A Computer Virus


A computer virus is merely a bit of computer programming code that has been designed to replicate itself and perhaps accomplish some other simple task such as displaying a message on the screen on a particular date. A simple idea—and frightening!

The idea of a computer virus has been around for quite a while, and at first it seemed mainly to be a topic of intellectual curiosity. How might one create a few lines of programming to be inserted into software designed for other purposes, that would be difficult to detect, that could replicate and spread itself to other software, and that might sometime in the future make its presence known to a computer user? Initially this seemed quite difficult.

But it isn't nearly as difficult as first supposed. A bright student of computer science and many computer hackers can figure out how to do it. The result can be amusing, or disastrous.

The early history of computer crime indicates that such crime accompanied the introduction of computers into business and industry. The crime might consist of illegally transferring money between accounts, or placing an order to be billed to a wrong account. Initially some of those involved in computer crimes managed to avoid legal prosecution by revealing what they had done and how they did it, and how the companies could avoid being victimized in the future. That was back in the days when computers were still mainly mainframes and were not yet in widespread use. Computer crime was an interesting and provocative topic to discuss in a computer literacy course, but somehow it seemed far removed from my daily life.

But times have changed. Mainframe computer systems still exist, but microcomputers now dominate the field. Many millions of people now own their own computer and/or make routine use of computers at work. I make daily use of computers, and my professional work depends on it. One of the computers I use is readily available to other people, and some of the software I use is used by my co-workers. Computer viruses have come to my campus, and our Computer Center has issued a specific warning about viruses on the type of computer that I use. All of a sudden I face the real possibility of being the victim of a computer crime!

But my personal work is only a small part of the problem. I live in a society that is becoming more and more dependent on computers. I frequently fly in airplanes that make use of sophisticated computerized instrumentation and autopilots; they depend on the computers of the air traffic control system. My bank account is computerized, and I make extensive use of credit card systems that are highly computerized. I make frequent use of telephones, and our telephone system is highly computerized. I could easily extend the list, but the point is clear. Computer crimes can easily and directly affect me and you.

I am struck by the parallel with AIDS, a real virus that has wrought misery and suffering among many people. There are now thousands of researchers worldwide attacking the AIDS problem, and perhaps someday a vaccine will be developed to help prevent its further spread. Meanwhile, widespread education about AIDS can help protect me and others from this disease.

But what about computer viruses and similar crimes conducted through and against technology? I can imagine that there are a growing number of people who know how to create a computer virus and introduce it into software. I can imagine that one does not need to be a
computer science genius to modify such computer code. Indeed, I can imagine that some secondary school students will eventually learn to do this.

It is serious enough when secondary school students break into the school computer network, look at confidential records, and perhaps change a few grades. It is still more serious when students with a similar bent have the potential to mess up the computer systems of the world.

In some sense the problem can be characterized by the observation that the world is growing smaller, and that the people of the world are growing more and more interdependent. A few hundred years ago our transportation systems were poor and many people lived out their entire lives within a few miles of their birth places. A virus mutation might affect just a small number of people, and then die out.

But now we live in the Information Age, and one characteristic of the Information Age is a steady improvement in transportation systems and the number of people who travel extensively. AIDS is a worldwide problem. It is being attacked on a worldwide basis by a combination of health education and medical research.

Similar statements hold for our communication systems and computer viruses. We face the possibility that there will be a rapid increase in the number of computer viruses, and that they will have a severe impact on our lives.

There are no simple answers to the computer virus problem. Each computer user can learn to take preventative actions, such as never making use of pirated software. (But there have been reports of computer viruses in factory sealed copies of commercially produced software.) And, of course, the technology that produces computer viruses can also produce computer programs designed to detect and eradicate computer viruses. AIDS and computer viruses are products of our Information Age society. They suggest that our education system needs to take a much more "global village" approach. Students need substantial knowledge to help protect themselves, and they need to develop values appropriate to viewing the world as a global village.