电脑实用技巧问答丛书

电脑防毒杀毒绝招365问

苏武荣　编著

人民邮电出版社

电脑实用技巧问答丛书

电脑防毒杀毒绝招365问

苏武荣 编著

人民邮电出版社

内 容 提 要

本书以问答形式，通俗地介绍了电脑病毒的概念、来历、命名、分类、危害，病毒防范与管理措施，流行病毒现象及识别方法，以及实用杀毒工具使用方法。同时还介绍了病毒解剖基础知识、新病毒捕获采集方法与病毒实例分析技术。

本书通俗、易懂，注重实用性和可操作性。读者对象为广大电脑用户，包括电脑初学者、非计算机专业师生和工程技术人 员、普通办公人员和管理人员，以及所有电脑爱好者。

电脑实用技巧问答丛书

电脑防毒杀毒绝招365问

苏武荣　编著

责任编辑　贾福新

*

人民邮电出版社出版发行

北京崇文区夕照寺街14号

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

*

开本：850×1168　1/32　1996年5月第1版

印张：10.125　　1997年5月北京第2次印刷

字数：259千字　　印数：8 001—13 000册

ISBN7-115-06074-6/TN·283

定价：16.00元

前　言

为什么要学？

电脑病毒给电脑应用带来的危害和不良影响，是广大电脑用户人所共知的。

几年来，尽管人们做了许多反病毒工作，但病毒问题仍然困扰着电脑用户。本人从1989年发现“小球”病毒以来，一直关注着病毒问题，曾设计过一些防毒、杀毒程序，也写过一些病毒专文，对SCAN & CLEAN、CPAV、NAV、KILL、KV100/KV200、DBNET/DB95、TNTVIRUS、F－PROT等杀毒软件都作过分析，对一些出名的防病毒卡也作过研究，也走过软件固化成卡的路。但总觉得，杀毒软件仍难对付日益增多的新病毒，防毒技术也仍难控制新机理病毒的传播，并且一些通用的、广泛使用的防毒软件/防病毒卡更会受到新病毒的攻击，人们寄希望以一个防病毒卡和杀毒软件来解决病毒问题的愿望变得渺茫了。因此，作为电脑操作使用、开发应用与管理人员，能够自己掌握一些必要的电脑病毒知识和病毒防治技术，无疑是至关重要的。

应该学什么?

作为电脑用户,必须了解电脑病毒的概念、来历、命名、分类、危害,以便认清电脑病毒的真面目,并采取必要的病毒防范与管理措施。当病毒突破防线,入侵电脑系统时,应该认识是什么病毒在行动,这时必须懂得选择最有效的杀毒工具来消灭它。如果现有的杀毒工具还无法对付它,应该懂得怎样追杀新病毒,并捕获、采集新病毒样本,向有关部门或专家发出求救信号。《电脑防毒杀毒绝招365问》正是从这方面入手,系统地为读者提供了一个学习的教材。

本书有什么特点?

采用问答形式又强调系统性。书中列出365问,分为6个部分,按基本概念、防毒、识别病毒、杀毒、查新病毒等顺序,比较符合病毒防治的系统原则,条理性较强,也突出了防毒的重要性。同时,还将一些集成反病毒工具分成防毒程序和杀毒程序,分列在防毒部分和杀毒部分介绍,便于读者对同类工具软件加以比较、选择。在前言和每一部分的开头,都对该部分的主要内容作些简介,同时在目录中对主要问题加星号,以便读者能够抓住重点,避免问答式编目给读者带来的零乱感。

力求通俗、易懂,突出实用性。书中既回答了一些知识性、指导性的问题,又重点介绍了各种查毒、防毒、杀毒工具软件的操作使用,而在介绍时并不是对这些软件使用说明的简单汇编或翻版,而是力图站在用户的角度上,讲解实用功能的综合使用方法,对于一些不常使用的功能就不作介绍。目的是使读者能够轻松地学习如何防毒、杀毒,认识常见病毒,了解病毒的结构和行为。

本书有什么内容?

全书各部分安排如下:

第一招:了解电脑病毒基本知识。介绍电脑病毒的起源与由来,

病毒概念与特性，病毒的定名与分类，以及病毒的激发破坏与危害情况。希望读者能够较全面地了解电脑病毒的本质，认清其真面目。

第二招：建立预防观念采取防毒措施。通过实例强调树立“预防为主、消防结合”的病毒消防观念的重要性，并指明了防毒原则。介绍了广谱防病毒程序 TIG.SYS、VSAFE、BOOTSAFE，以及防病毒卡的使用技巧与注意事项。特别指出了防毒技术的机理，并比较了 TIG.SYS 等防毒软件与通用防病毒卡的性能特点。希望读者能够建立正确的病毒消防观念，并采取正确的防毒措施，防患于未然。

第三招：识别百种常见病毒现象。介绍由病毒引起的系统异常现象，百种常见病毒现象和主要特征，以及推荐使用的杀毒工具。希望读者能够识别常见病毒，以便及早发现病毒。

第四招：掌握实用工具杀毒技能。指出杀毒技术的机理，给出了“杀毒原则”。介绍了 KILL、KV200/KV100、DB95/DBNET、SCAN & CLEAN、CPAV/MSAV、NAV、TNT、SDSCAN/UTSCAN 和 F-PROT 等常用杀毒工具使用技巧与注意事项。希望读者能够掌握实用工具杀毒技能，以便在发现病毒时能够使用合适的杀毒工具来清除病毒。

第五招：学习病毒解剖基础知识。介绍一些与病毒有关的 DOS 系统结构和重要参数，并简介了 DEBUG、PCTOOLS、NORTON 等调试工具软件的使用方法。希望读者能够掌握病毒解剖的基础知识，为捕杀新病毒作准备。

第六招：追杀捕获各种新的病毒。介绍人工识别病毒的方法，以及采集新病毒样本的技术。按病毒的寄生对象和传染机理，用不同方法从不同角度剖析了每一种类型的代表性病毒，并分析了它们各自的共性和特点。所归纳的诊治机理对于新病毒具有普遍的适用性。希望读者能够掌握各类病毒的特点和防治方法，能够对现有的杀毒、防毒工具还无法清除的新病毒或变种病毒予以诊治、排除。该部分对于希望用 DEBUG 等工具获取、分析病毒源程序并自行消除病毒的读者，无疑具有很好的参考价值。

您应该怎么学?

本书6招365问,您既可以按顺序系统地阅读,也可以选择感兴趣的问题查阅。如果您是一个初学电脑的用户,您应该认识电脑病毒的真面目,学习如何防毒、杀毒,以便增进您学习使用电脑的兴趣。那么,您应该学习第一至四招。如果您是一位在校学生,或者是一个电脑迷,您们是接触病毒最多的一群,认识常见的病毒,学习如何防毒、杀毒,并了解病毒的结构,了解病毒的行为,成为查毒能手,您便又获得一种特别的本领,这很可能是您求职、交友的敲门砖。那么,您不妨练习一至六招,特别是要攻读最具挑战性的第六招。当然,本书也可能会作为您应付"信息安全与病毒防治"课程的作业、考试的奇招。如果您是一个电脑专业工程师,您应该认识常见的病毒,了解病毒的结构,了解病毒的行为,做出更安全的信息系统。这是您责无旁贷的责任。那么,您应该赶快学完第一至四招。有空的时候,不妨再看看第五、六招。临时抱佛脚,也灵!如果您是一位办公人员,或者是一个家庭电脑使用者,您应该认识病毒可能有的破坏行为,建立防毒杀毒常识,以便获得上级或亲友的赞赏。那么,您最需要了解第一、二、三招,发现病毒时,马上学习第四招,也可以依样画葫芦。如果您是一个部门领导,您应该了解病毒所破坏的是无价的数据,如何使员工建立正确的防毒杀毒观念,创造一个无病毒的环境。那么,您最起码要看看第一、二招。有兴趣的时候,还可以查阅一下第三、四招。

一年365天,但愿《电脑防毒杀毒绝招365问》天天伴随您,让您摆脱电脑病毒的烦恼。

苏武荣

1996年1月于福州

目　录