人电脑用户，介绍电脑的不安全因素，提出电脑安全靠自己的观点，使读者明确本书的学习内容。

学习建议

在学习本章时，建议读者先回忆一下自己在使用电脑时曾经遇到过的各种不安全事件，加强安全防范意识，然后参考有关报刊杂志和网上的信息，初步弄清电脑可能会导致哪些安全问题，并了解一些最基本的防范手段。

此外，在学习过程中，要注意“想一想”和“显身手”等小栏目提供的训练，其中加了“*”号的题目在本章最后的“指明灯”中给予了必要的提示。

主要知识点和技能项

- 电脑不安全因素
- 用户安全管理
- 上网安全
- 系统安全
- 安全靠自己
- 硬盘维护

1.1 电脑危机四伏

长期以来，电脑病毒、文件误删除、黑客和恶意程序等安全问题都困扰着人们。如何让系统更加坚固？如何让数据更加安全？这些都是摆在所有用户和安全专家们面前的问题。

个人电脑普及到家庭以后，电脑安全问题已受到了大众的关注。对于初级用户来说，当学会了电脑的基本操作以后，最头痛的就是安全问题。死机和病毒的侵害、数据的丢失和网络问题都是我们时刻面临的威胁。因此，有必要对电脑安全的各个方面给予充分的注意，维护系统的正常运行。

目前，对计算机信息系统的违法犯罪行为及攻击的主要手段有以下几类：

1．越权存取

战争期间，敌对的国家既要防止本国计算机中机密数据被他人越权存取，又要千方百计窃取别国计算机中的机密。在冷战结束后，各情报机关不仅继续收集他国政治、军事情报，而且将重点转到经济情报上。

在金融电子领域用计算机犯罪更加容易，更隐蔽。犯罪金额增加 10 倍，只不过在键盘上多敲一个“0”。例如，深圳招商银行证券部电脑管理员孙某利用电脑作案，1993 年 12 月至 1994 年 4 月挪用公款和贪污资金 880 万元人民币，被判处死刑缓期执行。

2．黑客

采取非法手段躲过计算机网络的存取控制、得以进入计算机网络的人称为黑客。尽管对黑客的定义有许多种，态度褒贬不一，但黑客的破坏性是客观存在的。黑客干扰计算机网络，并且还破坏数据，甚至有些黑客的“奋斗目标”是渗入政府或军事计算机获得其信息。有的黑客公开宣称全世界没有一台连网的计算机是他不能渗入的，美国五角大楼的计算机专家曾模仿黑客攻击了自己的计算机系统 1.2 万次，攻击成功率为 88%。

3．计算机病毒

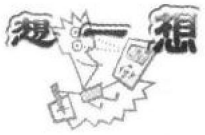
计算机病毒，是指编制的或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。由于传染和发作都可以编制成条件方式，像定时炸弹那样，所以计算机病毒有极强的隐蔽性和突发性。目前，病毒种类越来越多，主要在 DOS、Windows、UNIX 等操作系统下传播。1995 年以前的计算机病毒主要破坏 DOS 引导区、文件分配表、可执行文件，近年来又出现了专门针对 Windows、文本文件、数据库文件的病毒。

4．有害信息

这里所谓的有害信息主要是指计算机信息系统及其存储介质中存在、出现的，以计算机程序、图像、文字、声音等多种形式表示的，含有恶意攻击党和政府，破坏民族团结等危害国家安全内容的信息，以及含有宣扬封建迷信、淫秽色情、凶杀、教唆犯罪等危害社会治安秩序内容的信息。目前，这类有害信息基本上都是来自境外，主要形式有两种，一是通过国际互联网（Internet）进入国内，二是以计算机游戏、教学、工具等各种软件以及多媒体产品（如 VCD）等形式流入国内。目前计算机软件市场盗版盛行，许多含有有害信息的软件就混杂在众多的盗版软件中。

此为试读，需要完整PDF请访问：www.ertongbook.com

*（1）合法用户进行越权存取是否应该限制？
（2）什么是黑客？黑客是否都具有破坏性？
（3）计算机病毒能不能破坏文本文件？
（4）电脑有害信息主要来源于什么地方？



1.2　用户安全管理

无论是个人用户还是公用机房，每个人的电脑里都或多或少有一些私人的资料或者公司的重要文件，不希望太多的人访问。

如果是单机用户，通常可以将重要的文件压缩加密，以防止自己不在的时候文件被别人偷看。如果觉得不放心，还可以对注册表进行修改，彻底隐藏某个分区，不熟悉情况的人完全看不到。当然最好是在 BIOS 中设置开机密码，使没有经过授权的用户不能启动系统。此外，还应注意以下几点：

1. Windows 内置多用户管理

对公用计算机来说，应根据需要，将用户级别进行严格限制。在 Windows 系统中有比较完善的系统用户权限管理功能，可以按照超级用户的指定给每个用户以不同的权限。这样，某些用户就无法访问一些敏感数据或文件，从而保证了公司的机密不被外人知道。当然，这些手段使用以后也不能说完全截断了机密泄露的途径，更多的还是要通过平时的严格管理，杜绝这种危害甚大的系统安全问题。

2. 让硬件更加稳固

硬件是电脑系统的骨架和基础。因此，硬件工作的稳定是系统稳定和安全的最基本保障。试想，如果硬盘损坏，那么全部数据都会损失殆尽，这是无论用多少金钱都换不回来的。构成电脑硬件的主要元件是硅芯片和电子元件，因此，一些通用的维护技巧是必须掌握的。比如保证正常的温度和湿度，保证一定的通风，避免阳光直射，在不使用电脑时盖上罩子以免灰尘进入，避免将有强磁场的电器如电视机等放在电脑旁边等。除此之外，一些具有特殊要求的部件如 CPU、硬盘等，更应该细心地呵护。

3. 将病毒拒之门外

病毒危害系统安全的最主要途径是利用计算机软件。时至今日，人们已经知道的计算机病毒已经超过 3 万种。根据它们感染的对象不同，人们又把病毒分为引导型病毒和文件型病毒，前者主要危害分区表等系统关键数据，使系统无法启动、数据几乎全部损坏；后者则对重要的程序、数据和文档产生致命的破坏，使花费大量时间积累的数据无法读取或完全损坏。

4. 来自互联网的威胁

目前网民数量越来越大，网络已经深入日常生活。不过，在上网的用户中，由于自身的疏忽，被攻击和被感染的比例也非常大。经常看到很多用户在上网时出现无故死机或数据丢失等情况。由于网络是一个开放的环境，很难对制造这些行为的人给予打击。能够做的，只能是搞好自身的安全措施，尽量减少危害系统安全的因素。

对普通用户来说，使用防火墙是必须的、也是最简便的安全保护措施。通过规则的制订，可以过滤出对自己不利的因素。同时，还需要针对具体的网络应用程序进行修改，如 IE 和邮件收发等。只有准备工作充分，才能保证这些程序的正常使用。

5. 数据备份的必要性

计算机中的数据是指一切存储在计算机中的信息。而数据备份，就是将这些文件通过手动或自动的方式复制到一个安全的地方，以备不时之需。对于商业用户来说，数据备份是必须的，就像每天吃饭那么平常；普通用户也应该尽量备份数据，因为这是很重要的一步。

6. 避免数据损失

数据平时是存储在硬盘上的，但硬盘上的数据并非绝对安全，可能会因磁道损坏或病毒侵害等原因而丢失。尽管对系统做了各种优化和维护工作，但并不能百分之百地保证系统不出问题。如果硬盘上存储有重要文件，一定要备份到其他介质（如光盘）上。这样在数据发生损坏时，才不会手足无措。

（1）在哪些场合下宜使用多用户管理？使用多用户管理有哪些好处？

（2）为什么硬件的质量和日常维护对电脑安全有一定的影响？

（3）为什么 Internet 是最大的安全隐患之一？

（4）什么是数据备份？主要的备份对象有哪些？

试为你的电脑设置多个用户和密码，按用户级别进行权限限制。

1.3 网络风险

作为一个网络新手，面对网络的种种安全问题，应该怎么办呢？总不能因为惧怕黑客和不安全的事件发生而不上网，或者公司不使用网络，因为网络能带来许多的实惠和方便。

1. 对付病毒

电脑病毒是最具危害性的。病毒可以拒绝服务、损坏数据、把 PC 变成“公用”。绝大部

分病毒都是用汇编语言编写的，因为汇编语言是一种低级的语言，所以它编写出来的都是很小的程序。

病毒对网络安全是一个特殊威胁，因为当病毒被释放到网络中的时候，根本无法预测它的扩散能力有多么强。Internet 是最适合病毒传播的环境。所以作为 Internet 用户就必须学习或了解病毒的基础知识。

2. 特洛伊木马

特洛伊木马是包含在合法程序里的未授权程序。未授权程序可能在执行的时候不为人所知。可以肯定地说，目前被木马感染的机器大多是因为用户下载别的程序的时候，在不知情的情况下运行了木马，因为木马会被“有心者”捆绑在另一个用户想得到的程序里，这是很难发现的，也是意想不到的。被感染后的机器说得确切一点就是变成所有人的公用机器了，比网吧的机器还更“公用”，机器里所有的东西包括完全属于自己的密码将被别人窥视到，更可恨的是，会有人恶意地添加一些有害的文件在电脑上。

对于特洛伊木马可以从以下几个方面防范：

1）装一个能查杀目前已知木马的防火墙或者杀毒程序；

2）随时查看自己的网络开放端口；

3）随时查看与网络的连接，及时过滤掉非法的连接；

4）别完全信赖和依靠防护工具；

5）最重要的是多多少少了解一点关于木马的知识；

6）下载软件时最好要注意软件的原始大小，防止被人捆绑木马。

3. 口令的安全

经常有人说密码被人盗了、个人主页被人黑了等等，这就涉及口令安全这个敏感话题。那么怎样的口令才是安全的呢？可以说，没有绝对安全的口令。有人说在密码里出现#・¥*^~%等这类字符的是安全的，事实并非如此，因为一般的黑客字典里这些字符都是有的。如果真要想用特殊字符来掩饰口令的话，可以用◇◤♗⊙■十〒┣■ぞ这样的字符（目前有少数软件支持）或者汉字来做口令，但可能黑客字典也会加上它们，只不过是增加了破解难度和时间。

想要自己的口令相对安全，口令必须是至少 8 个字符长度，其次必须包括大小写、数字字母和控制符，不要用太常见的数字和字母做口令，最重要的是密码配上 1～3 个月要更换一次才算得上安全。因为这类口令一般是不会被玩闹者破解的，而大多高手也不会乐于破解一个毫无意义的个人口令。

1.4　安全靠自己

防毒、反黑不能完全依靠反病毒软件和防火墙之类的产品，因为反病毒软件总是走在病毒的后面。电脑的安全问题不仅仅与系统本身的安全有关，而且还与用户的安全意识有很大的关系。

1. 防毒意识

计算机病毒和生物病毒有个共同的特点，那就是具有传染性和破坏力。自从 20 世纪 50 年代第一个病毒雏形“磁芯大战”问世以来，短短的几十年时间内，病毒的种类发展到了上万种。其中，有破坏力非常强、能够直接对硬件产生损伤的 CIH 病毒；有耗费系统资源的蠕虫病毒；也有恶作剧式的小病毒。这些病毒通过多种途径传播，对计算机安全造成了很大的威胁。作为一名普通的 PC 用户应注意以下几个方面：

（1）不要使用来历不明的软盘或移动存储器。

（2）不轻易打开来历不明的邮件附件，如果收到了某些带有病毒的垃圾邮件，可以在 Outlook Express 中设置拒收。

（3）不要使用任何解密版的盗版软件，盗版者不可能全面考虑因为解密而产生的任何后果，更无法保证破坏了原软件完整性的盗版软件自身的干净和无毒，他们无需承担任何责任和风险。

（4）对于联网的计算机，在上网的时候尽量不要访问没有安全保障的小网站；对于使用 QQ 等聊天工具的人来说，不要随便打开陌生人发来的链接，不要随便接受陌生人传过来的文件或程序，这些都是病毒传播的主要渠道。

（5）对于局域网内的计算机，尽量不要开放共享文件夹。如果实在要开，也应该设置密码，以便使自己信得过的人才能访问，而大量无关人员则无法访问，这样就大大减小了病毒的传播机会。

（6）正确使用杀毒软件。

（7）使用病毒防火墙。

2. 防黑意识

黑客威胁着不少用户的安全，如何才能防止黑客入侵呢？作为一名普通用户应注意以下几点。

（1）不要在聊天室公布自己的重要邮箱，因为在聊天室中很有可能就有黑客，一旦让黑客知道了，邮箱就随时可能有危险。

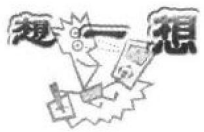
（2）最好不要在公用机上收发电子邮件，因为这样很有可能导致密码丢失。

（3）不要使用“记住密码”功能，有不少用户为了方便，总爱让程序记住密码，这样会大大地降低解密的难度。

（4）定时使用扫描程序扫描系统漏洞，并安装上补丁，减少黑客入侵成功的机率。

（1）为什么电脑安全还要靠自己呢？

（2）病毒是电脑安全的主要威胁之一，作为普通用户应该如何防毒呢？



1.5　操作系统的安全

操作系统是平时使用的基本平台，各种文件操作和具体的应用软件都离不开它。不过，由于操作系统牵涉的方面太多，其安全性问题也相对突出。以最常见的 Windows 系列操作系统为例，每隔一段时间，微软都会发布一个系统补丁，以弥补系统中的漏洞。但即使是这样，仍然有相当多的系统漏洞和 BUG 不能完全解决，这也成了黑客软件攻击的目标，同时也增加了在平时的使用中出错的几率。

对于普通用户来说，系统漏洞只有依靠官方补丁程序进行解决。补丁程序可以在一定程度上增加系统的安全性。

如果要想对系统情况有全面的了解，可以使用一些第三方软件来进行检查和补救。

东方卫士系统漏洞专杀工具就可以对系统进行安全性检查，这个工具将检测如下内容：隐藏在注册表中的自动运行程序、系统中的不安全共享、网络漏洞、由 Word、IE 以及 Outlook 等引起的安全隐患。对于普通用户来说，功能已经足够。

检查完毕，该软件会自动给出报告，说明发现多少个漏洞，如图 1-1 所示。

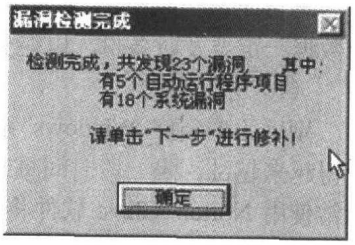


图 1-1　漏洞检测报告

这时需要点击“下一步”，对系统找出的漏洞进行修补，特别是网络安全漏洞，一定要保证全部修复，才可以保证系统在上网时不会被侵害。

1.6　硬盘的维护

硬盘维护的范围最广泛，同时也是最容易出现问题的硬件。由于硬盘是大多数数据的第一存储介质，它的好坏，直接影响到整个系统的数据安全。因此对它的维护也特别重要。

1．防止忽然断电

硬盘进行读写操作时，处于高速旋转状态中，目前主流硬盘转速都是每分钟 7200 转。如果在硬盘高速旋转时忽然关掉电源，将导致磁头与盘片猛烈磨擦，从而损坏硬盘。因此，在关机时，要等到硬盘指示灯完全熄灭以后，确定硬盘已经停止工作了再关掉电源，否则长久下去对盘片会有很大的伤害。

2．防止硬盘受震

硬盘是十分精密的设备，工作时，磁头在盘片表面的浮动高度只有几微米。不工作时，磁头与盘片是按触的。硬盘在进行读写操作时，一旦发生较大的震动，就可能造成磁头与数据区相撞击，导致盘片数据区损坏或划盘，甚至丢失硬盘内的文件信息。因此，我们在安装硬盘的时候，一定要将螺丝上紧，确保不会因为固定力量不够而使得硬盘发生震动，否则长此下去，容易使盘片发生物理损坏。在电脑工作的时候，千万不要挪动机箱，那样会使工作中的硬盘受到损坏。

3. 硬盘的整理

硬盘的整理包括两方面的内容：一是磁盘错误的扫描和修复，二是硬盘碎片的整理。由于软件的频繁装卸和使用时间的增加，硬盘不可避免地会产生一些逻辑或物理上的坏磁道，因此有必要每隔一段时间对硬盘进行一次扫描，发现了坏道以后要及时处理，能够修复的逻辑坏道要尽快修复，不能修复的物理坏道要单独划到一个分区中，不要再使用，以免坏道扩大，造成更大的损失。

硬盘在使用一段时间后，由于文件的反复存放和删除，往往会使许多文件，尤其是容量较大的文件在硬盘上占用的扇区不连续，碎片过多，这会极大地影响硬盘的速度，甚至造成死机或程序不能正常运行。因此，需要运行“磁盘碎片整理程序”对硬盘进行整理。要注意的是，整理的频率不能过于频繁，否则容易损害硬盘。

4. 防患于未然

备份是减少损失的最好方法。一般来说，并不是所有的数据都需要备份。但是，一些重要数据一定要及时备份，以避免大的损失。

（1）系统备份

别以为安装好 Windows 系统后就可以一劳永逸，因为随着各种应用程序的增多，系统会变得越来越乱，隔一段时间重装系统几乎是必须的。为了节约重装 Windows 所花费的时间，通常使用 Norton Ghost 软件将刚刚装好的系统做一个“克隆”，这样在系统崩溃以后，就可以在 10 分钟内恢复所有的系统数据。

（2）“我的文档”备份

“我的文档”里存储了长久以来积累的资料、项目档案、数据库等等，所以重新安装系统前进行文档备份非常必要，也非常重要。

重新安装好操作系统后，右键点击“我的文档”选择“属性”，在“移动”里面可以进行“我的文档”的重定向，指向先前备份的“我的文档”的目录即可。

如果经常需要重新安装操作系统，完全可以把“我的文档”整个文件夹拷贝到 C 盘以外的分区，每次重装系统后把“我的文档”属性里的指向修改一下即可。

（3）QQ 备份

如果打算只备份 QQ 消息数据，如聊天记录、用户信息以及系统消息等，那就比较简单。可以用拷贝的方法进行备份。

一般来说，可以在 C:\program files\Tencent 目录下找到安装文件及聊天资料等信息，只需把这个文件夹整个复制到其他分区即可完成备份。由于 QQ 属于绿色软件，所以在新系统下不需重装也可以直接运行备份 QQ。对于覆盖安装 QQ 的用户，一定要注意两次安装的目录都应该是同一个，否则聊天记录将丢失。

（4）邮件备份

邮件可能是网上应用最多的服务了。通常每个人都有好几个邮箱，对那些在线收发邮件的用户来说，备份的意义不太大。但是对于使用客户端软件收邮件的时候，邮件备份是十分必要的。

（5）收藏夹备份

对于使用 Windows 系列操作系统的用户来说，IE 是最经常使用的上网工具。对于一些使

此为试读，需要完整PDF请访问：www.ertongbook.com