图解电脑系列丛书

电脑病毒预防与清除

钱康 主编

科学普及出版社

图解电脑系列丛书

电脑病毒预防与清除

钱 康 主编

科学普及出版社

·北 京·

图书在版编目(CIP)数据

电脑病毒预防与清除/钱康主编. —北京:科学普及出版社,1997.5
(图解电脑系列丛书)
ISBN 7-110-04222-7

Ⅰ.电… Ⅱ.钱… Ⅲ.微型计算机-计算机病毒-防治-图解
Ⅳ.TP309-64

中国版本图书馆 CIP 数据核字(97)第 03750 号

科学普及出版社出版
北京海淀区白石桥路 32 号 邮政编码:100081
新华书店北京发行所发行 各地新华书店经售
中国科学院印刷厂印刷

*

开本:787×1092 毫米 1/16 印张:2.25 字数:30 千字
1997 年 5 月第 1 版 1997 年 5 月第 1 次印刷
印数:1—10000 册 定价:3.80 元

多思宣言

亲爱的小朋友们：

你们好！我是多思。

今天，电脑已经是我们不可分离的小伙伴啦。瞧，工厂、商店、银行、教室……电脑无处不在。爸爸说，没有电脑就没有现代化，不会用电脑，就不能成为合格的现代化的接班人。

从现在开始，让你我一同走进神奇的电脑世界。

主　　编　钱　康
执行主编　黄　伟
编　　委　钱　康　黄　伟　徐月宁　杨　静
　　张卫楠　谢　伟　王东兵　王生军
　　张晓彬　李海英　李俊生　胡雅丽
　　魏　龙　张福东
绘　　图　扬　扬　史　彤

责任编辑　赵兰慧
封面设计　扬扬　史彤
正文设计　纪军
责任校对　林华
责任印制　安利平

目　录

第一节　电脑病毒的特性

多思：爸爸，今天明明家的电脑在开机后，屏幕上出现了跳动的小球，并且每隔十几分钟就出现一次。

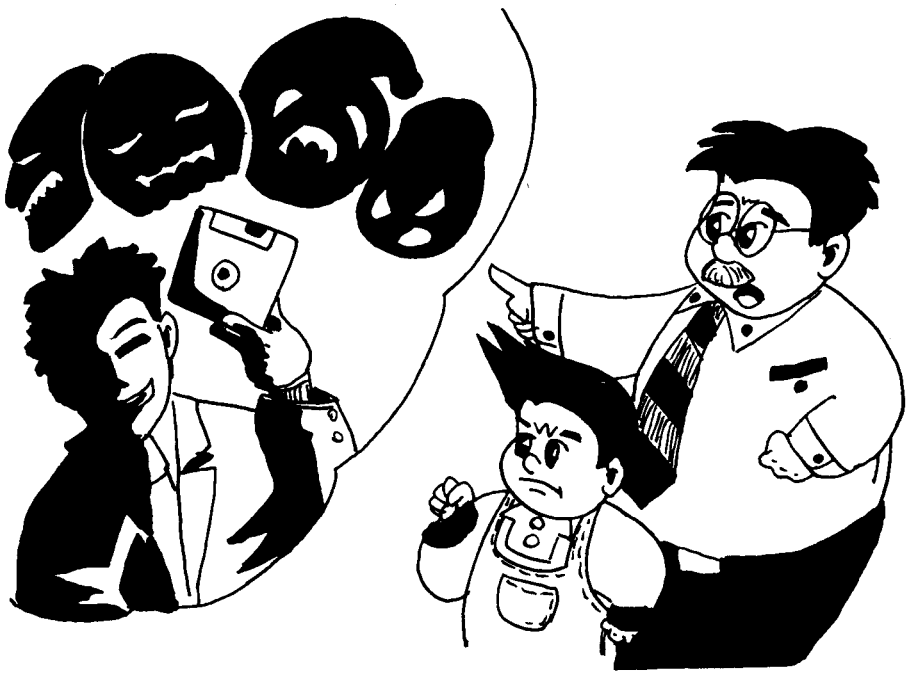
爸爸：这一定是电脑病毒在作怪。

多思：那什么是电脑病毒呢？

爸爸：电脑病毒是隐藏在电脑系统内的一种破坏性程序。它能够利用系统资源进行繁殖和生存，并通过系统数据进行传染。它和生物学病毒有相似的特性，例如，传染性、流行性、繁殖性、表现性等等。但它们的本质存在着明显的区别，前者是一种程序，而后者是一种微生物。电脑科学借用了生物学的术语，用“电脑病毒”表示具有上述特性的程序。

多思：原来电脑病毒是一种具有破坏性的程序啊。

爸爸：对。据资料介绍，计算机病毒源于搞恶作剧的人，有些人想显示自己在编程序方面的才华，他们所编写的病毒程序是无恶意的，只是想和对方开一个玩笑。另一个原因是恶意性的报复，



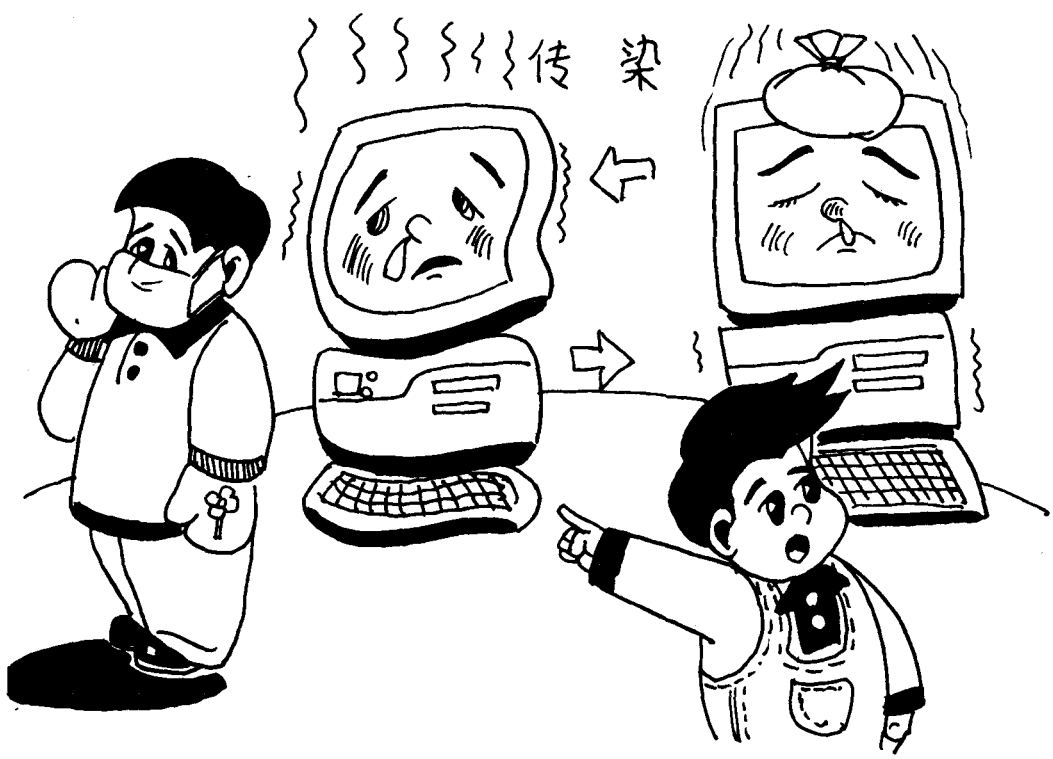
例如一些在计算机公司工作的人，或在某公司的计算机部门工作的人，他们一旦被解雇，心里不平衡，就想报复公司一下，例如某银行职员在计算机管理系统中插入了一小段程序，检查他的名字是不是在银行系统中的档案里，当他被解雇后，档案中再没有他的名字了，之后该程序对银行数据进行了破坏，从而达到了他个人报复的目的。

多思：明明的爸爸说，电脑病毒和人体感冒病毒一样，会传染的，真的吗？

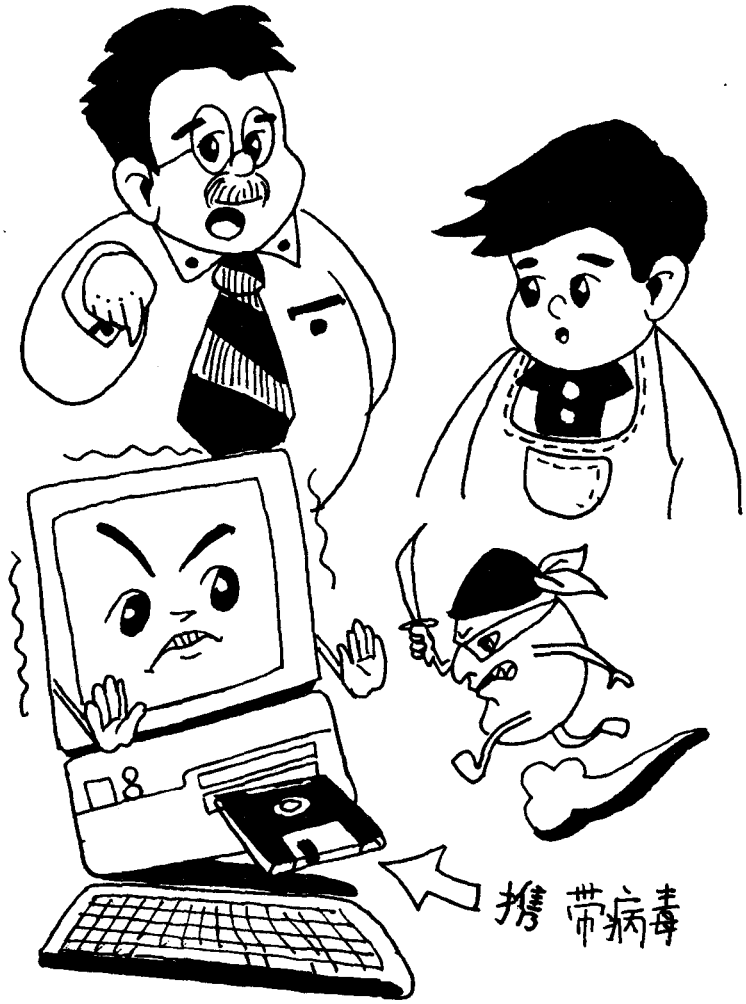
爸爸：对，传染性是电脑病毒的重要特点之一。当“健康”磁盘或者“健康”程序被染上病毒后，它将同母体程序一样成为新的传染源，传染性使得电脑病毒到处扩散，严重影响甚至彻底毁坏了电脑系统的正常运行。

多思：那么电脑病毒是怎样传染的呢？

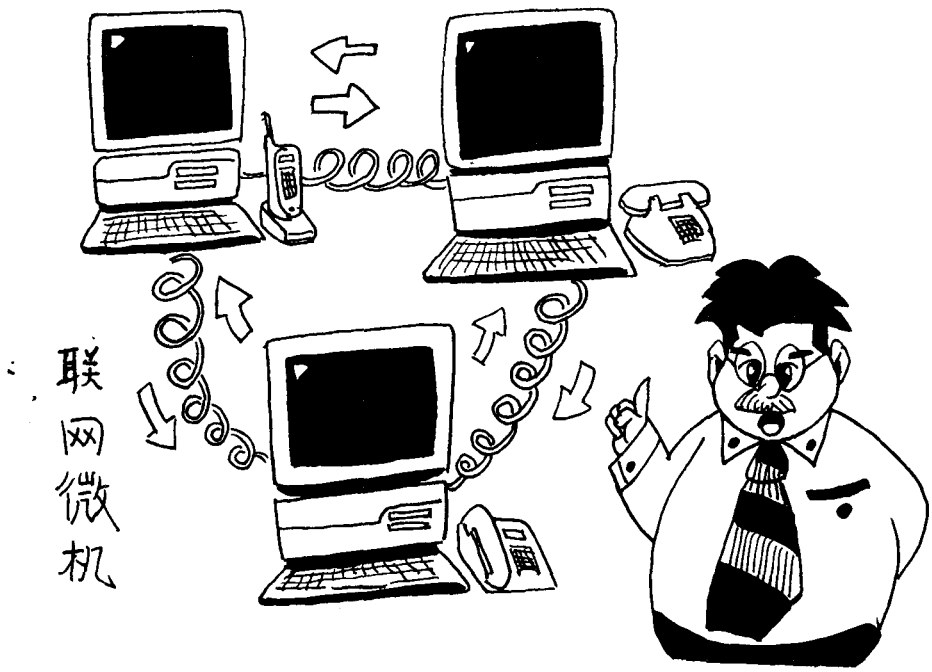
爸爸：电脑病毒只能传染给同类电脑，其主要传染途径是拷



贝。无论是整盘拷贝还是文件拷贝，只要源盘或源文件带有病毒，那么得到的复制盘或复制文件将同样带有病毒。



对于传染文件的外壳形病毒来说，在系统已染上病毒之后，如果运行未加写保护的软盘或硬盘上的可执行文件，或者使用 DOS 命令对文件进行操作，那么这些文件都被染上病毒。对于传染磁盘引导区的操作系统病毒，若系统已驻留病毒，则每当进行磁盘操作时，病毒就传染给执行文件。而当使用染毒磁盘引导系统时，在引导病毒驻留内存的同时病毒也传染给执行文件。



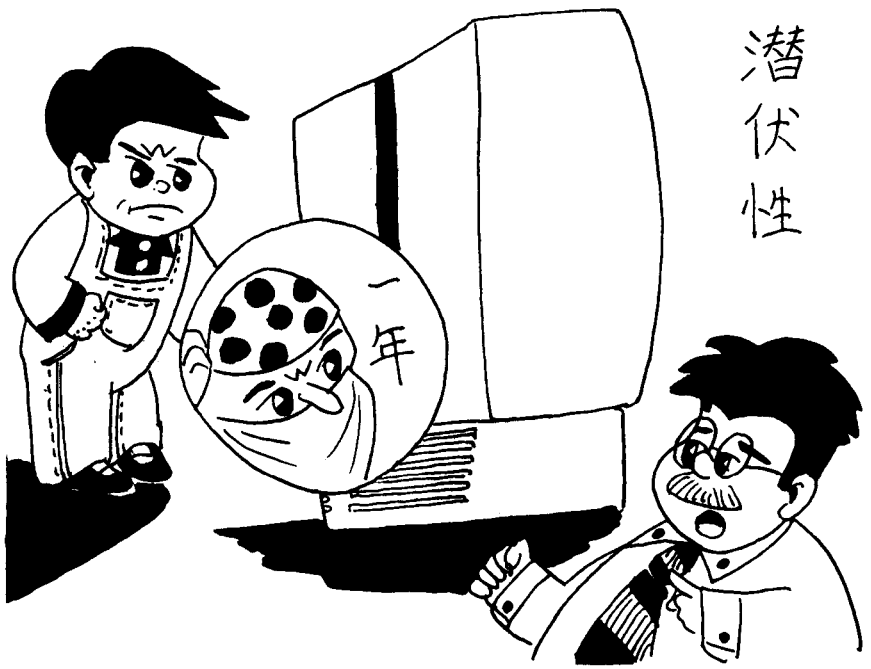
在计算机网络中，如果在已被病毒传染的网络中运行文件，则文件被传染，计算机网络是病毒传染的主要途径之一。软盘一旦染上病毒，它就成为病毒的载体，病毒隐藏在软盘中，随着软盘的使用，病毒就又传染给使用该盘的系统。而软盘的交流和交换，又促使了病毒的传播和扩散。这就是为什么病毒迅速蔓延和广泛传播的原因。

爸爸：电脑病毒除了具有传染性外，还有潜伏性、隐蔽性、破坏性呢！

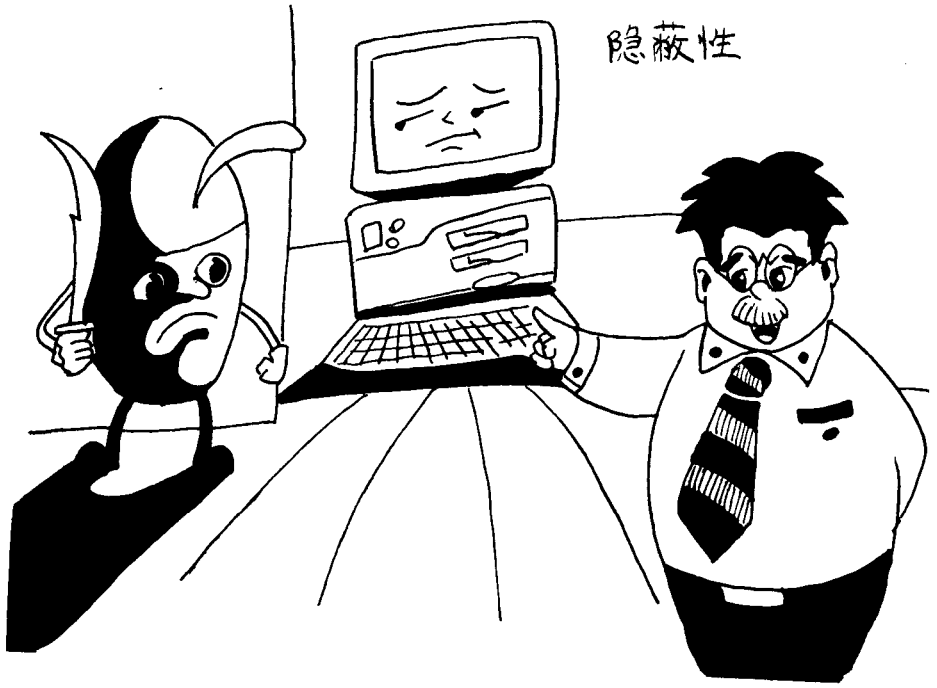
多思：爸爸，你能给我具体地讲一讲吗？

爸爸：可以呀！首先说说潜伏性。

潜伏性是指病毒发作之前，把自己隐藏在合法文件之中，偷偷地传播，以扩大其传染和破坏的范围。更有甚者，当年投放传染的病毒本年度只传染不发作。首次潜伏期长达1年甚至更长。潜伏期过后，病毒发作时想控制病毒传染为时已晚。其传染面已扩大到无法控制的局面。

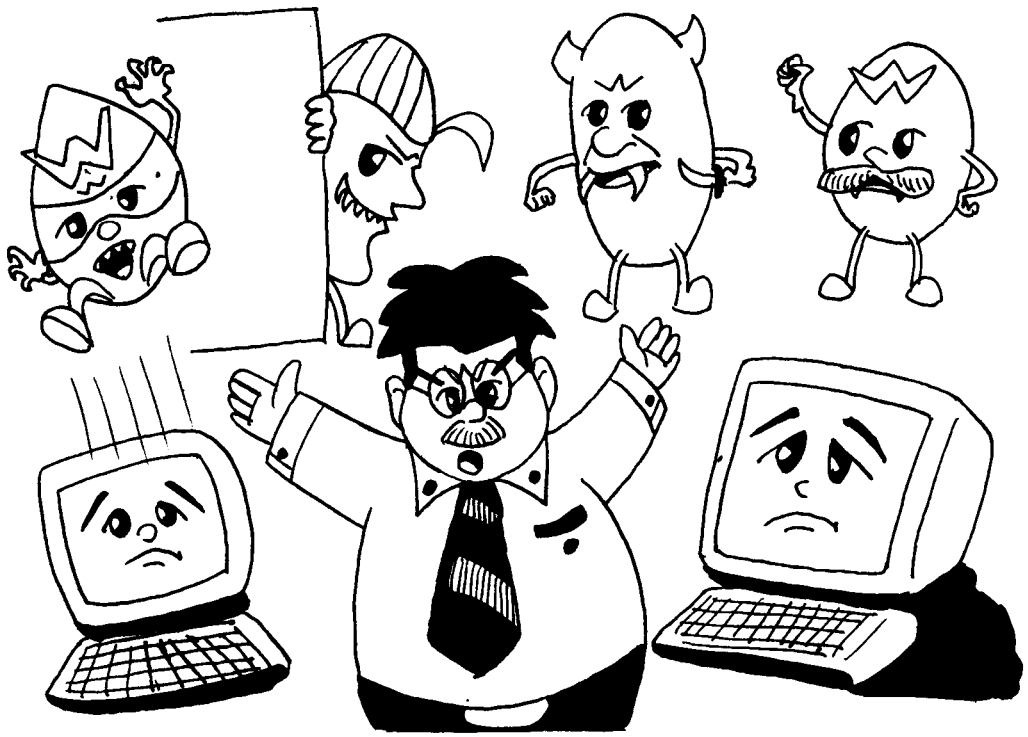


再讲一讲电脑病毒的隐蔽性。病毒的隐蔽性有两层含意：一是其存在的隐蔽性，它把自身依存于某种载体，不发作则不易发现；二是其攻击的隐蔽性，病毒运行系统是隐蔽的，它的传染过程、破坏数据过程一般也是隐蔽的，不易为用户察觉。



最后说一说电脑病毒的破坏性。病毒侵入系统的目的在于破坏系统，根据破坏系统的不同，可以把病毒分为良性病毒和恶性病毒。

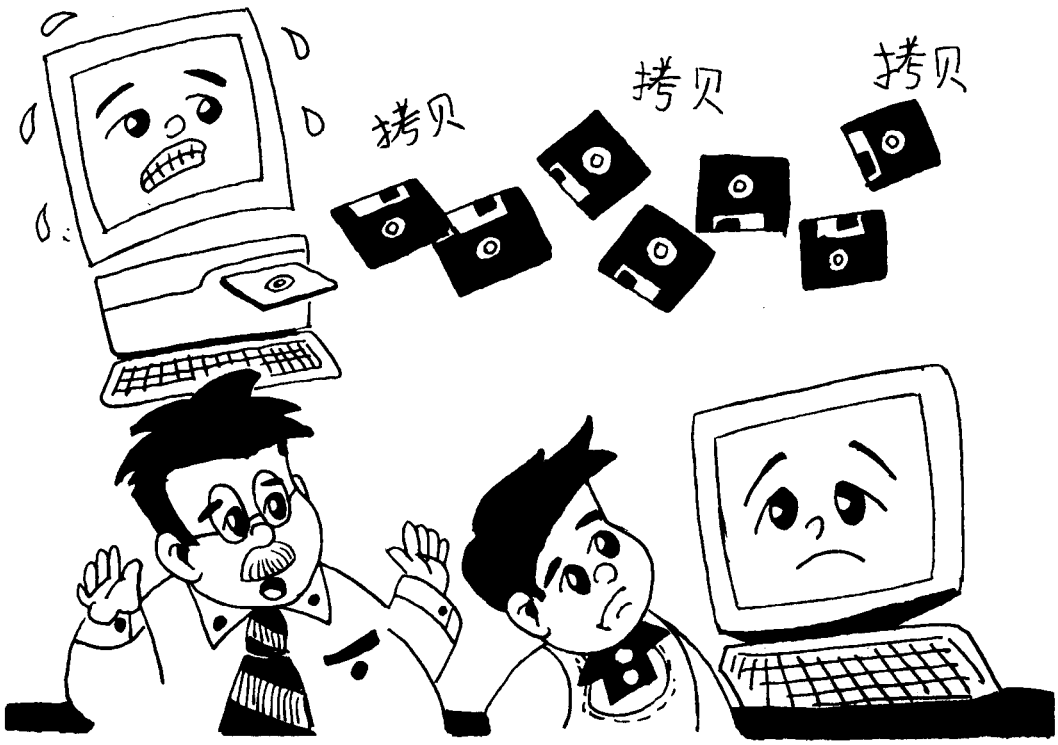
多思：病毒发作就是有小球在屏幕上滚动吗？



爸爸：不是的，不同的“病毒”在发作时，呈现不同症状，这是因为有的病毒发作时，可直接在屏幕上表现出来，如小球病毒发作时，会有许多小球在屏幕上滚动，而有些病毒则无表面现象，隐藏一段时间再发作，给系统造成不可预知的破坏，给人一种不知所措的感觉。另一方面，它的传染方式也是不一样的，例如，在普通的家用电脑单机用户中主要的传播媒介是软磁盘，由于不断频繁的拷贝，为病毒的传播提供了途径，而在网络系统中，病毒通过网络通信系统广为扩散。

破坏性是病毒的最重要特性，而其他特性是为了破坏而服务的，但没有隐蔽性、潜伏性和传染性，病毒就达不到破坏这一目的。

总之，电脑病毒实质上是一段人为设计的电脑程序，这个程序能够修改其他程序而把自身拷贝到其他程序之内，从而完成对其他程序的传染或破坏，直至对更多台电脑的感染和破坏。



多思：被染上病毒的电脑会遭到哪些破坏呢？

爸爸：通常有以下几种情况：

(1)破坏文件分配表，使用户磁盘上的信息丢失。

(2)改变磁盘分配，造成数据写入错误。

(3)删除磁盘上特定的可执行文件或数据文件。

(4)修改或破坏文件中的有关数据。

(5)影响内存中常驻程序的正常执行。

(6)更改或重新写入磁盘的卷标。

多思：真是够厉害的。那我们怎么能知道电脑是否被染上病毒呢？

爸爸：通过下面这些常见的现象，能够发觉电脑是否染上了

病毒。

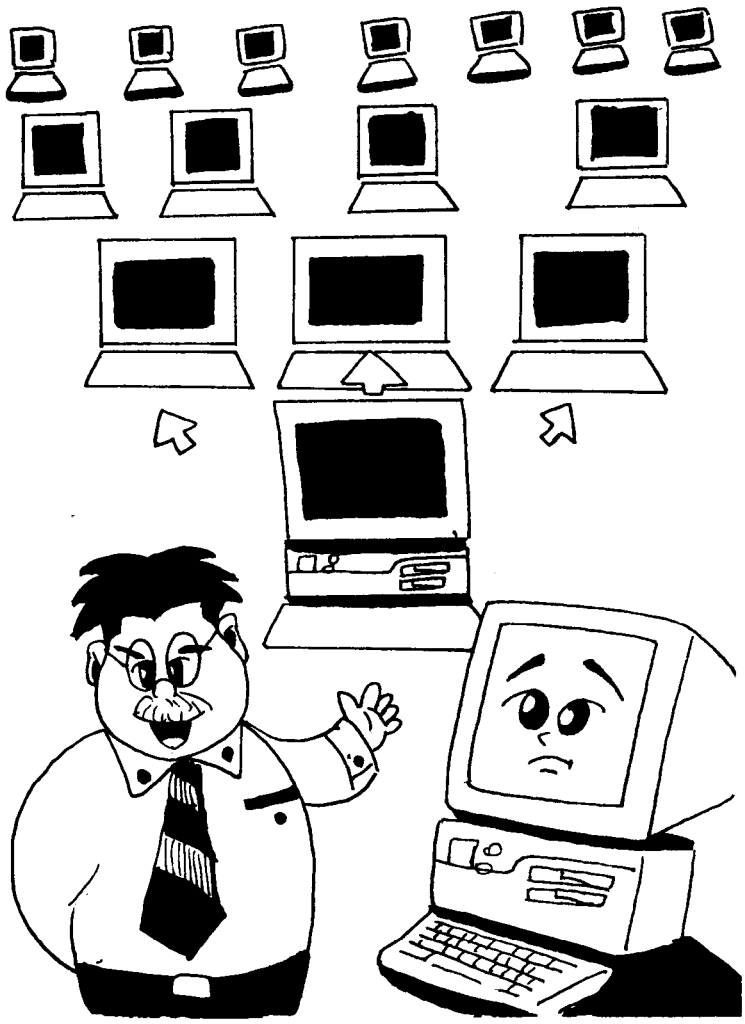
(1)在屏幕上出现不正常的显示画面。

(2)硬盘中的数据突然丢失或在目录中增加了几个文件。

(3)计算机的运行速度变慢了。

(4)文件的日期被修改了。

此外,现在有多种检查病毒或杀病毒的软件,利用这些软件你也能检查电脑是否被染毒,它甚至能检查出处于潜伏期的、隐蔽性极强的病毒。



第二节　病毒的传染方式

多思：爸爸，通过前面的学习，我知道病毒的传染是以计算机系统的运行和读写磁盘为基础的。

爸爸：是的，没有这两个条件，病毒是不会传染的。这是因为：

(1)不运行时，不存在对磁盘的读写和数据的共享。

(2)没有磁盘的读写操作，病毒就不能传入磁性存储介质中，而只能驻留在内存中或根本无法驻留内存。

(3)病毒要传染必须驻留在内存中。

(4)病毒驻留内存后，必须有适当的条件才能实施传染。

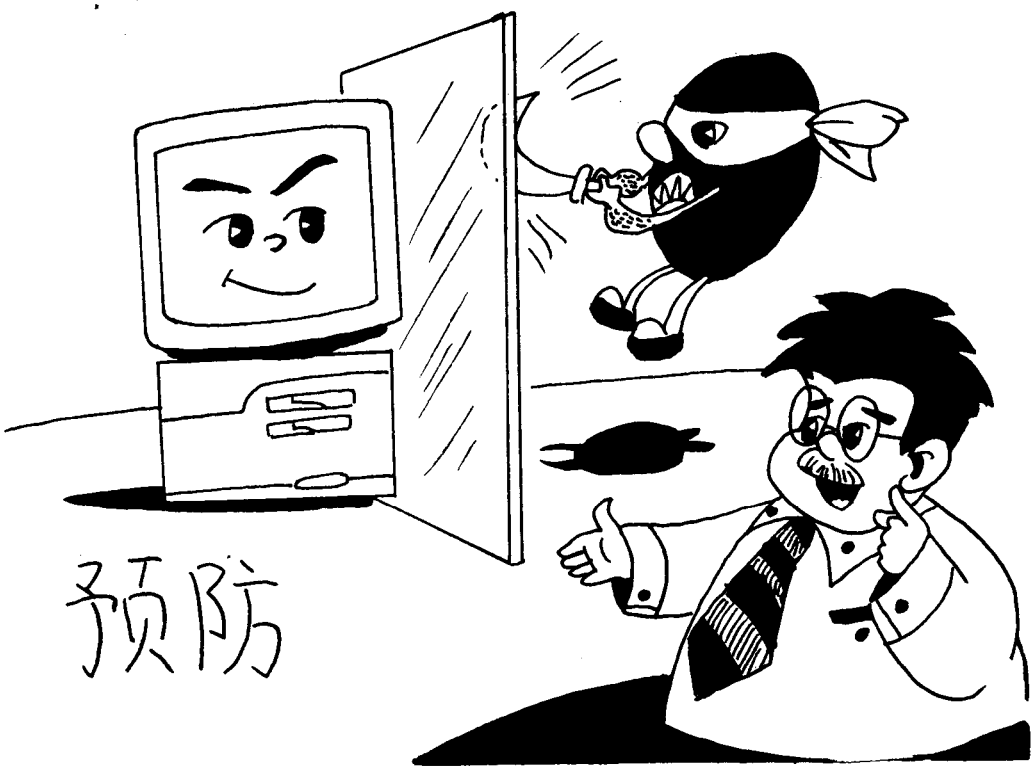
计算机病毒按传染对象的不同分为两大类，这就是引导区传染的病毒和可执行程序传染的病毒。

了解这些知识对我们防治电脑病毒是非常有意义的。

第三节　电脑病毒的预防

多思：电脑病毒这么厉害，难道我们就没有办法防治它了吗？

爸爸：当然有啦，和人类预防生物病毒一样，我们首先要预防电脑病毒。



多思：怎么样才能预防电脑病毒呢？

爸爸：阻止计算机病毒的侵入，做好预防工作是最重要的。预防计算机病毒应从两方面入手，第一要清除计算机病毒的滋生地；第二要切断计算机病毒的传播途径。下面是预防电脑病毒的一般方法：

(1)谨慎使用公共和共享的软件，因为使用这种软件的人很多而且比较杂，容易带有病毒。