快学快用

电脑安全与病毒防范

网上疑难解答 网 址：faq.hxex.cn
E-mail：faq@hxex.cn

电话疑难解答 010-88253801-168

卓越科技 编著

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

快学快用

电脑安全与病毒防范

卓越科技 编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书详细介绍了电脑病毒与安全防范的相关知识，对用户保障电脑的安全性等问题有很大帮助。

本书内容新颖、版式清晰、语言浅显易懂、操作举例丰富，在讲解时每章以“知识讲解+实战演练+上机练习”的方式讲解，每个知识点下面的操作任务以“新手练兵场”来介绍，并配有生动活泼的卡通和小栏目。另外，本书以图为主，图文对应，每章最后配有相关的上机练习题，并给出练习目标及关键步骤，以达到学以致用的目的。

本书定位于学习电脑病毒与安全防范知识的初、中级电脑用户，也可作为电脑维护人员和大中专院校师生的技术参考书籍。

图书在版编目（CIP）数据

电脑安全与病毒防范 / 卓越科技编著.—北京：电子工业出版社，2008.7
（快学快用）
ISBN 978-7-121-06642-9

Ⅰ. 电… Ⅱ.卓… Ⅲ.①电子计算机－安全技术②计算机病毒－防治 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2008）第 063621 号

责任编辑：刘 舫
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　　1/16　　印张：10　　字数：256 千字
印　　次：2008 年 7 月第 1 次印刷
定　　价：15.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

如今，学电脑已不再是什么新鲜事，大人、学生甚至老人都加入了学习电脑的队伍中。我们发现，同样是电脑入门，不同读者的学习方法是不同的，选择的图书也有很大差异。另外，在版式风格、页数多少和知识点取舍方面，读者的需求也各不相同……很多读者面临着“买不到适合自己的书”的困扰。

经过深入的市场调查和近两年的编写工作，《快学快用》系列图书终于和大家见面了！

本丛书的写作初衷是全面挖掘电脑初学者的需要，让不同层次的读者都能从中挑选到适合自己的电脑入门图书。我们的目标是让所有人都能看得懂、学得会、用得好，并提供快速解决实际问题的方法，真正做到满足工作和生活的需要。

有《快学快用》丛书在手，电脑学习不再困难！所有想学电脑、想玩电脑、想用电脑的朋友们，赶快行动起来吧！

丛书主要内容

本丛书涉及电脑基础与入门、打字与输入法、电脑上网、操作系统、Office 办公、硬件与维护、应用技巧、综合应用和图形图像等众多领域，每个类别图书都根据读者的不同年龄层次、不同文化程度、不同职业、不同学习方法……进行细分后量身打造，每本图书都针对某一类读者精心编写，在内容安排、讲解方式、排版风格等方面各不相同。

《快学快用》丛书主要包括以下图书：

- 电脑基础快速入门
- 电脑应用轻松入门
- 家用电脑快速入门
- 电脑上网快速入门
- 老年电脑快速入门
- 图解电脑快速入门
- 电脑应用融会贯通
- 电脑打字快速入门
- 1 天学会五笔打字
- 中文版 Windows XP 快速入门
- 中文版 Windows Vista 快速入门
- Office 2007 快速入门
- Excel 2007 表格处理
- PowerPoint 2007 幻灯片制作
- Office 2007 办公应用融会贯通
- Windows XP，Word 2007，Excel 2007 与电脑上网四合一
- Word 2007，Excel 2007，PowerPoint 2007 融会贯通
- 中文版 Photoshop CS3 图像处理
- 中文版 Flash CS3 动画制作
- Dreamweaver CS3 网页制作
- AutoCAD 2008 建筑绘图
- AutoCAD 2008 机械绘图
- 操作系统安装与重装
- 注册表与 BIOS 应用详解
- 电脑组装、维护与故障排除
- 电脑安全与病毒防范
- 精彩网址速查手册
- 网上开店与赚钱

- Windows Vista 实用技巧 1088 招
- Office 实用技巧 1088 招
- 电脑入门应急速查 1088 招
- 电脑上网技巧 1088 招

……

读者不必再大海捞针般地艰苦寻找需要的图书，《快学快用》丛书中，总有适合您需要的那一本。

本书主要特点

本书具有以下特点：

- **以操作为主，实例丰富：**在一些操作性较强的知识点下列出一个具有代表性的操作练习任务，并将每个练习的要求明确地提出来，有助于读者在学习一个知识点后就能上机实践。
- **内容新颖，知识含量高：**本书总结了市场上同类图书的优点，并在其基础上优化了学习结构、增加了大量新知识点。图书在讲解过程中还穿插了“温馨小贴士”和“秘技播报站”等小栏目，介绍相关的概念和操作技巧，丰富读者的知识面。
- **图示丰富，易于操作：**操作步骤讲解详细，图文对应，在插图中用❶、❷、❸等步骤序号列出具体操作方法，插图中还配有相关说明文字，帮助读者轻松理解和掌握知识。

本书读者对象

本书主要定位于学习电脑病毒与安全防范知识的初、中级电脑用户，可作为家庭用户、上班族、电脑维护人员以及青少年学生掌握电脑病毒与安全防范操作的参考用书，也可作为各种电脑培训学校和职业技术学校相关课程的参考教材，且非常适用于需在短时间内快速掌握如何防范电脑病毒与保护电脑安全的读者使用。

本书作者及联系方式

本书由卓越科技组织编写，西华大学马利亚主编，马利亚、于海波等编著，其中马利亚编写 1~5 章，于海波编写 6~9 章。由于作者水平有限，书中疏漏和不足之处在所难免，恳请广大读者及专家不吝赐教。

如果您在阅读本书的过程中有什么问题或建议，请通过以下方式与我们联系。

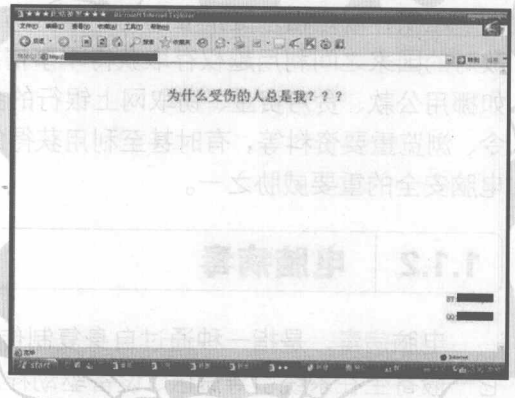
- **网站：**faq.hxex.cn
- **电子邮件：**faq@hxex.cn
- **电话：**010-88253801-168（服务时间：工作日 9:00~11:30，13:00~17:00）

反侵权盗版声明

目 录

第 1 章

你的电脑安全吗



一直以来，电脑病毒、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？是摆在所有电脑用户和安全专家们面前的问题。本章就对电脑安全的威胁者、电脑安全问题的类型与电脑安全技术这些基本内容进行简单讲解，从而为后面的深入学习打下牢固的理论基础。

1.1 是谁在威胁电脑安全

从个人电脑普及到家庭以后，电脑安全问题就被摆到了台面上。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。因此，了解影响电脑安全的主要因素是每个用户最为关注的事情，只有这样，才能做到知己知彼，从而将电脑安全的威胁者拒之门外。

1.1.1 越权存取

越权存取是指未经批准的用户非法访问本地电脑，并从中获取重要信息。在战争期间，敌对的国家之间利用越权存取获得军事情报；在金融电子领域，则利用它进行电脑犯罪，如挪用公款、贪污资金、窃取网上银行的金钱等；而在个人电脑中，则可以利用它盗取口令、浏览重要资料等，有时甚至利用获得的信息对用户进行金钱勒索。因此，越权存取是电脑安全的重要威胁之一。

1.1.2 电脑病毒

电脑病毒，是指一种通过自身复制传播而产生破坏电脑功能或毁坏数据作用的程序，它一般寄生在系统引导扇区、设备驱动程序或操作系统的可执行文件内，并能够利用系统资源进行自我繁殖，从而达到破坏电脑系统的目的。

下面我们来了解电脑病毒的分类、特性与危害等知识，以便能及早发现病毒，使自己的电脑时刻处于安全的环境中。

1. 电脑病毒的分类

电脑病毒的种类有很多，不同类型病毒的破坏能力也有大有小，按照其运行特征可以分为如下几种。

- ☑ **引导型病毒：**这类病毒一般感染系统的引导扇区，电脑一启动就在病毒的控制下。当有其他存储设备访问系统时，病毒将自动复制到这些存储设备中，进行传播。
- ☑ **文件型病毒：**这类病毒一般感染系统中的可执行文件，如果用户运行感染了病毒的程序，将立即激活病毒。
- ☑ **蠕虫病毒：**蠕虫病毒通过网络不断发送垃圾信息，使网络通道被堵塞，无法进行正常通信。蠕虫病毒可以在很短的时间内蔓延整个网络，造成网络瘫痪。这类病毒发作后一般常驻内存，不断自我复制以达到感染电脑并使网络堵塞的目的。
- ☑ **宏病毒：**是指利用宏语言编制的病毒，它一般感染 Word 和 Excel 等文档文件，造成文档无法正常使用。
- ☑ **混合型病毒：**混合型病毒一般具有多种病毒的特征，因此这种类型的病毒会造成更大的危害。

温馨小贴士

电脑病毒以恶性病毒居多，常常给用户带来不可预计和难以恢复的损失，让重要资料和数据灰飞烟灭。如 2006 年底出现的蠕虫病毒——“熊猫烧香”使许多用户的电脑处于瘫痪状态，其传播范围之广也是近几年中少有的，如图 1-1 所示为电脑感染“熊猫烧香”病毒的效果。

◆ 图 1-1

2. 电脑病毒的特性

电脑病毒一般具有如下特性。

- ☑ **传染性**：一旦感染上电脑病毒，它就会常驻内存，然后不停地复制自己，并通过网络、软盘、闪存盘等介质传播出去，如果没有发现病毒或缺少必要的安全防护措施，那么和染毒电脑有联系的电脑都有可能被病毒感染。
- ☑ **破坏性**：电脑病毒如果在其潜伏期内没有被发现，到了病毒的发作日期就会自动运行。病毒可以修改文件大小、修改系统注册表、在硬盘中制造大量无用的垃圾文件、占用磁盘空间，有的病毒还会删除可执行文件，造成系统瘫痪。
- ☑ **隐蔽性**：病毒具有很强的隐蔽性，有的病毒程序的名称和正常系统文件名称相似，如果不注意就会误认为是系统文件。有的病毒程序可以将自身属性设置为隐藏，在正常状态下是无法查看到的，因此，病毒的隐蔽性常常会迷惑许多普通用户。
- ☑ **难以预见性**：电脑病毒的代码都不相同，但其共性是都需要常驻内存、修改中断等，而有些正常的程序也具有这些特征，这些程序并不会对系统造成危害。另外，病毒的编写技术也在不断改进，因此病毒的难以预见性使病毒始终走在反病毒软件的前面。

3. 电脑病毒的危害

病毒发作带来的后果是不堪设想的，轻者破坏操作系统，重者可能导致硬件损坏。概括来讲，电脑病毒运行后造成的危害有如下几种。

- ☑ **占用内存**：所有程序的运行都在内存中进行，病毒程序运行后会占用大量的内存，并影响正常程序的运行，系统运行会变得极不稳定，出现某些命令无法执行的情况，最后引起系统崩溃。
- ☑ **修改系统引导信息**：有的恶性病毒可修改硬盘的引导信息、FAT 表等，造成系统无法启动，硬盘无法使用，严重的还会使整个硬盘中的数据丢失。
- ☑ **修改文件**：病毒可对某些类型的文件进行修改，使文件打开后变成乱码、内容颠

倒或者内容丢失，甚至会删除系统中有用的文件。

- **修改主板 BIOS 芯片：**有的病毒能够对 BIOS 芯片进行写入操作，破坏系统 CMOS 数据。一旦 CMOS 数据被毁，电脑将不能启动，或不能正常查找硬件信息供操作系统调用。
- **使输入输出设备出现故障：**有些病毒会使屏幕中显示各种各样的混乱字符，鼠标和键盘无法正常使用，打印机在打印时出现假报警、间断性打印、更换字符等现象。
- **丢失硬盘数据：**有的病毒运行后可改写硬盘中的数据，更有甚者将硬盘格式化，造成不可挽回的损失。

温馨小贴士

电脑病毒实际上是一些代码，它对电脑的危害取决于病毒制造者的意图，病毒的制造者可以编制病毒使电脑执行病毒制造者想执行的操作。

1.1.3 木马

木马的全称是“特洛伊木马（Trojan Horse）”，它来源于古希腊神话。在电脑中，木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘以及攻击 DOS 等特殊功能的后门程序。

木马通常有两个可执行程序，一个是客户端，即控制端，另一个是服务端，即被控制端。为了防止木马被发现，设计者往往采用多种手段伪装木马，并利用这种伪装吸引用户下载执行，而木马一旦运行并被控制端连接，则控制端将享有被控端的绝大部分操作权限，如给电脑增加口令、修改注册表或更改电脑配置等。

1. 木马的种类

严格地讲，木马的种类并没有一个标准的限制，大多数木马都不是单一功能的木马，它们往往是很多种功能的集成品，因此，这里只以其发展为标准进行分类。

- **第一代木马：**这一代木马功能简单，主要针对 UNIX 操作系统进行攻击，而针对 Windows 操作系统的木马则不多。该时期具有代表性的木马为 BO 和 Netspy 等。
- **第二代木马：**这一代木马功能大大加强，几乎能够进行所有的操作，且随着 Internet 的普及，开始通过网络进行大范围的传播。该时期具有代表性的木马主要有国外的 BO2000 与 Sub7，以及国内的冰河与广外女生等。
- **第三代木马：**这一代木马继续完善连接与文件传输技术，除此之外，还增加了可以穿越防火墙的功能，并出现“反弹端口”技术，如国内的灰鸽子等。
- **第四代木马：**这一代木马除完善之前的所有技术外，还增加了进程隐藏技术，使被控端更难发现木马的存在，如国内的广外幽灵与广外男生等。

温馨小贴士

世界上第一个电脑木马是出现在 1986 年的 PC-Write 木马。它伪装成共享软件 PC-Write 的 2.72 版本（事实上，编写 PC-Write 的 Quicksoft 公司从未发行过 2.72 版本），一旦用户运行该木马程序，则硬盘将被格式化。

2. 木马的启动方式

目前，木马最常用的启动方式为通过注册表、win.ini、system.ini、某些特定程序或文件以及文件关联 5 种，下面分别进行讲解。

1）通过注册表启动

它是最常用的木马启动方式。使用非常方便，但也容易被发现，因此一些设计者会在木马程序中加一个时间控件，以便实时监视注册表中自身的启动键值是否存在，一旦发现被删除，则立即重新写入，以保证下次 Windows 启动时自己能被运行。

2）通过 win.ini 启动

win.ini 文件的[Windows]中的 load 和 run 项会在 Windows 启动时运行，这给了木马可乘之机，它通过修改这两项的路径来进行启动。但由于 load 和 run 启动后会出现在配置文件“msconfig”中，极易让被控端发现，因此，该启动方式只被一些初级的木马设计者使用。

3）通过 system.ini 启动

木马程序在 system.ini 文件中加上其路径，这样 Windows 启动后木马也就随之启动，而且即使是以安全模式启动也不会跳过这一项，这样木马也就可以保证永远随 Windows 启动了，如尼姆达病毒就是通过这种方式启动的。

4）通过某特定程序或文件启动

这种启动方式又包括寄生于特定程序中与将特定的程序改名两种。

- ☑ **寄生于特定程序中：**木马设计者将木马和正常程序捆绑，程序在运行时，木马程序先获得控制权或另开一个线程以监视用户操作、截取密码等。这类木马程序的编写难度较大，需了解 PE 文件结构和 Windows 的底层知识。
- ☑ **将特定的程序改名：**这种方式常见于针对 QQ 的木马，如将 QQ 的启动文件 QQ2000b.exe 改为 QQ2000b.ico.exe（Windows 默认是不显示扩展名的，因此它会被显示为 QQ2000b.ico，而用户会认为它是一个图标），然后再将木马程序改为 QQ2000b.exe，这样当用户运行 QQ 时，实际是启动了 QQ 木马，再由 QQ 木马去启动真正的 QQ，从而获取 QQ 账号与密码。这种方式比上一种方式简单。

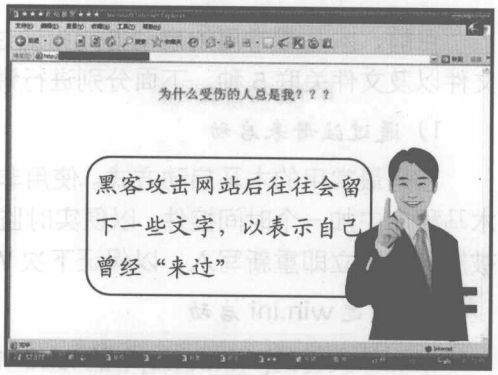
5）文件关联

这种启动方式是指木马程序会将自己与 txt 文件或 exe 文件关联，这样当用户打开一

个文本文件或运行一个可执行程序时，木马也就启动了。

1.1.4 黑客

“黑客”这个称谓源于英文 Hacker。最初，黑客是指那些独立思考、奉公守法的电脑迷，他们智力超群，从事黑客活动意味着对电脑的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献。而现在，黑客一般指电脑系统的非法侵入者，他们利用所掌握的技术毫无顾忌地非法闯入其他用户的电脑、某些敏感的信息禁区或者重要网站，以窃取重要的信息资源、篡改网站信息或者删除该网站的全部内容等。



◆ 图 1-2

尽管对黑客的态度褒贬不一，但黑客的破坏性是客观存在的。黑客已经成为网络安全的克星，自 2000 年初美国几大门户网站被黑客攻击以来，黑客对社会的危害更是触目惊心，如图 1-2 所示为某知名网站被黑客攻击后的效果。因此，黑客也成为影响电脑安全的重要因素之一。

1.1.5 有害信息

这里所谓的有害信息主要是指电脑系统及其存储介质中存在并出现的，以电脑程序、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，这类有害信息的来源基本上都来自境外，主要形式有两种，一是通过 Internet 进入国内，二是以电脑游戏、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。由于目前电脑软件市场盗版盛行，许多含有有害信息的软件就混杂在众多的盗版软件中。

1.2 电脑有哪些安全问题

在了解了影响电脑安全的主要因素后，下面来讲解电脑都有哪些安全问题，主要包括电脑硬件的安全问题、操作系统的安全隐患、电脑信息的安全问题与电脑网络的安全问题等内容，下面分别进行讲解。

1.2.1　电脑硬件的安全问题

电脑硬件由众多的电子元件组成，它是一个物理整体。因此，其安全问题主要是指环境、电压与静电等，其具体内容介绍如下。

- ☑ **环境**：由于这些电子元件都较精密，因此对于所处的环境有一定的要求，如室内温度应保持在 10~45℃之间，湿度范围最好在 30%~80%之间，周围环境应洁净等。只有满足这些条件，才能使其正常工作，否则易引起元器件损坏，从而影响电脑的正常运行。
- ☑ **电压**：电源的电压是否稳定对电脑硬件的影响也很大，正常范围应为 220V±10%，频率范围应为 50Hz±5%。由于日常所使用的电压经常发生波动，这种情况容易对电脑的电路与部件造成损害。所以，为电脑配备 UPS（不间断电源供应设备）是保护电脑硬件并使其能正常工作的首要措施。
- ☑ **静电**：静电对电脑硬件的危害最大，它不仅会影响电脑部件的正常工作，严重时可能会击穿 CPU、主板及内存等，因此，防静电很重要。

温馨小贴士

电磁干扰也是影响电脑硬件安全的因素之一，若电脑的周围有较强的磁场，则容易造成硬盘数据的丢失，影响电脑的正常运行，另外，还会使显示器发生花屏、抖动等故障。

1.2.2　操作系统的安全隐患

操作系统（Operating System，简称 OS）是平时使用的基本平台，各种文件操作和具体的应用软件使用都离不开它。不过，操作系统由于牵涉的方面太多，其安全性问题也相对突出。导致其不安全的主要原因主要包括其自身问题、进程管理、网络文件系统服务与后门等。

1. 操作系统自身的问题

操作系统是负责支撑应用程序运行环境以及用户操作环境的软件，同时也是电脑系统的核心与基石。因此，它是一个庞大的软件系统，且涉及了方方面面，从而不可避免地存在一些 Bug。

不仅其自身具有 Bug，操作系统在硬件兼容、软件冲突以及网络连接等方面也存在这种问题，一些黑客就利用 Bug 作为攻击用户电脑系统的途径。

2. 操作系统的进程管理

在操作系统中，用户可以创建进程，甚至可以在网络上的其他电脑中创建并激活远程进程，而且所创建的远程进程将继承创建进程的某些权限。当这些进程通过各种途径安装到电脑中时，其他用户就可以通过网络远程启动它们，从而使操作系统处于一个不安全的