

Robert Slade's

GUIDE TO COMPUTER VIRUSES

Second Edition

Springer

New York

Berlin

Heidelberg

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Santa Clara

Singapore

Tokyo

Robert Slade's

GUIDE TO COMPUTER VIRUSES

How to avoid them,
how to get rid of them,
and how to get help

Second Edition

With 19 Illustrations and a Diskette



Springer

Robert Slade
Vancouver Institute for Research into User Security
3118 Baird Road
North Vancouver BC
Canada V7K 2G6
Email: roberts@decus.ca

Cover photo © Omikron, Science Source/Photo Researchers.

Library of Congress Cataloging-in-Publication Data

Slade, Robert.

[Guide to computer viruses]

Robert Slade's guide to computer viruses : how to avoid them, how
to get rid of them, and how to get help. — 2nd ed.

p. cm.

Includes bibliographical references and index.

ISBN-13:978-0-387-94663-4 e-ISBN-13:978-1-4612-2384-9

DOI: 10.1007/978-1-4612-2384-9

1. Computer viruses. I. Title.

QA76.76.C68S55 1996

005.8—dc20

95-49098

Printed on acid-free paper.

© 1996, 1995 Springer-Verlag New York, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production coordinated by Impressions and managed by Bill Imbornoni; manufacturing supervised by Jeffrey Taub.

Typeset by Impressions Book and Journal Services, Inc., Madison, WI.

9 8 7 6 5 4 3 2 1

ISBN-13:978-0-387-94663-4 Springer-Verlag New York Berlin Heidelberg SPIN 10524179

To Gloria

PREFACE TO THE SECOND EDITION

For those who didn't buy the first edition, welcome aboard. For those who did buy the first edition, welcome back, and thanks for making the second edition possible.

For those who bought the first edition and are standing in the bookstore wondering whether to buy the second, what's in it for you? Well, for one thing, it's smaller. (No, no! Don't leave!) I tried to make the first edition a kind of master reference for antiviral protection. That meant I included a lot of stuff that I thought might possibly be helpful, even if I had some doubts about it. This time I've tried to be a little more selective.

I've added a little more material to Chapter 4 (Computer Operations and Viral Operations) dealing with the question of computer viruses infecting data files and the new "macro" viruses. I've added two new sections to Chapter 7 (The Virus and Society). One looks at the increasing problem of false alarms while the other looks at the ethics of virus writing and exchange.

Appendices B and C, dealing with software reviews, have had a lot of changes. A number of outdated or less important products have been removed. New critiques of the latest products on the market are also included. A number of the original reviews have been rewritten to reflect the latest versions and technology. Some evaluations, however, have been left unchanged. Even in the rapidly changing world of antiviral software, many products remain essentially unchanged from release to release.

The Vendor and Contacts Listing in Appendix D has been updated to reflect the latest information, of course. I have also tried to give the listing more structure and I hope this makes it easier to use.

The Antiviral BBS Listing, which formerly made up most of Appendix F, has been removed. Maintenance of the BBS list became an enormous chore for very questionable return. The decline in overall quality of the Fidonet and VirNet virus discussion groups was another factor. Finally, the enormous growth in access to the Internet has made the list less important. I have included some pointers regarding sources of antiviral information online.

The disk included with the first edition held a variety of antiviral software for the MS-DOS platform and one program for the Mac.

However, I had forgotten to include Tim Martin's "special purpose" KILLMONK program, and guess what everyone needed? This time I have included virus information, as well, courtesy of the Virus Test Center of the University of Hamburg. Amiga, Atari, MVS, and UNIX users also get some goodies. Unfortunately, until overwhelming sales convince Springer-Verlag that the book rates a companion CD, something had to be removed to make room. This does *not* reflect on the quality of the Flu-Shot and Integrity Master programs: I still consider them to be the best in their respective categories and recommend you find and use them.

You learn an awful lot about the English language when you write a book, especially when you're an old science grad who grew up in the days of "Humanities" instead of English classes. It's very humbling to realize just how inconsistent you are in the use of the language, terms, and references, particularly when science is so dependent upon consistency. The first edition would have been even more of a disaster without the expert editing (copy, proof, and literary) of my-best-friend-who-is-also-my-wife, Gloria.

In this edition, the publisher (Springer-Verlag), the typesetting firm (Impressions Book and Journal Services, Inc.), and I have tried to improve the level of stylistic coherence. In addition, I've tried to reflect the changes in technical English that are a result of the influence of "online English." For example, "E-mail" is now "email," because techies aren't fond of shift keys and use the hyphen only to identify command-line switches. "Trojan horse" is a common rather than proper noun in the data-security field and has nothing to do with Troy. (Those interested in the linguistic aspects of the online world are referred to *The New Hacker's Dictionary*. See the book review in Appendix E.)

In the course of preparing the second edition, we've identified a number of style issues that have not been addressed by the current style guides. Reviews of technical literature haven't helped an awful lot, since there don't seem to be any standards. We have tried to find the most common usage, although that is often hard to determine. (I must say that Laurie McGee, the copyeditor for this edition, has been able to find the most astonishing range of authorities for items that I thought were still in the realm of slang.) We hope the result is a more polished, lucid, and useful reference for you, the reader.

PREFACE TO THE FIRST EDITION

If you have bought this book in a panic because you suspect that your computer is already infected by a virus, please turn to Chapter 2—the “Beginner’s Panic Guide to Viral Programs.”

The only audience the book is *not* for is serious antiviral researchers—and those looking for a “how to write” cookbook. The CIO of a Fortune 1000 company needs to know the reality and scope of the problem, and how to “shortlist” the available resources. The technical manager needs product contact and assessment information. The technical support or help desk worker needs accurate information on how to deal with the problem. Small business owners need to know how to protect themselves and their business information. The computer retail and repair person needs to avoid infecting his or her customers. The home user needs all the help he or she can get.

The book is written to apply to all systems—micro, network, and mainframe. The concepts are the same in all cases. Examples are drawn from many systems, although MS-DOS predominates since the concepts are clearest when presented with MS-DOS examples. Technical experts working in other operating systems should be able to extrapolate from the examples given here—the average user shouldn’t have to worry too much about the technical differences. Contacts are listed for Amiga, Atari, Macintosh, MS-DOS, OS/2, and UNIX systems.

The text of the book has been written with the average nontechnical computer user in mind. Jargon and assumptions about familiarity with technical concepts are kept to a minimum. At the same time, based upon experience in seminars, the material is sufficiently esoteric to be new and of interest to technical experts outside the virus research field. The material is based upon a weekly column that has been vetted for accuracy by the best of the international virus research community, as well as upon seven years of compilation. The contact and review information is the result of thousands of hours of compilation and testing over four years.

Not all parts of the book will appeal to all audiences. For example, even the “Beginner’s Panic Guide” might be beyond the absolute neophyte who doesn’t yet know how to get a directory listing. I’m sorry, but to write a step-by-step guide at that level would just make the book too big. By the same token, experienced technical people will find the

description of basic computer functions to be quite elementary (although I hope not simple to the point of inaccuracy).

However, there should be something in the book for just about everyone. Even the executive or manager who can't read his or her own email should be able to understand the scope and concepts of the problem and appreciate the policies and procedures to minimize risk. In addition, given the wide range of viral activities and the scarcity of accurate information (not to mention the abundance of rumors and myths), even the most technically literate should find new information regarding defense and recovery. Hopefully for the vast majority of "intermediate" users, this should be a help, comfort, and resource.

I hope nobody who buys the book will ever need it. The odds, according to the best available studies, seem to indicate that a quarter of those who do will use it within two years. About 25 books have been published on this topic altogether. Many are over three years old, a lifetime in a field where software "generations" are measured in months. A number are written to promote a specific product. Those few remaining that are reasonably accurate are intended for the research, academic, or technical audience, and not for the average manager or user.

Most popular personal computer magazines have reviewed anti-viral software from time to time. These reviews tend to cover the same few products each time and have been almost universally condemned by the research community. The reviews are technically suspect and subjective. Mediocre products are consistently given the highest reviews, tending to indicate that rankings are assigned on the basis of advertising budget.

It is difficult to decide a proper order for the presentation of this material. To a large extent, the chapters are independent from each other and can be read in almost any order. I think this order makes as much sense as any, but feel free to read as you please. Much of this is intended to be reference material, although I hope it is readable as well. Also, some material is covered in more than one place. For example, defining the terms "stealth" and "polymorphism" requires much technical detail, so you will find as much information on them in the definitions chapter as in the chapter on viral functions and operations, possibly more.

Chapter 1 Introduction: Definitions, Jargon, and Myths

What is a virus? What related problems are not viral? What are the other types of "malware"? Terminology of viral programs and virus research.

Chapter 2 Beginner's Panic Guide to Viral Programs

What to do if you (or a friend) is infected and have made no preparations.

Chapter 3 History and Examples of Viral Programs

Some cases and descriptions of major viral programs or attacks on MS-DOS, Mac, and mainframes. The descriptions give some background and framework to the functions discussed in Chapter 4.

Chapter 4 Computer Operations and Viral Operations

Discussion of computer functions used by viral programs. Why a "perfect" defense isn't possible. How viral programs attack, and what to look for.

Chapter 5 Antiviral-Protection Checklist

How to protect yourself and reduce the risk of virus infection. Policies, procedures, and tools you already have to detect infections.

Chapter 6 Antiviral Software and Evaluation

What the types of antiviral software are, and their strengths and weaknesses. How to choose the best type for your situation.

Chapter 7 The Virus and Society

Opinion and social implications concerning:

- Hackers, crackers, phreaks, and virus writers
- The "no sharing" rule
- "Teaching" virus writing
- Trends in virus technology
- The scope of the problem
- Computer "Third World" hygiene

It may seem strange, but the appendices are longer than the book. They include:

- A Frequently Asked Questions
- B Quick Reference Antiviral Review Chart
- C Reviews of Antiviral Products
- D Antiviral Vendors and Contacts Listing
- E Antiviral Bookshelf
- F Sources of Information On-Line
- G Glossary (terms used in antiviral research)

H Antiviral Checklist

I Antiviral Files on Accompanying Disk

Included with this book is a disk with antiviral software for MS-DOS and Macintosh systems. All of the programs are functional and effective, and you are allowed to try any of them that you wish. Some are shareware, and if you continue to use the programs you should register them with the authors. Full details are included with the documentation in each archive file.

The disk is a 3½" high-density (1.44 megabyte) MS-DOS formatted disk. I am in full sympathy with those who find this to be a problem and can only ask for your forbearance in what is, after all, a matter of practical constraint in production. This format has been chosen as the most accessible to the greatest number.

I became interested in the virus field following studies into the social aspects of computing and the risks of various types of technologies. In 1987 the first major virus infestations occurred, taking them out of the realm of academic curiosity and into the position of real security threats. Acting initially as the unofficial archivist for the budding research community, I eventually specialized in evaluating antiviral products, maintaining what have come to be termed "Mr. Slade's Lists" of antiviral contacts, products, and BBSes. Since 1991 I have written a weekly "tutorial" column for the on-line community. Most recently this has been augmented by a weekly "news and gossip" column.

In a very real sense I did not write this book, I only compiled it. The field of virus research is very small, but even so the level of technical detail is so wide-ranging that no one person can encompass it all. To a large extent, then, this is the work of the international virus research community, and primarily those who meet around the digital campfire known as *VIRUS-L* or *comp.virus*, moderated through the dedication of Ken van Wyk (as of January 1996, moderated by Nick FitzGerald). The attendees are too many to name here. Some get named in the body of the book someplace—most don't. All have my thanks.

William D. Knipe did the cartoons.

Thanks to Dr. Kinsey who observed that you can eventually get some interesting results out of any field of research, as long as you collect enough data.

Thanks to all those computer users who, in 1989 and 1990, kept asking which antiviral software was the best and who got me into this.

CONTENTS

	Preface to the Second Edition	<i>vii</i>
	Preface to the First Edition	<i>ix</i>
CHAPTER 1	Introduction: Definitions, Jargon, and Myths	3
	What and What Not	3
	Related Programs	6
	Special Terms	12
	Viral Myths	16
CHAPTER 2	Beginner's Panic Guide to Viral Programs	29
	Don't Panic	29
	Power	31
	Backups	32
	Getting Started	33
	Assume You're Wrong	37
	Scanners	38
	Other Antivirals	39
	Local Reports	41
	Weird Behavior	43
	Cleanup	44
CHAPTER 3	History and Examples of Viral Programs	47
	Early History	47
	Viral Examples	54
CHAPTER 4	Computer Operations and Viral Operations	91
	Boot Sector Infectors	91
	File Infectors	97
	The Viral Use of Computer Operations and Functions	103
	Data Versus Programs	121
CHAPTER 5	Antiviral-Protection Checklist	131
	Antiviral Checklist	132
CHAPTER 6	Antiviral Software and Evaluation	145
	Standards and Measures	145
	User Reaction and Interface	150

	Types of Antivirals	152
	Other Considerations	161
	LAN Security	165
CHAPTER 7	The Virus and Society	169
	The Virus Community: Two Solitudes	171
	Viral Morality	177
	Trust	185
	Scope	189
	False Alerts	193
	Future Trends	196
APPENDIX A	Frequently Asked Questions	205
APPENDIX B	Quick Reference Antiviral Review Chart	217
APPENDIX C	Reviews of Antiviral Products	227
	Introduction to the Antiviral Reviews	227
	Activity Monitors	227
	AntiVirus-Plus (Techmar)	227
	InocuLAN (Cheyenne)	230
	Immune II (Higher Ground Diagnostics, Inc.)	232
	Change Detectors	235
	DISKSECURE (Padgett Peterson)	235
	HS 3.58 (Stroem System Soft)	237
	Integrity Master (Stiller Research)	239
	SafeWord Virus-Safe (Enigma Logic)	243
	SIX, BRECT (Zen Works)	246
	Vaccine/Sweep/D-Fence (Sophos)	248
	Scanners	250
	Antiviral Toolkit Pro (KAMI)	250
	F-PROT (Frisk)	252
	F-PROT Professional (Command/Data Fellows)	256
	IBM AntiVirus (IBM)	257
	LANProtect (Intel)	260
	VirAway (Techmar)	262
	Vi-Spy (RG)	264
	Multilayered Software	266
	AVAST! antiviral (ALWIL Software)	266
	Data Physician Plus! (Digital Dispatch)	268
	Dr. Solomon's Anti-Virus Toolkit (S&S International)	272
	F-PROT 1.xx (Frisk)	275

	Norton AntiVirus 3 (Symantec/Norton)	277
	SCAN suite (McAfee Associates)	280
	Thunderbyte Utilities (Thunderbyte)	283
	VET (Cybec)	286
	Virex for the PC (Datawatch)	288
	Virus Buster (Leprechaun)	291
	General Security Software	293
	Network Security Organizer (Leprechaun)	293
	PC/DACS (Mergent)	295
	PC-Vault (Johnson)	297
	SAFE (Micronyx)	299
	Security Guardian (Command)	301
	Watchdog (Fischer)	303
	Miscellaneous	306
	HyperACCESS (Hilgraeve)	306
	Rising Anti-Virus Card (Rising Computer Science)	309
	Watchdog (Fischer)	311
	Atari	313
	Chasseur II (Vidovic)	313
	FLIST and FCHECK (Lindberg)	314
	Protect6 (Osterud)	315
	VKILLER (Woodside)	315
	Amiga	316
	BootX (Stuer)	316
APPENDIX D	Antiviral Vendors and Contacts Listing	319
APPENDIX E	Antiviral Bookshelf	345
	Virus	345
	<i>Computer Viruses and Data Protection</i> , Ralph Burger	345
	<i>A Short Course on Computer Viruses</i> , Fred Cohen	347
	<i>Computers under Attack: Intruders, Worms and Viruses</i> , Peter J. Denning, ed.	348
	<i>A Pathology of Computer Viruses</i> , David Ferbrache	349
	<i>The Computer Virus Desk Reference</i> , Chris Feudo	350
	<i>The Computer Virus Crisis, 2nd ed.</i> , Fites, Johnston, and Kratz	351
	<i>Computer Virus Handbook</i> , Harold Joseph Highland	352
	<i>Rogue Programs: Viruses, Worms, and Trojan Horses</i> , Lance J. Hoffman, ed.	354
	<i>Computer Viruses and Anti-Virus Warfare</i> , Jan Hruska	355
	<i>The PC Virus Control Handbook</i> , Robert Jacobson	357
	<i>PC Security and Virus Protection Handbook</i> , Pam Kane	358

	<i>The Computer Virus Handbook</i> , Richard Levin	359
	<i>The Little Black Book of Computer Viruses</i> , Mark Ludwig	360
	<i>Naissance d'un Virus</i> , Mark Ludwig (translated by Jean Bernard Condat)	362
	<i>Virus!: The Secret World of Computer Invaders That Breed and Destroy</i> , Allen Lundell	362
	<i>Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System: What They Are, How They Work, and How to Defend Your PC, Mac or Mainframe</i> , John McAfee and Colin Hayes	363
	<i>Inside the Norton AntiVirus</i> , Norton/Nielsen	365
	<i>Virus Detection and Elimination</i> , Rune Skardhamar	365
	<i>Dr. Solomon's Virus Encyclopedia</i> , Alan Solomon	366
	<i>PC Viruses: Detection, Analysis, and Cure</i> , Alan Solomon	367
	<i>Survivor's Guide to Computer Viruses</i>	369
Related		370
	<i>It's Alive!</i> , Fred Cohen	370
	<i>Computer Crime</i> , David Icove/Karl Seger/William VanStorch	371
	<i>Computer Ethics</i> , Deborah Johnson	372
	<i>Computer-Related Risks</i> , Peter Neumann	372
	<i>The New Hacker's Dictionary</i> , Eric Raymond	373
	<i>NetLaw: Your Rights in the Online World</i> , Lance Rose	374
	<i>Computer Security Basics</i> , Deborah Russell and G. T. Gangemi Sr.	375
	<i>Digital Woes</i> , Lauren Wiener	376
Fiction		378
	<i>Shockwave Rider</i> , John Brunner	378
	<i>When H.A.R.L.I.E. Was One</i> , David Gerrold	379
	<i>The Tojo Virus</i> , John D. Randall	380
	<i>The Adolescence of P-1</i> , Thomas J. Ryan	381
	<i>Terminal Compromise</i> , Winn Schwartau	381
	<i>Snow Crash</i> , Neal Stephenson	384
APPENDIX F	Sources of Information On-Line	387
APPENDIX G	Glossary	389
APPENDIX H	Antiviral Checklist	401
APPENDIX I	Antiviral Files on Accompanying Disk	403
	UNZIP.EXE (MS-DOS)	403

KILLMNK3.ZIP (MS-DOS)	403
FP-220.ZIP (MS-DOS)	404
DISINF36.HQX (MAC)	405
DS242.ZIP (MS-DOS)	406
Virus Information	407
AMIGAVIR.ZIP, ATARIVIR.ZIP, INDEX.793, MACVIR.*, MSDOSVIR.ZIP, MVSVIR.ZIP, and UNIXVIR.ZIP	407
Index	409

RICHARDS' LAWS OF DATA SECURITY:

1. *Don't buy a computer.*
 2. *If you do buy a computer, don't turn it on.*
-

MEMOIRS OF A (RELATIVE) VIRUS RESEARCHER

"Hi, Rob."

"Oh, hi, Larry."

"You busy?"

"Oh, reading through message logs for virus-related stuff like usual."

"Geez, every time I call you're always doing that! How much time do you put in on that every week, anyway?"

"Oh, about 60 hours altogether, I guess."

"Rob, you know you're wasting your time on that stuff. I mean, it may be interesting, and all that, but no one is ever going to care about it. How often do you see a virus on somebody's machine, anyway?"

"Oh, it happens."

"Yeah, well . . . anyway, you got a minute?"

"Always time for my favorite brother-in-law. You still setting stuff up on your friend's machine?"

"Yeah, and I need some more space. There's a directory in Windows called TEMP and it has a whole bunch of files with .TMP extensions. Do I need them?"

"Nope. Like it indicates, they're just temporary files that Windows hasn't cleaned up when it finished with them. As long as Windows isn't running, just dump 'em."

"OK, good. That'll get me about a dozen megs. What about these files all over the place with .BK! extensions?"

"They're WordPerfect backup files. If your friend doesn't want them, you can get rid of them, too."

"You mean I have to go through every directory and delete them?"

"No, you can do it more easily. Remember that SEEK program? Ask it to look for them and redirect the output to a file. That way you get a list of all the filenames with a full pathname, and you can edit the file into a batch file to delete them all."

"Oh, OK, yeah, I can see that. Oh, by the way, I saw something strange just a minute ago. When I was rebooting the machine, right at the beginning it said 'Your PC is now Stoned.' Do you know why it did that?"

"Yes, as a matter of fact I can tell you exactly what it means, Larry. Your friend's computer has a virus."
