精品丛书“24小时轻松掌握系列”
全新改版，重装上市

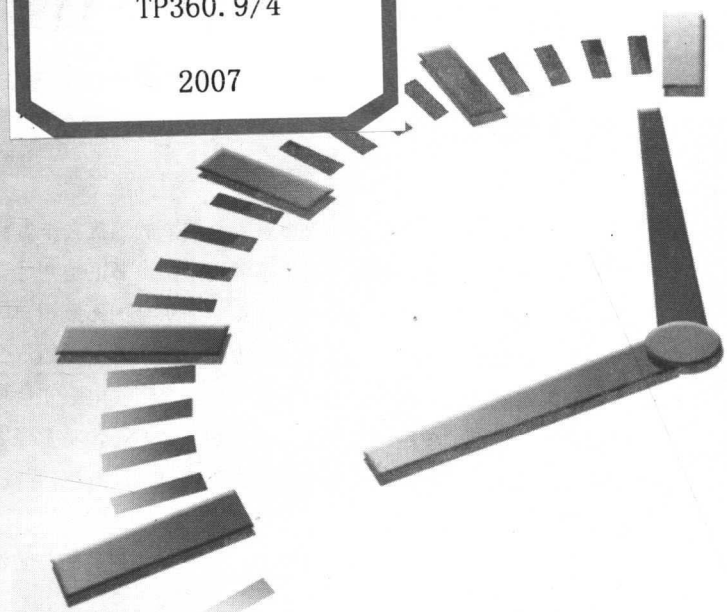
电脑安全设置

24小时轻松掌握

向光祥　编著

- 科学安排，24小时分步学习，轻松掌握。
- 贴近实用，木马病毒一网打尽，高枕无忧。
- 步步图解，原理与实践相结合，点睛透彻。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



电脑安全设置
24小时轻松掌握

向光祥　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

一直以来，众多用户都受着电脑安全问题的困扰。作为普通的网络用户，人们都有着共同的忧虑——病毒、木马严重影响着电脑的安全。本书正是立足于广大用户的这些普遍问题，将内容划分为病毒、木马、电脑安全管理3篇，力求全面拓展用户的防护知识并解决用户的疑难问题。

本书以计算机病毒、木马与电脑安全管理技术为主题，合理巧妙地分为24个小节，从系统设置到网络安全，从数据备份到数据恢复，介绍了电脑安全与防病毒方面的应用技巧。立足于扩展读者的知识面，使用户能有效地抵御病毒、木马，防范黑客的侵袭，能正确地安装杀毒软件、设置防火墙，在特殊电脑安全设置问题上可以手动排除故障，处理疑难、防患于未然，安全有效地使用计算机。

本书适用于初学者或者中级用户，是学习如何诊断与防治计算机病毒、木马等的参考资料。

图书在版编目（CIP）数据

电脑安全设置24小时轻松掌握/向光祥编著. —北京：
中国铁道出版社，2007.10
（24小时轻松掌握系列）
ISBN 978-7-113-08402-8

Ⅰ.电… Ⅱ.向… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（2007）第168794号

书　　名：电脑安全设置24小时轻松掌握
作　　者：向光祥
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街8号）
策划编辑：严晓舟　荆　波
责任编辑：荆　波　鲍　闻
封面设计：付　巍
封面制作：白　雪
印　　刷：北京市彩桥印刷有限责任公司
开　　本：787×1092　1/16　**印张**：18　**字数**：418千
版　　本：2007年12月第1版　2007年12月第1次印刷
印　　数：1～6 000册
书　　号：ISBN 978-7-113-08402-8/TP·2618
定　　价：28.00元

丛书序 只需 24 小时，轻松具备一种电脑技能

进入 21 世纪的你，如果还不能熟练地使用电脑，这不能不说是一种遗憾。

电脑的世界是十分美妙的世界，我们通过 Internet 了解世界，通过 E-mail 和朋友们沟通，上网购买所需要的图书……电脑，越来越成为生活的必需品，给我们的工作、学习和生活带来了巨大的帮助。

只要会中文，就可以享受高科技带来的便利

可是，在今天，还是有不少读者朋友，不会使用电脑，或者说不能熟练地驾驭电脑，让电脑帮我们完成各种工作，体验电脑文化带给我们的神奇感觉，享受高科技的产品带给我们的便利。

很多读者向我们抱怨，电脑学习这么难，而且，没有足够的时间去学习……根据我们多年的教学经验，只要会中文，可以阅读中文书籍，就能够看懂电脑的中文应用界面，培养基本的电脑技能，并逐步地熟练。只要你能定期抽出一个小时的完整时间，认真地实践我们提供的技能培养计划，就一定可以成功地驾驭电脑，并可以体验学习新知识的快乐。

科学安排，学会不难

我们把常用的电脑技能，分解成一个一个的学习单元。只要能定期抽出一个小时的空余时间，按照本书的安排，学习其中一个单元，一个小时一点进步，一个小时一点提高。由慢到快，电脑技能很快就可以上一个新的台阶。

按照我们的学习安排，只要 24 小时，一定可以掌握一种电脑应用技能。这个时候，学习的流程安排和内容就相当重要。

根据作者多年的经验，我们在这 24 个小时里面的每一个小时，或者安排读者学习某种技能；或者让读者跟我们学做某个实例；或者让读者强化训练某项技能。这 24 个小时的安排串联起来，就是一张电脑技能的学习地图，它伴随读者探索电脑奥秘的全过程。加上一定时间的训练，一定能教会读者应用电脑，并熟练起来。

按图索骥，提高最快

针对任何一项电脑技能的学习，24 小时培养计划，犹如学习中的 24 级台阶，由作者精心设计。读者可按这个学习顺序，由浅入深，由易到难，逐步掌握好有用的电脑技能。

学习是一个由慢到快的过程。每个人的情况不一样，一般来说，前面的基础打好了，后面的学习速度就会越来越快。所以，在一些内容的安排上，

我们遵循了这个特点。在最后的几个小时的学习计划中，学习内容具有并列特性，读者可根据自己的需要选择学习的顺序。

另外，作为正文的补充，有的图书我们还提供了附录，供读者查询某些资料。

边学边练，事半功倍

学习电脑技能，还要讲究一定的技巧。有了完美的学习方案，还得有足够的练习。

根据我们的经验，电脑技能的学习，上机练习非常重要。所以，建议读者在学习的过程中，同时找一台电脑练习所学内容。

一本图书，一台电脑，一边学习，同时按书中所讲练习，可加深印象，更能巩固技能，越用越熟练，越用越体会到使用电脑的乐趣。希望我们的每一本书，加上读者的 24 小时自我训练，能使读者的电脑水平在某一个方面得到飞快地提升。

联系作者，答疑解难

每一个读者，都有不同的基础和学习经验。我们虽然设计了大多数读者的学习地图，但由于每位读者电脑配置不一定相同，学习碰到的问题也可能各不相同。所以，除了本书之外，我们特地开辟了读者答疑邮箱：jb18803242@yahoo.com.cn。

如果读者在应用电脑的过程中碰到疑难问题，可以发邮件给我们，我们很乐意为您解答，并将典型问题放在下一版的图书中。

编 者

2007 年 10 月

前言

随着计算机技术的快速发展，人类已经进入了网络时代。网络给人们带来方便的同时也带来了一些不可避免的负面影响，比如感染计算机病毒、遭受网络攻击、信息被盗等。为了有效地防范网络攻击，维护自己的权益不受侵犯，就需要我们更多地了解各种网络攻击的原理与手段以及网络中存在的各种漏洞等知识，以便及时维护我们的系统。

本书特色

本书充分考虑了广大初、中级计算机用户在网络安全方面的根本需求，主要面对日常使用计算机的办公人员以及具有一定电脑应用技能的读者。对于最广大的计算机用户来说，实际上对计算机安全、网络安全、数据安全等并不精通，但又不可能花费太多精力去学习。因此，如何在最短时间内，花费不多的精力，让上述读者学到最实用的计算机安全、网络安全、数据安全知识，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、编写的。

本书内容丰富、深入浅出，适合初、中级读者学习。全书以操作步骤为主，提供了尽可能详细的操作步骤和分解图片，使所有操作一目了然。书中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。借助本书，用户可以联系自己的实际情况，逐步深入地学习计算机以及网络安全方面的基本知识、方法和技巧。

内容安排

全书按读者的学习进度划分为 24 个小时：

第 1~5 小时：具体介绍计算机病毒的发展历程、如何利用现今最为流行的病毒检测技术，迅速检测病毒并针对其特点及时清除病毒等问题，帮助计算机用户及时了解现今病毒的发展方向。对现在流行的几种常见计算机病毒彻底分析总结，并介绍如何利用“专杀工具”将病毒清除。

第 6~11 小时：介绍了木马程序的发展历程、常见木马攻击手段等内容，并对现今最流行的几种木马程序进行详细分析。利用木马专杀工具对木马查杀进行图解分析，帮助读者迅速了解木马专杀工具的使用，以及木马的发展趋势。

第 12 小时介绍了如何安全设置网络浏览器，有效地防止计算机病毒、木马的入侵。

第 13 小时介绍了对现今流行网络通讯工具 QQ、MSN、Foxmail 的安全设置，包括密码安全管理、垃圾邮件的过滤设置，等等。

第 14 小时通过介绍电脑从开机到管理，需要关注的几大安全设置问题，从而引起读者对电脑安全重要性的认识。

第 15 小时介绍流氓阻击软件，包括流氓软件的性质与分类，并对两种流氓阻击软件的应用进行了简要介绍。

第 16 小时注册表安全策略，介绍通过注册表编辑器的设置实现系统和网络安全的方法与策略。

第 17 小时介绍通过组策略工具的设置实现系统、网络安全的方法与策略。

第 18 小时介绍防火墙的功能与分类，详细分析了 Windows 自带的防火墙和天网个人防火墙的应用，以便读者迅速掌握防范黑客攻击的技巧。

第 19 小时对网络黑客的入侵步骤、工具进行分析，并给出各种攻击手段的应对措施，以便读者更好地保护系统。

第 20 小时介绍了系统的安全漏洞与如何进行端口检查，并分析总结了系统网络服务、系统漏洞、服务端口的扫描及检查方法。

第 21 小时介绍了如何对移动存储设备进行加密、解密，保护用户的数据存储安全。

第 22 小时介绍了如何对文件进行保护，包括文件的伪装、加密等，帮助用户保护文件的信息安全。

第 23 小时向读者介绍了如何修复损坏文档，包括手动或借助软件进行修复。

第 24 小时介绍数据的备份与还原，通过对几种备份还原数据工具的使用分析，使读者快速掌握数据备份与还原的技巧，减少用户数据丢失。

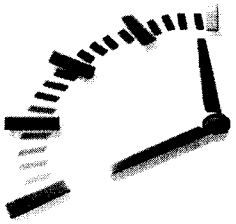
本书比较详细地介绍了防范计算机病毒、木马的攻击与计算机的安全管理，希望通过本书能让读者对网络安全问题有一个总体性的了解。

本书由向光祥编著，参与本书编写的还有马晓平，周宏侠，宋建龙，贾富，沈明，王枫，刘冰，韩涛，高霞，吕茜，李娜，李杨，杨阳，罗峰等，在此一并表示感谢。由于编者个人实践的局限，加之时间仓促，欢迎广大读者对书中不足之处批评指正。

编　者

2007 年 10 月

目 录



第 1 小时 计算机病毒概述

计算机病毒不是我们所熟悉的生物病毒，而是一个程序、一段可执行代码。但是，计算机病毒就像生物病毒一样，有独特的复制能力，同生物病毒一样很快地蔓延，而且常常难以根除。网络时代已经到来，计算机病毒已经对我们的信息系统、重要数据等造成了威胁，学习防治计算机病毒知识已经非常必要。

本章导读

- 计算机病毒定义
- 计算机病毒特征
- 计算机病毒分类
- 计算机病毒命名规则
- 计算机病毒运行原理
- 计算机病毒的破坏表现
- 计算机病毒发展趋势

1-1 计算机病毒的定义

计算机病毒并非是最近才出现的产物，事实上，早在 1949 年，距离第一部商用电脑出现前几年，电脑的先驱者约翰·范纽曼（John Von Neumann）在他所提出的一篇论文《复杂自动装置的理论及组织的进行》中，就已经把病毒程序的蓝图勾勒出来了。当时，绝大多数电脑专家都无法想象这种会自我繁殖的程序会出现在不久的将来，可是少数几个科学家默默地研究范纽曼所提出的概念。直到 10 年之后，在美国电话电报公司（AT&T）的贝尔（Bell）实验室中，这些概念在一种很奇怪的电子游戏中成形了，这种电子游戏叫做“磁蕊大战”（Core War）。

磁蕊大战是当时贝尔实验室中三个年轻程序人员在工作之余想出来的，他们是道格拉斯麦耀莱（H.Douglas McIlroy），维特·维索斯基（Victor Vysottsky）以及罗伯·莫里斯（Robert T. Morris），当时三人都只有二十多岁。

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》（以下称《条例》），在《条例》第二十八条中明确指出：“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。”此定义具有绝对的法律性、权威性。

计算机病毒的产生是社会信息化进程发展到一定阶段的必然产物。其产生过程可以通过此表达式概括：

程序设计→传播潜伏→触发、运行→实行攻击

下面我们开始探索计算机病毒，对于计算机病毒产生的原因可以总结如下：

- 出于好奇或兴趣

从事计算机等相关专业的人们在工作之余出于好奇或者兴趣，也有的是为了满足自己的表现欲，故意编制出一些特殊的计算机程序，让别人的电脑出现一些动画或播放声音，提出问题让使用者回答，以显示自己的才干。而此种程序流传出去就演变成计算机病毒，此类病毒破坏性一般不大。

- 产生于个别人的报复心理

出于此种情况，可能是在遭受其他人编写的病毒侵害后，同样编写病毒对其实施反击。

- 来源于软件加密

一些商业软件公司为了不让自己的软件被非法复制和使用，运用加密技术，编写一些特殊程序附在正版软件上，如遇到非法使用，则此类程序自动激活，于是又会产生一些新病毒，如巴基斯坦病毒。

- 产生于游戏

编程人员在无聊时互相编制一些程序输入计算机，让程序去销毁对方的程序，如最早的“磁芯大战”。

- 政治、经济和军事等特殊目的

一些组织或个人也会编制一些程序用于进攻对方电脑，给对方造成灾难性或直接性的经济损失。

1-2 计算机病毒的特征

计算机病毒如此疯狂肆虐的在网络中传播，主要是由于其本身具有的特性，计算机病毒的主要特征如图 1-1 所示：

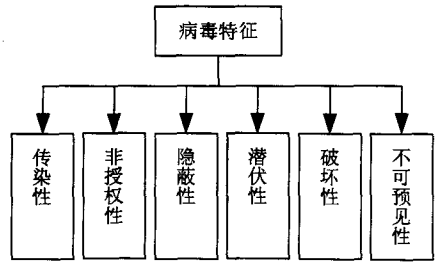


图 1-1

1. 传染性

传染性是指计算机病毒具有把自身复制到其他程序中的特性。当病毒一旦符合运行条件就会在相应的文件或存储介质中繁衍。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他计算机进行数据交换或通过网络接触，病毒就会继续传播。现在我们已经把是否具有传染性作为判别一个程序是否为计算机病毒的最重要条件。

2. 非授权性

非授权性是指病毒没有经过计算机用户授予的权限。一般正常的程序是由用户调用运行，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒则隐藏在正常的程序中，用户一旦运行该程序，病毒就会窃取到系统的控制权，并且优先于正常程序的执行。其动作、目的对用户是未知的，是未经用户允许的。

3. 隐蔽性

病毒为了在计算机里长久地“生存”，隐蔽性非常重要。通常病毒附在正常程序中或磁盘较隐蔽的地方，也有个别的以“隐藏文件”的形式出现，目的是不让用户发现它。如果用户不经过

仔细的代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序，而且受到传染后，计算机系统通常仍能正常运行，而且用户不会感到有任何异常。

4. 潜伏性

大部分的病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足特定条件时才启动其表现模块，破坏计算机系统。如“PETER-2”在每年 2 月 27 日会提出三个问题，答错后会将硬盘加密。著名的“黑色星期五”病毒在逢 13 号的星期五发作。国内的“上海一号”病毒会在每年三、六、九月的 13 日发作。当然，最令人难忘的还有每月 26 日发作的 CIH 病毒。这些病毒在平时会隐藏得很好，只有在发作日才会暴露出本来面目。

5. 破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。由此特性可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示些画面、无聊的语句或播放点音乐，或者根本没有任何破坏行为，但会占用系统资源；而恶性病毒破坏性较大，可能给系统带来灾难性的后果。

6. 不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。人们利用病毒的这种共性，制作了声称可查所有病毒的程序（某些杀毒软件）。这种程序的确可查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断地提高，病毒对反病毒软件永远是超前的。

1-3 计算机病毒的分类

计算机病毒种类繁多，通常我们实施的分类方法是按照寄生方式和传染途径来分类的。如图 1-2 所示：

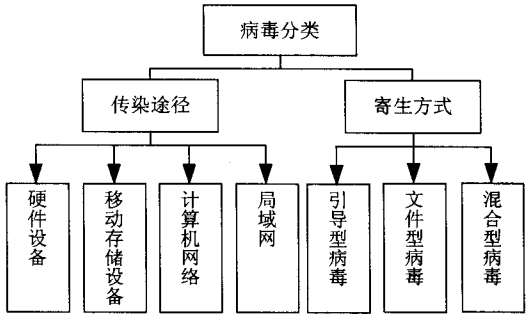


图 1-2

1. 引导型病毒

引导型病毒会更改（即一般所说的“感染”）磁盘上的引导扇区（BOOT SECTOR）的内容，软盘或硬盘都有可能感染病毒或者是改写硬盘上的分区表（FAT）。如果用已感染病毒的软盘来启动的话，则会感染硬盘。

2. 文件型病毒

文件型病毒主要以感染文件扩展名为.com、.exe 和.ovl 等可执行程序为主。它的安装必须借助于病毒的载体程序，即需要运行病毒的载体程序，方能把文件型病毒引人内存。已感染病毒的文件执行速度会减慢，甚至完全无法执行。有些文件遭感染后，一执行就会遭到删除。

3. 混合型病毒（集引导型与文件型两种病毒特性于一体）

混合型病毒综合系统型和文件型病毒的特性，它的“性情”也比系统型和文件型病毒更为“凶

残”。此种病毒透过上述两种方式来传播，更增加了病毒的传染性以及存活率。不管以哪种方式传播，只要中毒就会经开机或执行程序而感染其他的磁盘或文件，此种病毒也是最难杀灭的。

计算机病毒按其传染途径分类：

4. 通过计算机硬件设备进行传播

这些设备通常有计算机的专用 ASIC 芯片和硬盘等。这种病毒虽然数量极少，但破坏力却极强，对于这一类病毒，目前尚没有较好的检测手段。

5. 通过移动存储设备来传播

这些设备包括软盘、U 盘等。在移动存储设备中，软盘是使用最广泛移动最频繁的存储介质，因此也成了计算机病毒寄生的“温床”。目前，大多数计算机都是从这类途径感染病毒的。

6. 通过计算机网络进行传播

现代信息技术的巨大进步已使空间距离不再遥远，“相隔天涯，如在咫尺”，但也为计算机病毒的传播提供了新的“高速公路”。计算机病毒可以附着在正常文件中通过网络进入一个又一个系统，国内计算机感染一种“进口”病毒已不再是什么大惊小怪的事了。在我们信息国际化的同时，计算机病毒也在国际化。估计以后这种方式将成为第一传播途径。

7. 通过点对点通信系统和无线通道传播（局域网）

目前，这种传播途径十分广泛，在未来的信息时代，这种途径很可能与网络传播途径成为病毒扩散的“时尚渠道”。

1-4 计算机病毒的命名规则

目前全世界流行的病毒大约有数万种，为了方便管理，反病毒公司按照病毒的特性，将病毒进行了分类命名。虽然每个反病毒公司的病毒命名规则都不太一样，但大体都是采用前缀命名法来表示一个病毒的，命名形式为：

<病毒前缀>.<病毒名>.<病毒后缀>

但是上面的命名方式太过于专业化，为了使病毒名称方便记忆、形象化。于是很多人按照如下方式对计算机病毒进行命名：

1. 按病毒发作的时间

该命名方式取决于病毒表现或破坏系统的发作时间，这类病毒的表现或破坏部分如同定时炸弹，如“米氏”病毒，其病毒发作时间是 3 月 6 日，而 3 月 6 日是世界著名艺术家米开朗基罗的生日，于是得名“米开朗基罗”病毒。

2. 按病毒发作症状

该种病毒命名方式非常形象化，以病毒发作时的现象来命名，如“火炬”病毒，是因为该病毒发作时在屏幕上出现五支闪烁的火炬。

3. 按病毒自身包含的标志

以病毒中出现的字符串、病毒标识（图标等）、存放位置或病发表现时病毒自身宣布的名称来命名，如“熊猫烧香病毒”发作时，“熊猫”成群（如图 1-3 所示）。它的破坏力很强，给用户的电脑系统造成巨大的危害，并且导致大量应用软件无法运行。