计算机常用工具软件实用教程

辽宁省高等学校计算机基础课教材编委会／组编

祁瑞华　杨岚／主编

大连理工大学出版社
大连理工大学电子音像出版社

计算机常用工具软件实用教程

辽宁省高等学校计算机基础课教材编委会　组编

主编　祁瑞华　杨　岚

编著　王剑峰　郑旭红
　　李富宇　何素艳

大连理工大学出版社
大连理工大学电子音像出版社

计算机常用工具软件实用教程

祁瑞华　杨　岚　主编

大连理工大学出版社
大连理工大学电子音像出版社　出版

地址：大连市凌水河　邮政编码：116024

电话：0411-84708842　传真：0411-84701466　邮购：0411-84707961

E-mail：dzcb@dutp.cn　URL：http://www.dutp.cn

大连业发印刷有限公司印刷　　大连理工大学出版社发行

幅面尺寸：185mm×260mm　印张：19.25　字数：442千字

2005年8月第1版　2005年8月第1次印刷

责任编辑：王影琢　　责任校对：王晓玲

封面设计：宋　蕾

ISBN 7-900670-59-9　　定　价：29.00元

前　言

在计算机的普及程度日益提高的今天，计算机的应用已经深入到生活的各个方面。但很多用户还只是简单使用计算机的一般功能，对计算机使用和维护中用到的常用工具软件不了解，不能独立胜任计算机的一般维护，使用计算机过程中碰到的简单问题还是要求助于专业人员。实际上，大多数的计算机常用工具软件使用方便，只要掌握了其使用方法，会大大提高学习、生活的效率。

为了帮助一般计算机用户快速掌握常用工具软件的使用方法，我们编写了本书。本书是一本计算机常用工具软件的普及类教材，主要介绍日常工作与生活中最实用、最流行的计算机工具软件。全书共13章，包括：计算机病毒防治工具、防火墙工具、汉化翻译工具、多媒体工具、文件压缩工具、图形浏览截取工具、文件上传下载工具、网络联络工具、数据恢复与光盘刻录工具、文档阅读工具、系统优化工具、系统备份工具和系统分析评测工具。书中对这些工具软件的主要功能、操作使用的方法与技巧等，都给出了详细的说明。本书在介绍工具软件使用的同时还介绍相关知识，使读者深入了解该软件的有关理论基础，有利于举一反三的使用同类软件。

本书语言通俗易懂，适合作为大专院校的计算机常用工具软件等课程的教材，也可以作为计算机使用者和爱好者自学的教材和参考书。

本书的第一、二章由祁瑞华编写，第四、五章由郑旭红编写，第六、七章由王剑峰编写，第八、九章由杨岚编写，第三、十章由何素艳编写，第十一、十二和十三章由李富宇编写。

由于本书涉及的内容较广，作者水平有限，书中难免会有疏漏之处，敬请广大读者指正。

编　者

2005年8月

目　录

第 1 章　计算机病毒防治工具

如今，计算机病毒的传播范围越来越广泛，计算机病毒的传播手段也日益多样化：从传统的软盘、光盘，到今天的网络和日益普及的数码产品，都成为计算机病毒的载体。计算机病毒的破坏程度加大，使每一台计算机都受到来自计算机病毒的潜在威胁，甚至有的计算机已经感染了病毒。

实际上，计算机病毒并不神秘，只不过是一些程序，如果我们了解计算机病毒的原理和特点，掌握了一些防治计算机病毒的基本措施，安装了相应的防杀病毒软件，就可以防范和清除计算机病毒。

1.1　计算机病毒的基本概念

1.1.1　什么是计算机病毒

计算机领域引入“病毒”的说法，只是对生物学病毒的一种借用，用以形象地刻画这些“特殊程序”的特征。在《中华人民共和国计算机安全保护条例》中，对计算机病毒的定义如下：计算机病毒，是指编制、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。

简单地说，计算机病毒是一种特殊的危害计算机系统的程序，它能在计算机系统中驻留、繁殖和传播。同时具有与生物学中病毒某些类似的特征：传染性、潜伏性、破坏性、变种性。

感染了病毒的计算机，经常会出现一些异常的症状：莫名其妙地经常死机、重启动或是不能正常启动；程序不能运行；运行速度降低；磁盘空间迅速变小；破坏文件中的数据，删除文件；破坏屏幕正常显示，蓝屏、黑屏；破坏键盘输入程序，无法正常输入等。除了这些常见的症状，还有一些病毒会引起特殊的计算机异常，例如：网络天空病毒利用系统收信的邮件地址，疯狂地乱发病毒邮件，大量浪费网络资源，使众多邮件服务器瘫痪，让受感染的系统速度变慢。此外，网络天空病毒还会将自身伪装复制到系统中的共享目录中，使用 Microsoft Word 图标和两个扩展名来迷惑用户。

1.1.2　计算机病毒的分类

了解计算机病毒的分类，可以帮助我们根据计算机病毒的特点来发现和防治病毒。

1. 引导区病毒

一台计算机的正常启动过程是先读取引导扇区或者主引导记录，再将其加载进入内

存中，然后引导相应程序。而如果计算机感染了引导区病毒，就会先把病毒加载到内存，然后才进行正常的引导过程。

引导区病毒主要感染软盘的引导扇区、硬盘的引导扇区或者主引导记录，用感染了这种病毒的启动盘启动计算机就会导致计算机中毒。但是，如果只是读取感染有引导区病毒的软盘或者光盘上的文件，计算机不会被感染。如果计算机出现了软盘读写错误、无故读取软驱或是系统启动失败等问题，有可能是感染了引导区病毒。

目前，流行较为广泛的一种引导区病毒是 PolyBoot(也叫 WYX. B)。PolyBoot 是一种典型的感染主引导扇区和第一硬盘 DOS 引导区的内存驻留型和加密引导型病毒，也能感染软盘的引导区。PolyBoot 发作可能会破坏硬盘的主引导区，并导致用户数据丢失。

2. 文件型病毒

文件型病毒是指能感染文件、并能寄生在被感染的文件中传染扩散的计算机病毒。被感染的文件可能是可执行文件(扩展名为 COM、EXE 等)或文本文件(如 Word 文档、Excel 等)。文件型病毒通过修改可执行文件或文本文件的结构，将病毒代码插入宿主程序。例如：CIH 病毒就是一种文件型病毒，这种病毒破坏力很大，一旦发作能够使主机无法启动、硬盘数据全部被清洗。CIH 病毒主要的感染目标就是 Windows 95/98 下的可执行文件。

文件型病毒感染文件后，被感染文件的长度、日期和时间大多会发生变化。有些病毒传染前后文件长度、日期和时间不会发生任何变化，一般称为隐型病毒。隐型病毒传染文件后，通过对被感染文件进行数据压缩以达到“隐身”的目的。

3. 宏病毒

宏病毒是一种特殊的文件型病毒，宏病毒不同于一般的文件型病毒的特点是：宏病毒感染数据文件，其传播不区分操作系统，并且更容易传播。如果我们收到的文档或电子邮件带有宏病毒，只要打开这些文件，计算机就会被宏病毒感染。感染宏病毒后，在此计算机上打开或是新建的文件都可能带上宏病毒。目前，常见的宏病毒有感染 Word 的 Word 宏病毒，感染 Excel 的 Excel 宏病毒等。

4. 脚本病毒

脚本病毒依赖一种特殊的脚本语言(如：VBScript、JavaScript 等)起作用，同时需要主软件或应用环境能够正确识别和翻译这种脚本语言中嵌套的命令。脚本病毒在某方面与宏病毒类似，但脚本病毒可以在多个产品环境中进行。

脚本病毒可以通过 E-mail 附件、局域网共享传播和感染 htm、asp、jsp、php 等网页文件传播，感染力强，传播范围大。例如：爱虫病毒由于通过电子邮件系统传播，曾在短短几天内狂袭全球数百万计的计算机。

5. 恶意代码

恶意代码是指网页中使用了利用漏洞来修改系统的一段代码。由于恶意代码并不具备传染性和自我复制这两个病毒的基本特征，所以如果严格的区分，不能称其为病毒。下面主要介绍一下特洛伊木马和网络蠕虫。

(1)特洛伊木马

特洛伊木马通常是指伪装成合法软件的非感染型病毒,但它不进行自我复制。有些木马程序可以模仿运行环境,搜集所需的信息。例如,试图窃取用户名和密码的登录窗口就是一种常见的木马程序。

(2)网络蠕虫

网络蠕虫是一种通过间接方式复制自身的恶意软件。网络蠕虫是目前互联网上传播最广泛的病毒之一。2004 年 1 月,一种名为“MyDoom”的网络蠕虫爆发,大量发送垃圾邮件,给全球造成了 300 多亿美元的直接损失。网络蠕虫的传播速度相当惊人,成千上万的病毒感染曾经造成众多邮件崩溃,带来难以弥补的损失。

1.1.3　计算机病毒的预防

预防计算机病毒是指针对病毒的特点,利用现有的技术手段,更好地保护计算机不受病毒的侵害。在使用计算机时,有一些良好的习惯可以帮助我们预防计算机病毒。

1. 备份系统和重要数据

定期备份系统和重要数据,万一遭受病毒侵害,或是由于其他原因造成系统崩溃、数据丢失时,备份的文件可以帮助我们及时恢复。

2. 安装杀毒软件和病毒防火墙并及时升级

安装杀毒软件和病毒防火墙可以为计算机加上一层基本的防护,不建议同时安装多个杀毒软件。多个杀毒软件同时运行容易出现冲突,并会占用系统资源。

每天世界上都会出现新的病毒,安装杀毒软件和病毒防火墙后,只有及时升级病毒库才能够使系统处于最新的防病毒状态下。病毒库是个数据库,记录着计算机病毒的种种特征以便及时发现和查杀。杀毒软件就是依赖病毒库才能区分一般程序和病毒程序,有时我们也称病毒库里的数据为“病毒特征码”。病毒库是要时常更新的,这样才能尽量保护计算机不被最新的病毒所侵害。

3. 及时为系统打补丁

系统漏洞让病毒更容易入侵,所以,系统安装完毕要马上打补丁,还要定期到官方网站下载最新的补丁。

4. 将浏览器的安全级别设为中级以上

有些计算机病毒能利用网页浏览器中的不安全设置侵入计算机。浏览含有恶意代码的网页有可能导致感染上病毒,而设置较高的浏览器安全级别可以一定程度上预防这种感染。

5. 了解流行病毒的特征

很多媒体上会介绍目前流行的病毒,经常了解流行病毒的特征有助于发现和预防病毒。例如,系统经常内存不足、重启动以及产生垃圾文件等异常现象,可能是感染了病毒。具体是哪一种病毒,可以结合计算机的具体症状来分析、判断。大多的杀毒软件官方网站免费提供针对这些病毒的专杀工具,及时下载专杀工具来查杀这些病毒,能将损失降低到

最小。

6. 警惕电子邮件病毒

有些病毒通过电子邮件传播的时候会将自己伪装成一个正常的邮件，使用一些容易使人好奇或大意的主题和内容，例如，将邮件的主题设为“I love you”、“系统退信”等，而将病毒文件伪装成图片、屏幕保护程序等作为附件发送。一旦打开这样邮件的附件，就会感染病毒。所以，建议不要打开来历不明的邮件，尤其不要打开其中的附件。即使是准备接收的电子邮件，其附件在打开之前最好用杀毒软件进行病毒检查。

7. 数据交换前先进行病毒检查

使用移动硬盘、软盘、光盘等进行数据交换之前，先用杀毒软件对其进行病毒检查，预防病毒通过这些媒介进行传播。

8. 定期扫描系统

定期扫描系统可以发现潜伏在计算机上的病毒，预防其以后发作或是传染给别的计算机。

总而言之，没有绝对安全的计算机系统，只有重视并积极预防病毒，计算机才能处于相对的安全之中。

在计算机日常使用的安全措施中，选用杀毒、防毒软件是必不可少的。常用杀毒、防毒软件国产的有金山毒霸、江民杀毒软件、瑞星杀毒软件、3721 上网助手等，国外的有诺顿杀毒软件、卡巴斯基杀毒软件等。下面将着重介绍金山毒霸、诺顿杀毒软件和 3721 上网助手。

1.2 金山毒霸 2005

金山毒霸的系列产品一直在国产杀毒软件市场中占有重要的地位，其新推出的金山毒霸 2005 更是在升级和防毒的能力上有进一步提高，下面是金山毒霸 2005 的特点。

1. 主动实时升级

当有最新的病毒库或功能出现时，用户无需操作，金山毒霸 2005 可以自动安装。这项功能使用户随时可以获得最新的病毒特征库，防止被新病毒感染、破坏。

2. 抢先启动防毒系统

金山毒霸 2005 抢先启动的防毒系统可以抢在开机时运行的病毒之前，在 Windows 未完全启动时就开始保护计算机系统。这项功能避免了由于计算机系统带病毒杀毒，导致病毒查杀不干净的情况。

3. 主动修复漏洞

金山毒霸 2005 能够扫描操作系统及各种应用软件的漏洞。当新的安全漏洞出现时，金山毒霸 2005 会下载漏洞信息和补丁，经扫描程序检查后自动帮助用户修补。这项功能可避免利用该漏洞的病毒侵入系统，使用户的操作系统保持安全状态。

此外，金山毒霸 2005 还会扫描系统中存在的简单密码、完全共享文件夹等其他安全隐患。

4. 跟踪式反间谍

金山毒霸 2005 采用全新的网络程序校验策略。除了传统反黑、拦截木马等功能外，同时对普通应用程序进行跟踪监控。一旦应用程序的大小、内容等属性发生异常变化，系统将特别提醒用户注意，能够有效防止木马、间谍软件“冒名顶替”盗取用户数据。

5. 木马防火墙

金山毒霸 2005 通过多种技术来实现对木马进程的查杀。一旦发现系统中有木马、黑客或间谍程序访问网络，金山毒霸 2005 会及时拦截该程序对外的通信访问，然后对内存中的进程进行自动查杀，保护用户网络通信的安全。这项功能对防止盗取用户信息的木马、黑客程序特别有效。

1.2.1　金山毒霸 2005 的安装

安装正版的金山毒霸 2005 的流程可以分为三步：安装金山毒霸 2005、注册金山通行证和购买金山毒霸。下面分别介绍。

1. 安装金山毒霸 2005

可以购买正版光盘安装，也可以登录金山公司的网站（http://www.kingsoft.com），免费下载金山毒霸 2005 的安装包。完整的下载文件为 EXE 文件，适用于 Windows 98/ME、Windows 2000 专业版、Windows XP 家庭版/专业版。可以直接运行安装，安装界面如图 1-1 所示。

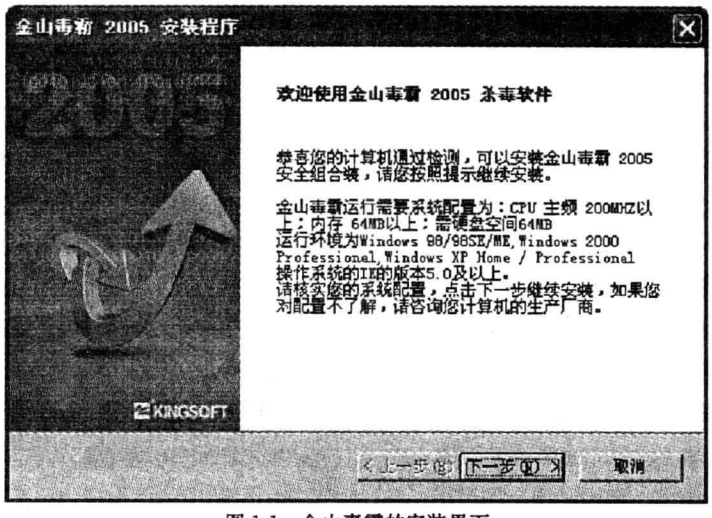

图 1-1　金山毒霸的安装界面

需要注意的是，安装金山毒霸 2005 之前，应该首先卸载旧版金山毒霸。当直接在旧版金山毒霸存在的基础上安装金山毒霸 2005，安装程序将自动检测计算机中旧版的金山毒霸，并提示卸载所有旧版本。

安装程序将检测其他杀毒软件和金山毒霸 2005 的兼容性，当发现不兼容的情况时，友好提示用户是否继续安装，以保证金山毒霸 2005 的正确安装。

2. 注册金山通行证

在安装金山毒霸 2005 的过程中需要输入金山通行证，如图 1-2 所示。

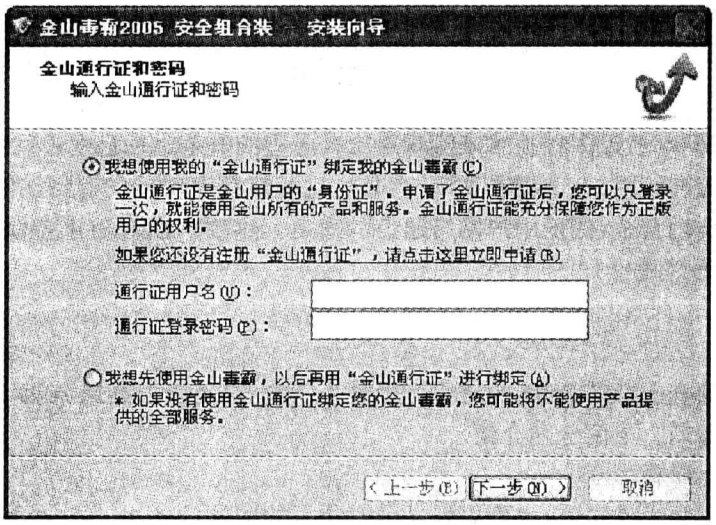

图 1-2　金山通行证输入界面

金山通行证是用户在金山在线的“身份证”。申请了金山通行证后，一次登录即可使用金山各种网络服务和各种个性化服务。申请金山通行证是免费的，申请金山通行证时，需要绑定电子邮箱或手机。绑定电子邮箱或手机用于重置二级密码，是最高级别的帐号保护措施。建议选择稳定和常用的电子邮箱申请通行证。

3. 购买金山毒霸

要想得到长期可靠的服务，付费购买正版的金山毒霸是必要的。金山公司为用户提供了多种付费购买金山毒霸服务时间的方式，用户可以根据自己的实际情况选择一种。

金山毒霸 2005 安全组合装内含金山毒霸 2005、金山网镖 2005 和金山木马专杀 2005。其中，金山毒霸 2005 的主要功能为病毒的查杀和实时监控、隐私保护、垃圾邮件监控、创建应急盘和网页代码的检测等；金山网镖 2005 是个人网络防火墙，功能为拦截查杀黑客程序、木马和间谍软件，防护网络攻击等；金山木马专杀 2005 的主要功能是查杀木马、管理进程及启动项、修复系统环境和扫描可疑文件等。

在软件安装结束之后，金山毒霸 2005 的安装程序还会提示进行软件升级和系统漏洞检查。

1.2.2　金山毒霸 2005 的启动

安装了金山毒霸 2005 后，金山毒霸 2005 将在开机时自动启动，启动后在桌面任务栏的右端将会出现一个红色的小盾牌，即金山毒霸 2005 的图标。双击该图标可以进入金山毒霸 2005 的主界面。

如果在任务栏上看不到金山毒霸 2005 的图标，也可以单击“开始”→“所有程序”→“金山毒霸 2005 安全组合装”→“金山毒霸 2005”启动金山毒霸 2005，启动后金山毒霸 2005 的主界面如图 1-3 所示。