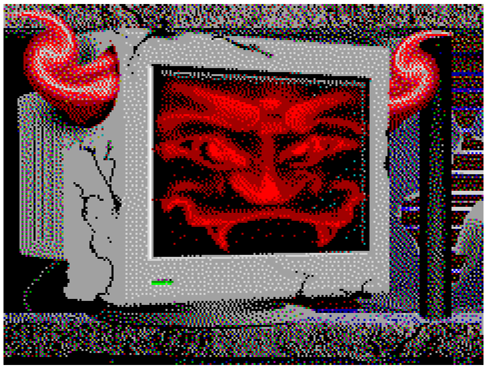

COMPUTER VIRUSES
AND THE
"FALSE AUTHORITY SYNDROME"

_***

SIDEBAR STORIES

WHAT IS A BOOT SECTOR VIRUS?

Every IBM PC floppy disk has a reserved area known as the "boot sector." Every floppy disk's boot sector contains a small program known as the "boot code."

If your computer detects a floppy in the A: drive when it boots, it executes the boot code which in turn looks for an operating system on the floppy. If the boot code doesn't find an operating system, it will display "Non system disk or disk error" on your video monitor. A boot sector virus infects the floppy disk's boot code and spreads to your computer's hard disk if you boot with an infected floppy in the A: drive.

Thanks largely to False Authority Syndrome, users now often panic at the first sign of odd computer behavior, sometimes inflicting more damage on themselves than any virus could do on its own (assuming they even had a virus in the first place).

Ross Greenberg earned international fame as one of the pioneers in IBM PC antivirus software. He went into semi-retirement in his mid-30s. Greenberg continues to lecture about viruses, wrapping up with a simple analysis of how he made his fortune: "I'd still be slaving away at a desk for another 25 years if people backed up [their computer data] and kept a cool head."

VIRUS ALERTS AND ONLINE SERVICES

Almost all "alerts" of viruses in files on major online services prove unfounded. False alerts generally crop up in one of four common scenarios: an antivirus program incorrectly detected a boot-sector virus in an executable file; an antivirus program incorrectly detected an executable-file virus in an executable file; an antivirus program incorrectly detected a virus in a data file; an antivirus program correctly (or incorrectly!) detected a boot-sector virus on a floppy or hard disk, and the user mistakenly thinks he got infected from a downloaded file.

In some cases a user who posts the virus warning doesn't know what file he downloaded (if any) or even what areas he visited on the online service! CompuServe sysop Don Watkins deals with these people all too frequently: Something weird happens to their computer, and they remember using CompuServe recently, and they believe the myth about viruses spreading mostly in downloaded files... They assume that their computer's weirdness must be caused by a virus, and that CompuServe somehow transmitted it to them. They log on again and scream bloody murder, saying things like 'Why don't you idiots check your files for viruses?' and so forth. We ask if they checked their computer with an antivirus program and they usually say no. People used to blame power surges and lightning strikes for causing their problems. Now they blame viruses.

Watkins knows the complicated nature of computers. "A lot can go wrong with them and viruses make for a 'sexy' explanation," he notes. "Remember, before viruses came along, everybody blamed the computer's weirdness on lightning strikes and power surges."

If you plan to shout "virus!" on a BBS or major online service, you should include at least the following information in your warning message: the name & version number of the software which detected the virus the specific identifying name of the virus it detected, information on whether the virus infects boot sectors or standard executable files, the downloaded filename which contained the infected file, the "download count" which tells how many other users retrieved the file in question before you post your warning.

Sysops on major networks check first to see if the virus in question infects only the "boot sector" of floppies & hard disks. If this proves the case, the sysops will have to diplomatically tell the user he left a bogus virus report.

Sysops then check the file's "download count" to see how many users had previously retrieved it. If hundreds of people have downloaded it, dozens will have checked it for viruses. The download count can tell sysops if a user left a bogus virus report.

Sysops then check the date the virus first appeared and compare it to the file's upload date. They may have received the file in 1990 for example, yet the virus in question didn't appear until 1993. If so, the sysops will know the user left a bogus virus report.

Sysops may want to know the name and version number of the antivirus software which detected the virus. If the user has an outdated copy or a version known to contain bugs, the sysops will ask the user to get a newer version.

EMPLOYEE FIRED FOR NOT HAVING A VIRUS

A programmer we'll call "Monty" lost his job in 1992 when his boss erroneously claimed to have found a virus on his computer. The boss had checked Monty's computer with an antivirus program and it alerted on
software Monty had written for the company. The antivirus software said the company's program had "changed," and the change might have involved a computer virus. Monty had recently recompiled the program, which certainly would account for why it had changed. But Monty's boss didn't consider this. He immediately jumped to the following conclusions: if a virus might have changed the program, then a virus must have changed it; since a virus changed the program, the virus must be part of the program; since a virus is in the program, Monty must have written the virus; since Monty wrote the virus, he must have written it on company time. Monty arrived at work the next day only to have his boss meet him at the front door. Escorted to a conference room, Monty faced a number of bigwigs who accused him of writing a virus on company time. They fired him on the spot and gave him a box containing the personal contents of his desk. Monty's boss escorted him out of the building.

Monty filed for unemployment benefits, but the company refused to pay. Monty had no choice but to hire a lawyer. The firm's lawyer learned what had really happened and he advised them to settle out of court. The company quickly changed its tune - Monty lost his job when management reorganized the computer department! They gave him a belated "severance bonus" and a glowing recommendation letter. And of course Monty received full unemployment benefits.

The story has a happy ending. Another company hired Monty for more pay. He says his ex-boss still works at the old firm and calls it "poetic justice for them."

THE MICHELANGELO SCARE

Researchers discovered a new computer virus in 1991. An examination showed it would erase IBM PC hard disks each year on March 6 - the birthday of renaissance painter Michelangelo. The name stuck.
Michelangelo remained an obscure threat until January of 1992, when a major U.S. computer manufacturer announced it had accidentally shipped 500 PCs carrying the virus. Another computer manufacturer issued a press release the same day announcing their decision to include

antivirus software with every computer.

This coincidence probably intrigued the major newswires; reporters sniffed for a story. United Press International found one when it talked to a group calling itself the "International Partnership Against Computer Terrorism." They also interviewed antivirus mogul John McAfee (himself no stranger to the media). UPI filed a newswire saying "hundreds of thousands of computers around the world" might fall victim to Michelangelo on March 6. A few days later, another major company admitted it accidentally distributed 900 floppy disks infected with Michelangelo. Then a Reuters reporter filed a newswire claiming the virus resided on "millions of personal computers around the world," with an estimate of five million attributed to John McAfee. A "data recovery consultant" named Martin Tibor started getting media attention around this time, offering quotes like "I'm finding virus catastrophes everywhere" and "I see the victims of viruses all the time." Antivirus firms snapped to attention as the media grew fascinated with Michelangelo. Symantec scored a publicity coup when it ran a full-page ad announcing a free detection utility. Representatives from antivirus firms - some of them employed in marketing departments - called Michelangelo a "very serious threat."

Newspapers and TV stations ran "local impact" stories with quotes largely supplied by local computer salesmen. These "experts" simply parroted what they'd read in newspapers the previous day. Hysteria swept across the planet as frightened users drained store shelves of antivirus software. When the software dried up, customers purchased books about viruses.

Many virus researchers dismissed the hysteria as unwarranted, but reporters wouldn't listen to them. Stories about Michelangelo rarely questioned the astronomical estimates. And estimates about the impending disaster continued to rise - a Reuters newswire at the height of the scare claimed one out of four PCs in the U.S. would fall prey to Michelangelo! The tide of reporting changed on March 4 - just two days before "M-Day" - when an Associated Press editor finally listened to furious experts. Newswire stories started to focus on the fear sweeping the world rather than the virus itself. But this didn't stop the incredible hysteria. March 6 came in like a lion... and went out like a lamb. Worldwide reports ranged from 10,000 to 20,000 computers, not five million. Perplexed reporters phoned experts who had accurately predicted Michelangelo's impact. "Why did everybody else claim five million?" a reporter would ask. "Because you talked to all the wrong people, that's why," an expert would respond. The Michelangelo virus had turned into a worldwide media fiasco. Red-faced newswire agencies stopped reporting about it the very next day. Indeed, all major newswires had stopped reporting about it by 6am Eastern time the next day! They didn't run a single story about computer viruses for the next 13 days.

Opinions about this fiasco fall into two groups. Those who gave estimates in the millions say publicity itself made all the difference. They believe computer users learned about Michelangelo before it wreaked havoc. These people do have a point: the virus attacked 10,000 or more PCs despite worldwide hysteria.

Experts who predicted in the thousands point to data showing Michelangelo didn't have a big foothold - it just had big publicity. They believe fear about the virus created a number of "false reports" when users panicked at the first sign of an odd computer behavior. The experts do have a point: panicky users often inflict damage on their computers and then blame it on a virus.

ABSTRACT

Many people in the computer field sound confident when they talk about computer viruses - yet very few have adequate knowledge of this technically obscure subject. Most fall prey to what some virus experts call "False Authority Syndrome," and it contributes significantly to the spread of fear & myths about computer viruses. I will persuade readers to question the credentials of anybody (myself included!) who claims to speak with authority on this subject.

This treatise deals with virus issues related to the IBM PC family of computers, but its main thrust about False Authority Syndrome spans all computing platforms. Readers should have at least a basic concept of viruses, networks, BBSs, and online services like CompuServe. It will also help if readers understand the basics of a "boot sector" and know about the Michelangelo computer virus scare of 1992. (You'll find sidebar stories on these topics if you need them.)

AUTHOR BIOGRAPHY

Rob Rosenberger is an internationally recognized expert on computer virus myths & hoaxes. He has consulted on computer virus and computer security books written by Janet Endrijonas, Pamela Kane, and Richard B. Levin. Rosenberger also serves as a consultant on computer virus issues to PC Magazine technical editor Neil Rubenking.

Rosenberger's credentials include a critically acclaimed 1988 treatise on computer virus myths which has appeared in over 220 books & publications around the world in four official translations. [Plus at least two unauthorized translations: Hebrew & Arabic versions surfaced during "Operation Desert Storm."] U.S. Defense Department point papers cite Rosenberger's treatise on virus myths as a bibliographic source. Rosenberger made news in 1992 when he predicted "only 10,000 hits total, worldwide" during the Michelangelo virus scare. [Newswire reports claimed at least five million computers would lose their data; some reports put the figure as high as 15 million computers in the U.S. alone.] His research into global media hysteria surrounding the virus appeared as a front-page analysis article in ISPNews, a computer security industry publication. Rosenberger has written or co-authored a number of virus-related articles for magazines in the U.S. & Britain. He also has starred in a "Computer Survival Series" video about viruses. Completely unrelated to his computer virus credentials, Rosenberger has authored three books & a video about the "shareware" concept and has written on the subject for numerous magazines. He lectures around the country about shareware and has consulted on books written by David D. Busch, Michael Callahan, and John C. Dvorak. Rosenberger's speaking/lecture experience covers a range of subjects including computer viruses, Borland programming languages, and the "try before you buy" concept known as shareware. His speaking highlights include: National Academy of Sciences Computer Working Group (1989) American Chemical Society Convention, Lead Speaker, Software Track (1989) PC-Expo Chicago panelist (1993) Regular panelist, Shareware Industry Conference (1990-94).

FALSE AUTHORITY SYNDROME

A couple of years ago I dropped by the Software Etc. store in Fairview Heights, Illinois just to browse. Another customer had come in before me and told an employee he had a problem with his video monitor. The employee warned the customer he had contracted a newly discovered computer virus, which he proceeded to describe in great detail. I interrupted the employee. "Sir, you have it completely wrong. That virus doesn't exist. It's the latest hoax." "Oh, no," the employee replied. "We've got e-mail reports from our sales headquarters telling us to keep our eyes open for it." To which I countered, "Some upper-tier sales manager has been duped and is telling you BS. McAfee Associates and others have issued public statements dismissing that virus as a hoax. What you've described simply cannot be done by any virus. Period." I then turned my attention to the customer. "Stop listening to this guy. You don't have this magical virus he's describing because it simply doesn't exist. You have some other problem with your video monitor."

What credentials does this salesman have in the field of computer viruses? He may have flipped burgers at a McDonald's restaurant two weeks ago for all we know. Right now he sells merchandise at a computer store - does this qualify him to give advice about computer viruses? Most people who claim to speak with authority about computer viruses have little or no genuine expertise. Some virus experts describe it as "False Authority Syndrome" - the person feels competent to discuss viruses because of his job title, or because of his expertise in another computer field, or simply because he knows how to use a computer. I want you to question the credentials of anybody who talks about computer viruses. Indeed, I want you to question my credentials in this field!

The U.S. Air Force highlights the concept of False Authority Syndrome in Tongue & Quill, their official publication on effective writing: Nonexpert opinion or assumed authority - Don't be swayed (or try to sway someone else) based on the opinion of an unqualified authority. The Air Force is chock-full of people who, because of their position or authority in one field, are quoted on subjects in other fields for which they have limited or no experience.

(As this Air Force publication notes, False Authority Syndrome can attack people in all fields of expertise.)

Computer salesmen, consultants, repairmen, and college computer teachers often succumb to False Authority Syndrome. In many cases a person's job title sounds impressive, but his or her job description at most may only include references to vague "computer security" duties.

Network administrators typically fall into this category. Most hold the title of "company virus expert" simply because their job description includes network security. They may have no real education in computer security, but their experience in the field of computer networking gives them confidence when talking about the unrelated field of computer viruses. People who suffer from False Authority Syndrome too often assert conclusions from insufficient data and they habitually label their assumptions as fact. Quoting again from Tongue & Quill: We jump to conclusions from too little evidence; we rely too much on "samples of one" (our own experience); something happens twice the same way and we assume the ability to forecast... Unfortunately, our natural desire is to make positive, solid statements, and this desire encourages the asserted conclusion.

Consider the case of Gary L. Allen. Writing in a letter to Computerworld, he offered his analysis of 1992's worldwide Michelangelo virus scare. Allen listed his virus-fighting credentials: "I am an MIS manager, and we found Michelangelo on disks distributed by one of our software vendors, and it never made it into our local-area network." Allen went on to say: "If we had not been prompted [by the media] to scan [for the Michelangelo virus]... it surely would have made it onto the network hard drives and from there who knows where."

This network administrator checked for a virus because the press told him to do so! Allen made "positive, solid statements" as Tongue & Quill notes. Amazingly, this network administrator claims he checked for a virus because the press told him to do so! Allen also assumes the Michelangelo virus would have "surely" infected his network drives. Virus experts could easily debate this, but why should they have to debate him in the first place? Allen's words expose him as a "virus pseudo-expert."

VIRUS PSEUDO-EXPERTS

I once lectured about viruses to a small group of businessmen in 1991. A network administrator stood up at one point and proclaimed his company (a law firm) would literally close its doors for good "if a destructive virus of any type gets on our system." They would sell the office equipment; the secretaries would find new jobs; the lawyers would take their filing cabinets to other law firms. The company would fold if even one destructive virus infiltrated their network.

Shocked by his statement (and trying to regain control of the lecture), I asked what would happen if fire swept through the firm's building. No sweat: they kept backups off-site and had contingency contracts for just such emergencies. I responded, "Well, there you go. If a virus ever gets on your computers, burn your building to the ground and your problem is solved!"

The audience laughed - but I fumed. I would have fired this man on the spot if he worked for my company! I don't want anyone on my payroll who would instantly put everyone out of work due to his own pompous ignorance. Sadly, ignorant network administrators all too often perpetuate myths about the dangers posed by computer viruses. Ken Hall, a manager at Georgia Tech's Financial Data Technology Office, wrote a typical story for Atlanta Computer Currents magazine in response to the Michelangelo scare of 1992. Hall's seventh paragraph touts a common myth: "Traditionally, viruses have infected computers that have downloaded programs form [sic] dial-up bulletin boards." Experts have tried for years to squelch this myth and others, but pseudo-experts like Hall greatly outnumber them.

Computer Security Experts

Some people hold a rare position in large companies where their entire job title is "computer security." It's not just an additional duty. Their job covers the whole range of security issues, from teenage hacking to espionage, from fires to natural disasters - and of course computer viruses. You'll find False Authority Syndrome here as well.

Experts and BBSs

The "BBSs spread most viruses" claim. Virus pseudo-experts tell you to avoid computer bulletin boards, claiming they account for the spread of most virus infections. And yet genuine virus experts believe just theopposite: they view BBSs as an extremely safe way to obtain software.

Pseudo-experts blame BBSs for spreading most viruses because it seems so plausible to blame them. You can get a virus if you share software, and bulletin boards share a lot of software. Pseudo-experts therefore assume BBSs account for most reported cases of infection - and they wrongly label their assumptions as fact. Computer security personnel at Scott Air Force Base, Illinois attended a job-related course in early 1995. The course included a special handout: Russell & Gangemi's "Computer Security Basics," a book last updated in 1992. Computer books typically have short lifespans: many will disappear from store shelves within a year. But "Computer Security Basics" serves as an industry reference and you could still find it at Waldenbooks stores in late 1995.

Russell & Gangemi mention the shareware program "Flu_Shot" by name on page 88 and tell readers they can obtain it "from both commercial and public domain sources," i.e. from BBSs. Yet on page 87 the book warns readers to "be wary about new public-domain or shareware programs... Don't allow users to install software obtained from [BBSs]." This contradiction sounds minor on the surface; in reality it perpetuates a common virus myth. Specifically, it helps fuel a myth among computer security personnel. Russell & Gangemi also recommend readers to the "Computer Virus Industry Association," an organization widely dismissed before the book's first publication as a publicity front for antivirus mogul John McAfee.

Computer security personnel don't just read books - they watch training videos, too. ViaGrafix, a company specializing in computer training videos, markets a video about computer viruses. Produced in 1992 and still sold in 1995, the ViaGrafix video touts the mythical story of the "Gulf War virus."   Again, this only helps fuel myths among computer security personnel.

Wolfgang Stiller, an internationally recognized virus expert and author of the "Integrity Master" antivirus program, says "computer security experts today - people who deserve that title - tend to have a good background on how viruses operate. They can dispense some good advice." But he chooses his words carefully when asked to comment on virus expertise among computer security personnel. "They're a little more likely than the average person to understand viruses," Stiller notes. "Some would say they're a lot more likely to understand them, but I've met a fair number who don't know a thing about viruses, or, even worse, they've got misconceptions. In light of the fact they are computer security experts, their misconceptions carry a lot more weight than the average person. Errors are much more damaging when they come out of the mouths of these people." In a word... ultracrepidarian: (n., adj.) a person who gives opinions beyond his scope of knowledge.

Stiller sums up False Authority Syndrome among computer security experts: "Put me on a panel with a computer security person, and I won't claim to have his level of security expertise. But the computer security guy will invariably claim to have my level of virus expertise. How can you convince the audience in a diplomatic way that he doesn't?"

(Stiller offers an interesting analogy: he wonders about the policemen who vouch on TV for The Club(R). Do the officers specialize in car-theft investigations - or do they write traffic tickets?)

Computer Repairmen

Network administrators and computer security personnel may have some of the best job titles, but they don't have a lock on the market when it comes to virus pseudo-experts. The list also includes computer consultants & repairmen. In one example, CompuServe user Rob Parker posted a message in early 1995 lamenting his laptop's dead hard disk: Thinking the problem was a virus, the tech[nician] tried a number of virus scanners, all negative. He then tried to reformat the hard disk... He claimed that the [hard disk] was ruined, and that a virus had done it.

Ask yourself this Suppose your computer started acting weird all of a sudden. How would you react? Would you instinctively reach for antivirus software as your first course of action? Computers are extremely complex. All sorts of things can go wrong - software glitches, hardware failures, user error, you name it. The next time your computer does something weird, ask yourself: "How would I react if I'd never heardabout computer viruses?"

In a nutshell, the repairman used two or more programs to detect viruses on the laptop. None of these programs found a virus. The repairman then tried to reformat the laptop hard disk - but the attempt failed. So he claimed a virus had physically destroyed the hard disk. Genuine experts on CompuServe dismissed the repairman's conclusion. Parker now wonders if the repairman made up the story. Did he feel compelled to give his customer an important-sounding excuse for why the drive failed? Parker got off easy: his hard disk failed during the laptop's warranty period. But his experience raises important questions. How many repairmen have incorrectly told customers to fork over money because they claimed "a virus physically destroyed the computer"? How many computer users believed it?

Magazines, Newspaper & Television

Paul Mayer, an expert on marketing for small software companies, wrote a regular column for a computer magazine. His editors once paid him to write an article on viruses. Mayer's virus credentials appeared in the fourth paragraph: I have personally had two contacts with viruses in 15 years of working with computers. The first encounter caught me completely off-guard. I was prepared for the second.

Mayer wrote the story from the perspective of a regular user. He believes the magazine picked him to write it because he had first-hand user experience with viruses. And to his credit, Mayer consulted with a genuine virus expert while writing the article. Unfortunately, reporters in the mainstream media will quote almost anyone when it comes to viruses - and they habitually quote local people. A typical story illustrates this point. Published in the St. Louis Post-Dispatch during 1992's worldwide Michelangelo virus scare, it quoted various local businessmen, among them: Craig Johnson, manager of a local Software Plus store; Ernest White, manager of a local Babbage's store; Todd Jones, salesman at a local Software Centre store.

The Media and Michelangelo

This problem afflicts TV reporters as well. An NBC Nightly News story, broadcast during 1992's Michelangelo scare, included an interview with a computer salesman. He mentioned his customers' panic and the reporter asked if "the panic is justified." The salesman responded: "yes." And there you have it: panic is justified if you think your computer might have a virus. So says a nationally recognized computer salesman. Even "computer-literate" mainstream reporters commit serious blunders when they write stories about viruses. Numerous reporters logged onto CompuServe, GEnie, Prodigy, and America Online during the Michelangelo scare and posted messages to "all." Each message asked the same question: "Want to be interviewed for a story on the Michelangelo virus?"

These reporters didn't search for experts - they went on a "cattle call" for frightened computer users. One USA Today reporter, expecting an avalanche of calls, asked people not to tie up his phone unless he or she actually got hurt by the Michelangelo virus on its upcoming March 6 trigger date. Consider the tragic accident where actor Christopher Reeve broke his neck. The mainstream media quickly turned to spinal-injury specialists for comment. Why didn't they ask a podiatrist if Reeve will ever walk again?

Never underestimate the mainstream media's role in the spread of False Authority Syndrome. Empirical Research Systems (a computer industry polling firm) conducted a survey in 1991 of corporate employees tasked in some way with computer security. 43% of respondents - almost half - formed their opinions about viruses just by reading newspapers! Newspaper reporters talk to these people to get details (and quotes) for a story. This means the press feeds information to virus pseudo-experts, who gladly regurgitate it for other reporters, who write more stories about viruses, which other pseudo-experts read... thus creating an endless circle of misinformation and a never-ending supply of "instant experts." This same survey concluded with a sad statistic: it estimates two-thirds of employees tasked with computer security duties have inadequate knowledge about computer viruses.

IMPLICATIONS

Computer neophytes easily succumb to False Authority Syndrome. They feel more important by spreading the word about dangerous viruses. If someoneelse points out their errors, these people will often justify their actions in terms of fear. As Marcello noted in his apology, he feared both for his computer and for his job.

Widespread myths & misinformation have also convinced people to fear safe methods of computing and to put their trust in less-safe methods. In her book Rx PC: The Anti-Virus Handbook, Janet Endrijonas claims "approximately 70 percent of all viruses are boot sector viruses." Wolfgang Stiller and other experts put the total above 90%.

Boot sector viruses, by their nature, don't travel in software downloaded from BBSs - yet pseudo-experts constantly point to downloaded software as the biggest avenue for the spread of viruses. In his book Inside the Norton Antivirus, Peter Norton dismisses the myth about the dangers of downloaded software. "Bulletin boards do more to spread the awareness of viruses... The primary method of communication concerning viruses is through BBSes [sic]." Robert Slade, writing in his book Guide to Computer Viruses, goes even further:

If I had to choose one viral myth that contributed most to the unchecked spread of [viruses] that exists today, it would be that of the 'safety' of commercial software... The feeling of false security relies on three assumptions: (1) that [software downloaded from BBSs] is a major viral vector, (2) that commercial software is never infected... (3) that there are no viral vectors other than software.

SUMMARY & CONCLUSION

I don't want to dispel any particular computer virus myths someone may have told you - that's not my goal here. Rather, I want you to question a person's expertise if he or she claims to speak with authority on computer viruses. This way we can prevent all the "blind leading the blind" techno babble. And we can reduce the number of people who believe all the myths out there.

Most people have little or no expertise in the field of computer viruses. People with little or no expertise often fall prey to False Authority Syndrome. False Authority Syndrome contributes significantly to the spread of fear and myths about computer viruses. PC Techniques editor Jeff Duntemann sums it up best: "If people exercised greater discretion in who and how and to what degree they place their trust, we would know more as a community - and we would know it better. There would be fewer paths for bad or phony knowledge."

BIBLIOGRAPHY

Allen, Gary L. "Warning helped" (letter to the editor), Computerworld (22 Feb 93):32

Barnette, Martha. "High-Tech Hygiene," CompuServe Magazine (Nov 92):20 25

Cheswick, William R. and Bellovin, Steven M. "Repelling the Wily Hacker,"

Computerworld (16 May 94):113-20

Christy, Jim (Special Agent). "Drive safely on the Information Superhighway," Intercom [U.S. Air Force Communications Command] (Aug 94):15

Coates, James. "'Good Times' virus just a bad on-line myth," Chicago Tribune (21 May 95):1 Computer Security Institute. Manager's Guide to Computer Viruses. San Francisco:Computer Security Institute, c.1992

Connell, Christopher. "White House Virus," Associated Press (29 Oct 93):newswire

Daly, James. "Virus threat could be overstated," Computerworld (14 Sep 92):16

Daly, James. "Virus shots," Computerworld (14 Sep 92):82

Daly, James. "Virus paranoia," Computerworld (16 Nov 92):37

Dvorak, John C. and Somerson, Paul. "The Virus Scare: Media Hype, Minor Nuisance, or Serious Threat?", PC/Computing (May 92):106

Endrijonas, Janet. Rx PC: The Anti-Virus Handbook. Pennsylvania: Windcrest/McG raw Hill, 1993

Endrijonas, Janet. Data Security. California: Prima Publishing, 1995

Ferelli, Mark. "Shareware Gets Bum Rap As Virus Source," Computer Technology Review (Jul 92):10

Fike, Sarah. "V-day? Few hits reported," Belleville [Illinois] News-Democrat (7 Mar 92):1A

Garreau, Joel. "Treasury Exposed Computer Virus Info; Whistleblowers Halted Display Available to Anyone With a Modem," Washington Post (19 Jun 93):newswire Hall, Ken. "Michelangelo and Other Viruses," Atlanta Computer Currents (Apr 92):30

Howard, Bill. "Abort, Retry, Fail?", PC Magazine (15 Sep 92):576

Icove, David and Seger, Karl and VonStorch, William. Computer Crime: A Crimefighter's Handbook. California: O'Reilly & Associates, 1995

Jacobson, Robert V. The PC Virus Control Handbook (2nd Edition). San Francisco: Miller Freeman Publications, 1990

Kane, Pamela. PC Security and Virus Protection Handbook. New York: M&T Books, 1994

Kane, Pamela. V.I.R.U.S. Protection: Vital Information Resources Under Siege. New York: Bantam Books, 1989

Kane, Pamela and Rosenberger, Rob. "Michelangelo: Anatomy of a Virus Scare," ISPNews (May-Jun 92):1-...

Levin, Richard B. The Computer Virus Handbook. Berkeley: Osborne/McGraw Hill, 1990

Markoff, John. "Virus Threat is Overstated, an IBM Study Concludes," New York Times (9 Sep 92):unk

Mayer, Paul. "Better Safe Than Sorry," Shareware Magazine (Sep-Oct 93): 26 7

Mungo, Paul and Clough, Bryan. Approaching Zero. New York: Random House, 1992

National Computer Security Association. Computer Virus Market Survey. New York: DataQuest, 1992

NBC Nightly News. Broadcast story about the Michelangelo computer virus (5 Mar 92)

Norton, Peter and Nielson, Paul. Inside the Norton Antivirus. New York: Brady Publishing, 1992

Oxford English Dictionary. Oxford: Clarendon Press, 1989

Peterson, A. Padgett. "Tactical Computers Vulnerable To Malicious Software Attacks," SIGNAL Magazine [Armed Forces Communications & Electronics Assn.] (Nov 93):74-5

Raskin, Robin and Kabay, M.E. "Antivirus Software: Keeping Up Your Guard," PC Magazine (16 Mar 93):209-69

Rosenberger, Rob. "It's shareware, not virusware: Misconceptions about safety prevent many people from using shareware," Computerworld (18 Feb 91):25

Rosenberger, Rob. Computer Survial Series: "The Virus Myth." VHS video, 75 min. Seattle: TUG Productions, 1991

Rosenberger, Rob. "All About Viruses," Shareware Magazine (Jan-Feb 92): 48 9

Rosenberger, Rob. "Virus Myths and Twists" (letter to the editor), Windows User (May 93):14

Rosenberger, Rob. "Modems, bulletin boards and other tools of Satan," Computerworld (3 May 93):57

Rosenberger, Rob and Greenberg, Ross. Computer Virus Myths (10th edition). New York: Rosenberger & Greenberg, 1988-94

Rosenberger, Rob. Michelangelo Fiasco: A Historical Timeline. Illinois: Rosenberger, 1992

Russell, Deborah and Gengemi, G.T. Sr. Computer Security Basics. California: O'Reilly & Associates, 1992

Salamone, Sal. "Security Trends in Colleges," NCSA News [National Computer Security Assn.] (Jul-Aug 92):9

Sanford, Robert. "Vaccine Frenzy: Computer Owners Guard Against Virus," St. Louis Post-Dispatch (4 Mar 92):1A

Sanford, Robert. "An 'Allergy': Michelangelo Virus Pops Up, But Does Little Damage," St. Louis

Post-Dispatch (7 Mar 92):11A-12A

Slade, Robert. Guide to Computer Viruses. New York: Springer-Verlag, 1994

Smith, George. "The Little Virus That Didn't," Washington Journalism Review (May 92):unk

Smith, Jan. "Viruses: Gone or Just Forgotten?", CompuServe Magazine (Oct 94):28-31

Stiller, Wolfgang. Defeating Viruses and Other Threats to Data Integrity (4th Edition). Florida: Stiller Research, 1994

Trend Micro Devices. "Computer Virus Prevention: Facts and Fiction." California: Trend Micro, c. 1993

Ulanoff, Lance. "Virus Spread: Who's to Blame?", PC Magazine (13 Oct 92):31 2 U.S. Air Force. Tongue and Quill, publication AFP 13-2. Washington, DC: HQ USAF, 1985

Waller, Douglas and Thompson, Mark. "Onward Cyber Soldiers," Time (21 Aug 95):38-46

Webster, Bob and Gwartney, Kurt and Heuckendorf, Michelle. PC Virus: Understanding and Prevention. VHS video, 50 min. Oklahoma: ViaGrafix, 1992

Wiggen, Regina. "Michelangelo, Computer Security, and the Research Community," Agricultural Research (May 92):2