# 电脑病毒知识拓展了解和防范[推荐五篇]

来源：网络 作者：暖阳如梦 更新时间：2024-06-08

*第一篇：电脑病毒知识拓展了解和防范电脑已经成为我们生活的一部分，电脑给我们的生活带来了丰富多彩的事情，那么计算机中了病毒有什么症状呢?通常情况下，当计算中病毒后，在电脑操作者看来并无明显的特征，但是我们仍然可以通过一些细节问题来判断电脑是...*

**第一篇：电脑病毒知识拓展了解和防范**

电脑已经成为我们生活的一部分，电脑给我们的生活带来了丰富多彩的事情，那么计算机中了病毒有什么症状呢?通常情况下，当计算中病毒后，在电脑操作者看来并无明显的特征，但是我们仍然可以通过一些细节问题来判断电脑是否已中病毒。下面就让小编带你去看看电脑病毒知识拓展预防和处理，希望能帮助到大家!

电脑感染病毒的10种症状及简单处理办法 电脑中病毒的症状介绍

电脑中病毒的症状(一)文件或文件夹无故消失：

当发现电脑中的部分文件或文件夹无缘无故消失，就可以确定电脑已经中了病毒。部分电脑病毒通过将文件或文件夹隐藏，然后伪造已隐藏的文件或文件夹并生成可执行文件，当用户点击这类带有病毒程序的伪装文件时，将直接造成病毒的运行，从而造成用户信息的泄露。

电脑中病毒的症状(二)运行应用程序无反应：

部分电脑病毒采用映像劫持技术，将常用的应用程序运行路径进行更改为病毒运行目录，从而当我们试图运行正常的程序时，其实是运行了病毒程序，导致电脑病毒的启动。

电脑中病毒的症状(三)电脑启动项含有可疑的启动项：

检查“系统配置实现程序”窗口，如果发现有不明的可执行目录，则可以确定自己的电脑已经中病毒啦。当然更多时候病毒程序是利用修改注册表项来添加自启动项。

电脑中病毒的症状(四)电脑运行极度缓慢：

当电脑运行速度明显变得缓慢时，就及有可能是电脑中病毒所致。中病毒的电脑，通过病毒程序会在后台持续运行，并且绝大多数病毒会占有过多的CPU及内存，而且木马病毒大都会借助网络来传播用户隐私信息。

电脑中病毒的症状(五)杀毒软件失效：

通过杀毒软件用于对系统进行防护，因此当杀毒软件无法正常运行进行杀毒操作时，就可以确信电脑已中病毒，此时我们需要借助网络来实行在线杀毒操作。大部分安全防护软件如360，金山卫士，QQ管家这三款比较主流的国产安全防护软件都有自主防御的防御模块，而病毒或木马最先攻击的就是安全防护软件的自主防御模块。如果您发现主动防御模块被关闭或安全防护软件直接无法启动或内存错误，很有可能是安全防护软件也招架不住这种强悍的病毒而瘫痪了

电脑中病毒的症状(六)电脑运行异常：

病毒会占用过多的系统性能，以及造成文件的破坏，甚至严重影响系统的稳定性。当电脑出现无故蓝屏、运行程序异常、运行速度太慢以及出现大量可疑后台运行程序时，就要引起注意，可能电脑已经中病毒啦。

电脑中病毒的症状(七)系统语言更改为其他语言

大家的计算机系统语言默认是简体中文，如果开机后发现急速阿吉系统语言被修改为其他语言，很有可能是中了恶意病毒了，可以试用安全防护软件扫描清除病毒

电脑中病毒的症状(八)蓝屏黑屏

黑屏比较少见，蓝屏却比较多见了。中了莫名的恶意病毒可能在运行某个游戏或某个软件时突然计算机蓝屏，蓝屏代码可能是某条常见代码，可能是说计算机为了保护系统自动强行重启。

电脑中病毒的症状(九)主页篡改，强行刷新或跳转网页，频繁弹广告

主页被篡改是早期病毒的主要攻击对象，计算机操作系统中毒后一般都会发生浏览器主页被篡改的现象，所以当年IE伴侣这款修复主页篡改的小软件挺受欢迎。如果同时伴有浏览器页面不停反复载入/刷新或无缘无故弹出广告，那么很有可能是中毒了

电脑中病毒的症状(十)应用程序图标被篡改或空白

计算机桌面的程序快捷方式图标或程序目录的主e\_\_e文件的图标被篡改或为空白，那么很有可能这个软件的e\_\_e程序被病毒或木马感染。小编印象中蠕虫病毒会进行此类感染修改

电脑中病毒后简单的处理方式

一、正在上网的用户，发现异常应首先马上断开连接

如果你发现IE经常询问你是否运行某些ACTIVE\_\_控件，或是生成莫明其妙的文件、询问调试脚本什么的，一定要警惕了，你可能已经中招了。典型的上网被入侵有两种情况：

1、是浏览某些带恶意代码的网页时候被修改了浏览器的默认主页或是标题，这算是轻的;还有就是遇到可以格式化硬盘或是令你的windows不断打开窗口，直到耗尽资源死机??这种情况恶劣得多，你未保存和已经放在硬盘上的数据都可能会受到部分或全部的损失。

2、是黑客的潜在的木马发作，或是蠕虫类病毒发作，让你的机器不断地向外界发送你的隐私、或是利用你的名义和邮件地址发送垃圾，进一步传播病毒;还有就是黑客的手工入侵，窥探你的隐私或是删除破坏你的文件。

处理办法：马上断开连接，这样能将自己的损失降低的同时，也避免了病毒向更多的在线电脑传播。请先不要马上重新启动系统或是关机，进一步的处理措施请参看后文。

二、中毒后，应马上备份转移文档和邮件等

中毒后运行杀毒软件清除是不在话下的了，但为了防止杀毒软件误杀或是删掉你还处理完的文档和重要的邮件，你应该首先将它们转移备份到其他储存媒体上。有些长文件名的文件和未处理的邮件要求在windows下备份，所以第一点这里笔者建议您先不要退出windows，因为病毒一旦发作，可能就不能进入windows了。

不管这些文件是否带毒了，你都应该备份，用标签纸标记为待查即可。因为有些病毒是专门针对某个杀毒软件设计的，一运行就会破坏其他的文件，所以先备份是以防万一的措施。等你清除完硬盘内的病毒后，再来慢慢分析处理这些额外备份的文件较为妥善。

三、需要在windows下先运行一下杀CIH的软件(即使是带毒环境)

如果是发现了CIH病毒的，要注意不能完全按平时报刊和手册建议的措施，先关机、冷启动用系统盘来引导再杀毒，应在带毒的环境下也运行一次专杀CIH的软件。这样做，杀毒软件可能会报告某些文件在受读写保护无法清理，但带毒运行的实际目的不在于完全清除病毒，而是在于把CIH下次开机时候的破坏减到最低，以防它再次开机破坏主板的BIOS硬件，那么就会黑屏，让你的下一步杀毒无法进行。

四、需要干净的DOS启动盘和DOS下面进行杀毒

到现在，就应该按很多杀毒软件的标准手册去按步就班地做，即关机后冷启动，用一张干净的DOS启动盘引导是不能少的了;另外由于中毒后可能windows已经被破坏了部分关键文件，会频繁地非法操作，所以windows下的杀毒软件可能会无法运行。所以请你也准备一个DOS下面的杀毒软件来以防万一。

即使能在windows下运行杀毒软件的，也请用两种以上工具交叉清理。在多数情况下windows可能要重装，因为病毒会破坏掉一部分文件让系统变慢或出现频繁的非法操作。比如即使杀了CIH，微软的outlook邮件程序也是反应较慢的。建议不要对某种杀毒软件带偏见，由于开发时候侧重点不同、使用的杀毒引擎不同，各种杀毒软件都是有自己的长处和短处的，交叉使用效果较理想。

五、如果有Ghost和分区表、引导区的备份，用之来恢复一次最保险

如果你在平时作了windows的Ghost备份，用之来镜像一次，得到的操作系统是最保险的。这样连潜在的未杀光的木马程序也顺便清理了，当然，这要求你的GHOST备份是绝对可靠的，呵呵，要是作Ghost的时候把木马也“备份”了就……

六、再次恢复系统后，更改你的网络相关密码

包括登录网络的用户名、密码，邮箱的密码和QQ的等等，防止黑客已经在上次入侵过程中知道了你的密码。另外因为很多蠕虫病毒发作会向外随机发送你的信息，所以适当的更改是必要的。

以上所述是Caesar给大家介绍的电脑感染病毒的10种症状及简单处理办法的相关知识，希望对大家有所帮助，如果大家有任何疑问请给我留言，Caesar会及时回复大家的电脑病毒知识：病毒能破坏电脑硬件吗?

按照不同的维度，电脑病毒可以分为很多种，根据病毒的破坏能力可划分为以下几种：

无害型：除了传染时减少磁盘的可用空间外，对系统没有其它影响。

无危险型：这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

危险型：这类病毒在计算机系统操作中造成严重的错误。

高危险型：这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

值得注意的是，一些无害型病毒也可能会对新版的DOS、Windows和其它操作系统造成破坏。比方说，在早期的病毒中，有一个“Denzuk”病毒在360K磁盘上能很好地工作，不会造成任何破坏，但是在高密度软盘上却会引起大量的数据丢失。

对电脑硬件造成破坏的病毒属于高危险型病毒，这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料和灾难性的破坏，由这些病毒导致其它程序产生的错误也会破坏文件和扇区。

曾搞得人心惶惶、掀起了不小波澜的CIH病毒就是一种能够破坏计算机系统硬件的恶性病毒。它是已被认定的首例能够破坏计算机系统硬件的病毒，同时也是最具杀伤力的恶性病毒。

CIH病毒的传播途径主要是Internet和电子邮件，使计算机病毒的传播首次摆脱了传统存储介质的束缚，让Internet和光盘成为加速计算机病毒传播最有效的催化剂。CIH病毒发作时，一方面全面破坏计算机系统硬盘上的数据，另一方面对某些计算机主板的BIOS进行改写。BIOS被改写后，系统无法启动，只有将计算机送回厂家修理，更换BIOS芯片。由于CIH病毒对数据和硬件的破坏都是不可逆的，所以一旦CIH病毒爆发，用户只能眼睁睁地看着价值不菲的计算机和积累多年的重要数据毁于一旦。

其实，病毒破坏硬件的“手段”，不外乎有以下几种，了解了这些“手段”，有助于我们及时找到预防方法和应对策略。

1、破坏主板、显卡的Flash BIOS

CIH病毒就是以该方式破坏主板的。病毒用乱码“冲掉”了BIOS中的内容，使机器不能启动。不过现在很多主板都带有FlashBIOS写保护跳线，可以有效防止CIH病毒破坏主板。

2、破坏硬盘

一般情况下，分区、高级格式化对硬盘都没有什么损伤，惟独低级格式化对硬盘的寿命有较大的影响。如果出现一种病毒，不停地对硬盘的0磁道做低格式化，硬盘容量就会慢慢被蚕食，而且0、1、2……磁道坏了，若想再使用该硬盘，需要在BIOS中重新设定起始磁道，再进行低级格式化，操作较为繁琐。

3、破坏光驱

光驱中的光头读取不到信号时就会加大激光发射功率，长期如此将会影响光驱的使用寿命。病毒可以让光头走到盘片边缘无信号区域不停地读盘，光头在无法读取信号的情况下，加大发射功率努力读盘，持续不了几天，光驱就要“NoDisc”了。所以要经常注意光驱灯的闪亮情况，判断光驱是否在正常工作。

4、超外频、加电压破坏CPU、显卡、内存等

病毒通过改BIOS参数，加高CPU电压使其过热而烧坏，或提高CPU的外频，使CPU和显卡、内存等外设超负荷工作而过热烧坏。这类事件的前兆就是死机。可喜的是，目前很多主板都有CPU温度监测功能，超温后立即降频报警，基本可以杜绝烧坏硬件的情况发生。

5、超“显频”破坏显卡

目前很多中高档显卡等都可以手动改变其芯片的频率，并且方法更简单，直接在Windows注册表里修改即可。如果病毒改动了“显频”，显卡就容易超负荷工作而烧坏。这种情况的前兆是死机，因此，当电脑频频死机时，请不要忽视对“显频”的检查。

6、破坏显示器

众所周知，每台显示器都有自己的带宽和最高分辨率、场频，彼此之间有固定的配合。若其中有一项超过，就会出现花屏，严重了还会烧坏显示器。病毒可以通过篡改显示参数来破坏显示器(如把分辨率、场院频改到显卡能支持的最高档等)。虽然新型显示器有DDC标准化与系统联络，但是若在使用过程中显示器出现了花屏，建议还是立即关掉显示器的电源，重新启动后进入安全模式再找排查原因。

从计算机病毒的发展史来看，病毒的出现与消匿都遵循一定的规律。一种新病毒出现后在一段时间内会迅速传播、发展变种，然而反病毒技术也随之产生，抑制其扩散、作恶。随着操作系统升级，更多新的病毒会出现，反病毒技术再结合病毒特点研究解决之法。计算机病毒与反病毒技术在相互牵制的过程中使自身不断发展壮大。反计算机病毒是一个漫长而持续的过程，路漫漫其修远兮，吾将上下而求索。

防范电脑病毒，这些知识点你get了吗?

许我们曾听人说过：“电脑有病毒了，赶紧找杀毒软件!”电脑又不是动物和人类，它怎么会有病毒呢?

电脑病毒是由人所编写的，存在电脑中的一种短小、特殊的程序，这种程序平时处于“安静”状态，并不马上发作，在一定情况下，它就会发作，对电脑系统造成破坏。例如，小球病毒就是一种电脑病毒，它发作时，会出现许多跳跃的小球，再提示“你的电脑成为石头!”接着，电脑中的数据就慢慢被破坏掉了。使计算机无法启动。另外，蠕虫病毒能通过网络邮件系统快速自动扩散传播，在短时间内造成大面积网络阻塞或造成世界的互联网络瘫痪。有一些病毒还可以通过网络任意控制你的计算机，并获得重要文件等等。电脑病毒能够像生物病毒一样，在许多电脑之间传播，危害极大。电脑可以通过软件盘、网络传播，使电脑“生病”。

预防与防护

1、如何预防电脑中病毒?

安装杀毒软件及网络防火墙，及时更新病毒库。

不随意安装不知晓的软件。

不去安全性得不到保障的网站。

从网络下载后及时杀毒。

关闭多余端口，做到使电脑在合理的使用范围之内。

关闭IE安全中的ACTIVE\_\_运行，好多网站都是使用它来入侵你的电脑。

如果有条件，尽量使用非IE内核的浏览器，如OPERA。

不要使用修改版的软件，如果一定要用，请在使用前查杀病毒&木马，以确保安全。

2、中勒索病毒怎么办?

Win7、Win8、Win10的处理流程：

打开控制面板-系统与安全-Windows防火墙，点击左侧启动或关闭Windows防火墙。

选择启动防火墙，并点击确定。

点击高级设置。

点击入站规则，新建规则。

选择端口，下一步。

特定本地端口，输入445，下一步。

选择阻止连接，下一步。

配置文件，全选，下一步。

名称，可以任意输入，完成即可。

3、中其他病毒怎么办?

(1)电脑还可以运行。

1.如果电脑中毒后，可以正常运行，那么就千万不要再去进行登录什么账号或者是修改密码等操作，应该及时的使用电脑杀毒软件给你的电脑杀毒。

2.然后等待杀毒完成后，一定要重启电脑，因为大多数病毒都是在重启后，才会彻底清除的，重启完成后，再去修改你中毒期间用过的账号密码。

(2)电脑无法正常运行。

1.如果中毒后，电脑出现无法正常运行的情况，例如说程序打不开，电脑键盘鼠标被锁定死机，那么一定要及时的拔出的你网线，用无线路由器的直接关闭路由器。

2.然后重启电脑的过程中，不停按F8进入网络安全模式，然后再去正常连接网络，下载电脑中的杀毒软件，给你的电脑杀毒就可以了。

3.或者直接重装系统，然所有盘的都格式化一遍。

**第二篇：电脑病毒知识了解和科普**

病毒一直以来大部分的用户都非常关注与对其感到非常好奇，一个短短的代码就可以让整个系统崩溃甚至死机，下面就让小编带你去看看电脑病毒知识和了解，希望能帮助到大家!

被电脑病毒攻击了怎么办?带你一一识破九种病毒软件!

你对病毒软件了解吗?

接下来我们将要介绍九种常见的病毒软件，以确保知道你被攻击时如何处理。

1.病毒

计算机病毒是大多数媒体和普通终端用户在新闻报道中所称的每一个恶意软件程序。

幸运的是，大多数恶意软件程序都不是病毒。计算机病毒修改其他合法主机文件，当受害者的文件被执行时，病毒也被执行。

纯粹的计算机病毒在今天并不常见，只占所有恶意软件的10%不到。

病毒是唯一一种“感染”其他文件的恶意软件。这使得他们特别难以清理，因为恶意软件必须从合法程序执行。

这样使得即便最好的杀毒程序也很难消灭它，不过，也有在许多情况下，我们只需要隔离或删除受感染的文件即可。

2.蠕虫

蠕虫比计算机病毒存在的时间还要长，可以追溯到大型机时代。

20世纪90年代末，电子邮件的使用使蠕虫流行起来，近十年来，计算机安全专家受困于被作为消息附件出现的恶意蠕虫。

一个人打开一封蠕虫邮件，整个公司很快就会被感染。

3.木马

电脑蠕虫已被特洛伊木马恶意软件取代，成为黑客们的首选武器。

木马伪装成合法的程序，但它们包含恶意指令。它们已经存在了很长时间，甚至比计算机病毒还长，而且更容易入侵我们的计算机。

4.多种形式病毒和外来物种

通常，恶意软件程序在终端用户看来是特洛伊木马，但一旦执行，它就会像蠕虫一样通过网络攻击其他受害者。

今天的许多恶意软件程序被认为是rootkit木马或秘密程序。从本质上讲，恶意软件程序试图修改底层操作系统，以获得最终控制权并躲避防恶意软件程序。

要消除这些类型的程序，您必须从内存中删除控制组件，首先是防恶意软件扫描。

僵尸程序本质上是特洛伊木马、蠕虫病毒的组合，它试图使个别被利用的客户端成为一个更大的恶意网络的一部分。

僵尸网络的规模从几千台受攻击的计算机到一个由一个僵尸网络主机控制的拥有数十万个系统的巨大网络不等。

这些僵尸网络经常被出租给其他犯罪分子，他们利用这些网络达到自己的邪恶目的。

5.勒索软件

勒索软件会加密您的数据，并将其作为人质，这一直是过去几年来勒索软件获得巨大回报的手段，而且这种情况仍然在不断增多。

勒索软件经常使公司、医院、警察局甚至整个城市陷入瘫痪。

大多数勒索软件程序都是木马程序，这意味着它们必须通过某种社会工程来传播。

勒索软件可以像其他任何类型的恶意软件程序一样被阻止，但是一旦被执行，如果没有备份，就很难逆转破坏。

根据一些研究，大约四分之一的受害者支付了赎金，其中大约30%的人仍然没有获得被解锁的文件。

无论哪种方式，打开加密的文件都需要特定的工具、解密密钥甚至一些运气。建议最好确保所有关键文件都有离线备份。

6.无文件恶意软件

传统的恶意软件通过文件系统传播并感染新系统。

无文件恶意软件目前占所有恶意软件的50%以上，而且还在不断增长，它是一种不直接使用文件或文件系统的恶意软件。

最终的结果是，无文件攻击更难检测和停止。如果您想从事计算机安全方面的工作，您应该非常熟悉这些技术和程序。

7.广告软件

广告软件是最轻微也最容易中招的恶意软件，它试图让受攻击的终端用户暴露在不必要的、潜在的恶意广告中。

一个常见的广告软件程序可能会将用户的浏览器搜索重定向到包含其他产品促销信息的类似web页面。

8.恶意广告

不要与广告软件混淆，恶意广告是使用合法的广告或广告网络，偷偷地向毫无戒心的用户的电脑发送恶意软件。

例如，网络罪犯可能会花钱在合法网站上投放广告。当用户点击广告时，广告中的代码要么将他们重定向到恶意网站，要么在他们的电脑上安装恶意软件。

在某些情况下，嵌入广告中的恶意软件可能会自动执行，而不需要用户执行任何操作，这种技术被称为“偷渡下载”。

9.间谍软件

间谍软件最常被那些想要查看亲人电脑活动的人使用。

当然，在有针对性的攻击中，犯罪分子可以使用间谍软件来记录受害者的按键，并获得密码或知识产权。

广告软件和间谍软件程序通常是最容易删除的，通常是因为它们的意图不像其他类型的恶意软件那么邪恶。

找到恶意的可执行文件并阻止它被执行——你就完成了。

查找和删除恶意软件

如今，许多恶意软件程序一开始都是特洛伊木马或蠕虫，但随后却被植入僵尸网络，让黑客进入受害者的电脑和网络。

许多高级持续威胁攻击(APT)都是以这种方式开始的:它们使用木马获得进入数百或数千家公司的最初立足点，而人类攻击则潜伏在其中，以寻找有趣的知识产权。

绝大多数恶意软件的存在是为了偷钱——直接从银行账户里偷钱，或者通过偷密码或身份信息来间接偷钱。

如果幸运的话，您可以使用Microsoft的Autoruns、Microsoft的Process E\_\_plorer或Silentrunner等程序找到恶意的可执行程序。

如果恶意软件程序是隐形的，您必须先从内存中删除隐藏组件，然后再将程序的其余部分提取出来。

通常情况下，将引导MicrosoftWindows进入安全模式或通过其他方法，删除可疑的隐身组件，并运行防病毒扫描器，在删除了隐身部分后清理剩余部分。

不幸的是，寻找和删除单个恶意软件程序组件很容易出错。

此外，您不知道恶意软件程序是否已经修改了系统，使其不可能再完全值得信任。

除非你在恶意软件清除和取证方面受过良好的训练，否则，当你在电脑上发现恶意软件时，备份数据，格式化驱动器，重新安装程序和数据。

做好补丁，确保最终用户知道他们做错了什么。这样，你就得到了一个值得信赖的计算机平台，在战斗中勇往直前，没有任何挥之不去的风险或问题。

带你认识电脑病毒

1.病毒存在的媒体

根据病毒存在媒体，病毒可以划分为网络病毒，文件病毒，引导型病毒。网络病毒通过电脑网络传播感染网络中的可执行文件，文件病毒感染电脑中的文件(如：COM，E\_\_E，DOC等)，引导型病毒感染启动扇区(Boot)与硬盘系统引导扇区(MBR)，还有这三种情况的混合型，例如：多型病毒(文件与引导型)感染文件和引导扇区两种目标，这样的病毒通常都具有复杂算法，它们使用非常规的办法侵入系统，同时使用了加密与变形算法。

2.病毒破坏力

根据病毒破坏力可划分为以下几种：

无害型：除了传染时减少磁盘可用空间外，对系统没有其它影响。

无危险型：这类病毒仅仅是减少内存，显示图像，发出声音及同类音响。

危险型：这类病毒在电脑系统操作中造成严重的错误。

非常危险型：这类病毒删除程序，破坏数据，清除系统内存区与操作系统中重要信息。

这些病毒对系统造成的危害并不是本身算法中存在危险的调用，而是当它们传染时会引起无法预料与灾难性的破坏。由病毒引起其它程序产生的错误也会破坏文件和扇区，这些病毒也按照他们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的DOS，Windows和其它操作系统造成破坏。例如：在早期病毒中，有一个“Denzuk”病毒在360K磁盘上很好的工作，不会造成任何破坏，但是在后来的高密度软盘上却能引起大量数据丢失。

3.病毒特有的算法

根据病毒特有算法，病毒可以划分为：

伴随型病毒：这一类病毒并不改变文件本身，它们根据算法产生E\_\_E文件的伴随体，具有同样的名字与不同的扩展名(COM)，例如：\_\_COPY.E\_\_E的伴随体是http://\_\_COPY.COM。病毒把自身写入COM文件并不改变E\_\_E文件，当DOS加载文件时，伴随体优先被执行到再由伴随体加载执行原来的E\_\_E文件。

“蠕虫”型病毒：通过计算机网络传播，不改变文件与资料信息，利用网络从一台机器的内存传播到其它机器的内存，计算网络地址，将自身的病毒通过网络发送。有时它们在系统存在，一般除了内存不占用其它资源。

寄生型病毒：除了伴随与“蠕虫”型，其它病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统功能进行传播，按算法分为：

练习型病毒：病毒自身包含错误不能进行很好的传播，例如一些病毒在调试阶段。

诡秘型病毒：它们一般不直接修改DOS中断与扇区数据，而是通过设备技术与文件缓冲区等DOS内部修改，不易看到资源，使用比较高级的技术。利用DOS空闲的数据区进行工作。

变型病毒(又称幽灵病毒)：这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容与长度。它们一般作法是一段混有无关指令的解码算法与被变化过的病毒体组成。

恶意病毒“四大家族”

一、宏病毒

由于微软的Office系列办公软件和Windows系统占了绝大多数的电脑软件市场，加上Windows和Office提供了宏病毒编制与运行所必需的库(以VB库为主)支持和传播机会，所以宏病毒是最容易编制与流传的病毒之一，很有代表性。

宏病毒发作方式：在Word打开病毒文档时，宏会接管计算机，然后将自己感染到其他文档或直接删除文件等等。Word将宏和其他样式储存在模板中，因此病毒总是把文档转换成模板再储存它们的宏。这样的结果是某些Word版本会强迫你将感染的文档储存在模板中。

判断是否被感染：宏病毒一般在发作的时候没有特别的迹象，通常是会伪装成其他的对话框让你确认。在感染了宏病毒的机器上，会出现不能打印文件，Office文档无法保存或另存为等情况。

宏病毒带来的破坏：删除硬盘上文件，将私人文件复制到公开场合，从硬盘上发送文件到指定的E-mail，FTP地址。

防范措施：平时最好不要几个人共用一个Office程序，要加载实时的病毒防护功能。病毒变种可以附带在邮件的附件里，在用户打开邮件或预览邮件的时候执行应该留意，一般杀毒软件都可以清除宏病毒。

二、CIH病毒

CIH是本世纪最著名与最有破坏力病毒之一，它是第一个能破坏硬件的病毒。

发作破坏方式：主要是通过篡改主板BIOS里的数据造成电脑开机就黑屏，从而让用户无法进行任何数据抢救与杀毒的操作。CIH的变种能在网络上通过捆绑其他程序或是邮件附件传播，并且常常删除硬盘上的文件及破坏硬盘的分区表。所以CIH发作以后，即使换了主板或其他电脑引导系统，如果没有正确的分区表备份，染毒的硬盘上特别是其C分区的数据挽回的机会很少。

防范措施：已经有很多CIH免疫程序诞生了，包括病毒制作者本人写的免疫程序。一般运行了免疫程序就可以不怕CIH了。如果已经中毒但尚未发作，记得先备份硬盘分区表与引导区数据再进行查杀，以免杀毒失败造成硬盘无法自举。

三、蠕虫病毒

蠕虫病毒以尽量多复制自身(像虫子一样大量繁殖)而得名，多感染电脑与占用系统，网络资源，造成电脑与服务器负荷过重而死机，并以使系统内数据混乱为主要的破坏方式。它不一定马上删除你的数据让你发现，比如著名的爱虫病毒与尼姆达病毒。

四、木马病毒

木马病毒源自古希腊特洛伊战争中著名的“木马计”而得名，顾名思义就是一种伪装潜伏的网络病毒，等待时机成熟就出来害人。

传染方式：通过电子邮件附件发出，捆绑在其他的程序中。

病毒特性：会修改注册表，驻留内存，在系统中安装后门程序，开机加载附带木马。

木马病毒的破坏性：木马病毒发作要在用户的机器里运行客户端程序，一旦发作就可设置后门，定时地发送该用户的隐私到木马程序指定的地址，一般同时内置可进入该用户电脑的端口，并可任意控制此计算机，进行文件删除，拷贝，改密码等非法操作。

关于电脑病毒的知识

电脑病毒到底是什么?

电脑病毒(以下均用病毒代替)到底是什么呢?

说出来你可能不信，病毒跟我们电脑上的QQ呀，浏览器呀这些本质上并没有什么区别。

甚至可以说，病毒只是我们电脑里面的平平无奇的程序而已。

说程序也许不太好理解，说软件你就知道了吧。

既然它们也是软件，那它们为什么被称之为病毒呢?

这是因为，它思想出了问题，你还别笑，事情真就是这样的。

举个栗子大家肯定就更清楚了，小偷跟抢劫犯也和我们一样是正常的人吧?

但是他们为什么会被称作小偷和抢劫犯，还被抓起来呢?

就是他们思想出了点问题，正常人一般不会去偷东西跟抢劫吧?

思想出了问题是首要原因，还有一个很重要的原因，就是他们做了危害社会的事情，也就是偷了东西和抢了东西，如果只是想，并没有真正的实施，那也不能抓他们不是。

回到正题，现在我们就知道了，病毒本质上也是软件，跟我们电脑里面装的那些软件没什么不同。

但之所以称它为病毒呢，是因为它可以对我们的电脑做有危害的事情。

现在你知道病毒是什么了吧?

它就是想对我们电脑不利的软件。没错，就是这么的简单。

那么安装杀毒软件是为了什么呢?

就是在它们动手之前抓住它们，不让它们得逞，这就是杀毒软件的作用!

木马和病毒有什么区别

除了病毒，我们还经常听到的一个词叫做木马，那么木马跟病毒又有什么区别呢?

木马本质上也是一种病毒，因为它也会对电脑产生危害。

但是由于它的目的和作案手法跟一般的病毒不太一样，所以我们就把它单独拎了出来，还给它起了个名字叫木马。

病毒因为对电脑有害，所以叫做病毒。那木马这个名字又是从何而来的呢?

这听着跟电脑好像没啥关系呀?

别急，先听我给大家说段 木马屠城记 的故事吧。

传说古希腊时代，特洛伊有个王子叫帕里斯。

帕里斯在访问希腊的时候，拐走了希腊的王后 海伦。

为此，希腊人与特洛伊结下了血海深仇，希腊国王决定要远征特洛伊。

特洛伊城墙可以说是坚不可摧，希腊人攻了9年，也没攻下特洛伊的城池。

到第10年的时候，希腊将领奥德修斯献了一计。

他把一批勇士藏进一匹巨大的木马腹内，放在城外，然后佯作退兵。

特洛伊人以为敌兵已退，就把木马作为战利品搬入了城中。

到了夜间，埋伏在木马中的勇士跳了出来，打开了城门，希腊将士一拥而入攻下了城池。

而我们计算机中的木马，就是从这个故事借鉴来的。

因为我们的木马程序干的也是同样的事情：先悄悄的潜伏在你的计算机里，等需要它们的时候呢，它们再开始干活。

所以木马的特点就是难以发现，平时基本没什么危害，但是隐患很大!

我们经常听说谁谁的电脑被控制了，用的就是木马。

总结一下，木马就是一个别人在你不知道的情况下用来控制你电脑的软件。

为什么要强调你不知道呢?

因为还有很多控制你电脑的软件嘛

比如Teamviewer、向日葵，这些都是用来控制电脑，但都是在你知道并允许的情况下操作的，所以它们是合法软件嘛。

一般的病毒呢基本上就是以破坏你的电脑为主要工作。

比如大名鼎鼎的熊猫烧香就是一款破坏力极大的病毒，它能把电脑里的所有文件都变成熊猫烧香的图标，严重的甚至可能导致死机。

还有 17 年的永恒之蓝勒索病毒，它能把我们电脑上的文件全部都锁住，只有交了钱才可以解开。

病毒一般都有较大的危害性和可传播性。

**第三篇：(EDP.003)酒店电脑病毒防范管理制度**

第一章 总则

第一条 为明确北京唐韵山庄酒店电脑主管部门对计算机设备的维护管理职责，规范酒店信息系统用户行为，制定本制度。

第二条 本制度中所指计算机设备属于酒店的固定资产，包括台式计算机、显示器、笔记本电脑、打印机、复印机、扫描仪等设备；计算机耗材主要包括键盘、鼠标、刻录光盘（DVD/CD）、色带、墨盒、墨粉、硒鼓等。

第三条 本制度中的笔记本电脑是指利用酒店资金购买配置，供本酒店员工公务使用的笔记本电脑。

第四条 本制度适用于酒店所有部门管理人员和员工。

第二章 职责

第五条 酒店电脑部为本酒店计算机设备归口管理部门，负责计算机设备及桌面系统的维护和管理工作，负责对本酒店的计算机设备使用进行监督、管理、维护。

第六条 酒店各业务部门应设置电脑协管人员，确认电脑使用责任人，协助电脑部做好本部门的计算机设备管理工作。

第七条 计算机设备的管理采用“谁使用，谁负责”的原则。酒店用户有保护计算机设备物理安全的责任和义务，应按规定放置、保管、使用和归还计算机设备。

第三章酒店电脑病毒防范管理制度

第八条 电脑部负责对本酒店病毒防范工作统一组织实施，指定专人作为管理员来负责具体实施此项工作，管理员定期对各部门防病毒软件版本和软件病毒码升级和更新进行检查。

第九条 电脑部建立病毒防治监控服务系统，确保每台在网计算机都安装有防病毒软件，并负责对防病毒软件进行升级和在网计算机实施病毒监控管理，强制实施统一的防病毒策略，任何人不得随意更改防病毒策略。

第十条 各部门要认真落实防病毒管理职责，加强对员工的防病毒知识教育和防病毒工作自查。计算机用户有防范病毒和恶意软件的责任和义务。

1．未安装防病毒软件的计算机用户应联系电脑部进行安装，否则因未安装杀毒软件造成的后果由用户负责。

2．用户要定期查看计算机是否更新了病毒数据代码，如果防病毒软件出现工作异常，病毒特征库过旧（距离最近一次更新时间超过两周）等问题，应该及时通知计算机维护人员进行维护。

3．严禁用户以任何方式卸载防病毒软件、停止防病毒服务和更改防病毒软件配置。

4．计算机用户发现计算机中病毒时应该立刻断开网络连接，必要时关闭计算机，并及时报告电脑部。

5．笔记本电脑应定期接入局域网进行病毒库更新和查杀病毒。

6．应控制来源不明的介质、不明安全来源的下载软件或文档、不明安全的邮件和超级链接等。

7．外来移动存储介质应在进行病毒检查和杀毒后才可在计算机设备上使用。

第十一条 严禁未安装防病毒软件的计算机接入局域网。电脑部应定期检查各部门的计算机防病毒工作进行检查，并通报检查结果。

第十二条 电脑部应对防病毒软件制定相应的实施策略，对所有计算机实施实时监控扫描，客户机可以根据需要进行手动扫描；每周进行预设病毒扫描并生成报告。电脑部还应对易受病毒攻击的机器：如邮件服务器、外部网站、经常接入外网的有盘站、远程通讯用机等设备启用实时杀毒并每天查毒。

第十三条 若用户计算机中毒后主动攻击其他计算机，影响局域网正常使用时，电脑技术人员必须迅速对其网络使用做安全限制或断开该用户的网络连接，待查明中毒原因和清除彻底后，才允许重新接入局域网。

任何人不得研究、制作、散布计算机病毒、黑客程序、木马程序，不得故意危害信息系统的安全，不得向他人提供含有病毒、黑客程序、木马程序的文件、软件和媒体。

**第四篇：电脑病毒的传播**

计算机病毒传播方式除传统的软盘、U盘和盗版光盘传播外，目前主要是通过因特网传播。

就当前的病毒特点分析，传播途径有两种，一种是通过网络传播，一种是通过硬件设备传播。首先，我们来看看网络传播的途径和解决方案。

网络传播，又分为因特网传播和局域网传播两种。网络信息时代，因特网和局域网已经融入了人们的生活、工作和学习中，成为了社会活动中不可或缺的组成部分。特别是因特网，已经越来越多地被用于获取信息、发送和接收文件、接收和发布新的消息以及下载文件和程序。随着因特网的高速发展，计算机病毒也走上了高速传播之路，已经成为计算机病毒的第一传播途径。

一、因特网传播:

Internet既方便又快捷，不仅提高人们的工作效率，而且降低运作成本，逐步被人们所接受并得到广泛的使用。商务来往的电子邮件，还有浏览网页、下载软件、即时通讯软件、网络游戏等等，都是通过互联网这一媒介进行。如此频繁的使用率，注定备受病毒的“青睐”。

通过电子邮件传播:

在电脑和网络日益普及的今天，商务联通更多使用电子邮件传递，病毒也随之找到了载体，最常见的是通过Internet交换Word格式的文档。由于Internet使用的广泛，其传播速度相当神速。电子邮件携带病毒、木马及其他恶意程序，会导致收件者的计算机被黑客入侵。email协议的新闻组、文件服务器、FTP下载和BBS文件区也是病毒传播的主要形式。经常有病毒制造者上传带毒文件到FTP和BBS上，通常是使用群发到不同组，很多病毒伪装成一些软件的新版本，甚至是杀毒软件。很多病毒流行都是依靠这种方式同时使上千台计算机染毒。

BBS是由计算机爱好者自发组织的通讯站点，因为上站容易、投资少，因此深受大众用户的喜爱，用户可以在BBS上进行文件交换(包括自由软件、游戏、自编程序)。由于BBS站一般没有严格的安全管理，亦无任何限制，这样就给一些病毒程序编写者提供了传播病毒的场所。各城市BBS站间通过中心站间进行传送，传播面较广。随着BBS在国内的普及，给病毒的传播又增加了新的介质。

专家提示:培养良好的安全意识。对来历不明的陌生邮件及附件不要轻易打开，即使是亲朋好友的邮件也要倍加小心。通过浏览网页和下载软件传播:

很多网友都遇到过这样的情况，在浏览过某网页之后，IE标题便被修改了，并且每次打开IE都被迫登陆某一固定网站，有的还被禁止恢复还原，这便是恶意代码在作怪。当你的IE被修改，注册表不能打开了，开机后IE疯狂地打开窗口，被强制安装了一些不想安装的软件，甚至可能当你访问了某个网页时，而自己的硬盘却被格式化……那么很不幸，你肯定是中了恶意网站或恶意软件的毒了。

当您浏览一些不健康网站或误入一些黑客站点，访问这些站点的同时或单击其中某些链接或下载软件时，便会自动在您的浏览器或系统中安装上某种间谍程序。这些间谍程序便可让您的浏览器不定时地访问其站点，或者截获您的私人信息并发送给他人。“屏蔽恶意网站”功能，使用内臵默认和自由添加两个方式确定恶意网站列表，识别恶意网站地址，有效封杀通过恶意网站进行感染的病毒和木马。同时，随着光华反病毒软件的每日自动升级，恶意网站列表将不断更新，所以不必担心列表中的网站数量有限。

“绿色上网功能”，可以屏蔽上网过程中出现的各种恶意组件，免受间谍软件、广告软件的打扰真正实现您自由自在的网络游弋。

拒绝恶意软件:在光华反病毒软件中点击菜单“工具→插件→绿色上网”，打开绿色上网插件窗口。同样，针对不同类型的恶意软件，光华为我们进行了详细的分类，有国内、国外、聊天、安全、游戏等等。我们在相应的分类上点选自己想屏蔽的组件，即可屏蔽上网过程中出现的各种恶意组件，免受间谍软件、广告软件的打扰。

“关闭IE广告窗口”即可禁止某些网站的弹出广告，让你用IE上网时更加省心。

提示:不要随便登陆那些很诱惑人的小网站，因为这些网站很可能有网络陷阱。不要轻易下载小网站的软件与程序，下载的软件需先进行安全检查，确认无安全无病毒后再安装使用，确保您的计算机始终处于安全的环境下。

通过即时通讯软件传播:

即时通讯(Instant Messenger，简称IM)软件可以说是目前我国上网用户使用率最高的软件，它已经从原来纯娱乐休闲工具变成生活工作的必备利器。由于用户数量众多，再加上即时通讯软件本身的安全缺陷，例如内建有联系人清单，使得病毒可以方便地获取传播目标，这些特性都能被病毒利用来传播自身，导致其成为病毒的攻击目标。事实上，臭名昭著、造成上百亿美元损失的求职信(Worm.Klez)病毒就是第一个可以通过ICQ进行传播的恶性蠕虫，它可以遍历本地ICQ中的联络人清单来传播自身。而更多的对即时通讯软件形成安全隐患的病毒还正在陆续发现中，并有愈演愈烈的态势。截至目前，通过QQ来进行传播的病毒已达上百种。

P2P，即对等互联网络技术(点对点网络技术)，它让用户可以直接连接到其它用户的计算机，进行文件共享与交换。每天全球有成千上万的网民在通过P2P软件交换资源、共享文件。由于这是一种新兴的技术，还很不完善，因此，存在着很大的安全隐患。由于不经过中继服务器，使用起来更加随意，所以许多病毒制造者开始编写依赖于P2P技术的病毒。

提示: 在聊天时收到好友发过来的可疑信息时，千万不要随意点击，应当首先确定是否真的是好友所发。要防范通过IRC传播的病毒，还需注意不要随意从陌生的站点下载可疑文件并执行，而且轻易不要在IRC频道内接收别的用户发送的文件，以免计算机受到损害。

通过网络游戏传播:

网络游戏已经成为目前网络活动的主体之一，更多的人选择进入游戏来缓解生活的压力，实现自我价值，可以说，网络游戏已经成了一部分人生活中不可或缺的东西。对于游戏玩家来说，网络游戏中最重要的就是装备、道具这类虚拟物品了，这类虚拟物品会随着时间的积累而成为一种有真实价值的东西，因此出现了针对这些虚拟物品的交易，从而出现了偷盗虚拟物品的现象。一些用户要想非法得到用户的虚拟物品，就必须得到用户的游戏帐号信息，因此，目前网络游戏的安全问题主要就是游戏盗号问题。由于网络游戏要通过电脑并连接到网络上才能运行，偷盗玩家游戏账号、密码最行之有效的武器莫过于特洛伊木马(Trojan horse)，专门偷窃网游账号和密码的木马也层出不穷，这种攻击性武器无论是菜鸟级的黑客，还是研究网络安全的高手，都视为最爱。

二、局域网传播

局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。组成网络的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此，有可能在很短的时间内感染整个网络中的计算机。局域网络技术的应用为企业的发展作出巨大贡献，同时也为计算机病毒的迅速传播铺平了道路。同时，由于系统漏洞所产生的安全隐患也会使病毒在局域网中传播。

三、通过不可移动的计算机硬件设备传播

此种传播方式，是通过不可移动的计算机硬件设备进行病毒传播，其中计算机的专用集成电路芯片(ASIC)和硬盘为病毒的重要传播媒介。通过ASIC传播的病毒极为少见，但是，其破坏力却极强，一旦遭受病毒侵害将会直接导致计算机硬件的损坏，检测、查杀此类病毒的手段还需进一步的提高。

硬盘是计算机数据的主要存储介质，因此也是计算机病毒感染的重灾区。硬盘传播计算机病毒的途径是:硬盘向软盘上复制带毒文件、带毒情况下格式化软盘、向光盘上刻录带毒文件、硬盘之间的数据复制，以及将带毒文件发送至其它地方等。

专家提示:定期使用正版杀毒软件查杀病毒非常重要。

四、通过移动存储设备传播

更多的计算机病毒逐步转为利用移动存储设备进行传播。移动存储设备包括我们常见的软盘、磁带、光盘、移动硬盘、U盘(含数码相机、MP3等)、ZIP和JAZ磁盘，后两者仅仅是存储容量比较大的特殊磁盘。软盘主要是携带方便，早期在网络还不普及时，软盘是使用广泛、移动频繁的存储介质，因此也成了计算机病毒寄生“温床”。光盘的存储容量大，所以大多数软件都刻录在光盘上，以便互相传递;同时，盗版光盘上的软件和游戏及非法拷贝也是目前传播计算机病毒主要途径。随着大容量可移动存储设备如Zip盘、可擦写光盘、磁光盘(MO)等的普遍使用，这些存储介质也将成为计算机病毒寄生的场所。

随着时代的发展，移动硬盘、U盘等移动设备也成为了新攻击目标。而U盘因其超大空间的存储量，逐步成为了使用最广泛、最频繁的存储介质，为计算机病毒寄生的提供更宽裕的空间。目前，U盘病毒逐步的增加，使得U盘成为第二大病毒传播途径。专家提示:在学校里的公用机房、网吧等特定公共场所使用U盘(闪存)等移动设备的用户要特别谨慎小心，以防感染木马，造成自己的信息失密并被窃取。

五、无线设备传播

目前，这种传播途径随着手机功能性的开放和增值服务的拓展，已经成为有必要加以防范的一种病毒传播途径。随着智能手机的普及，通过彩信、上网浏览与下载到手机中的程序越来越多，不可避免的会对手机安全产生隐患，手机病毒会成为新一轮电脑病毒危害的“源头”。手机、特别是智能手机和3G网络发展的同时，手机病毒的传播速度和危害程度也与日俱增。通过无线传播的趋势很有可能将会发展成为第二大病毒传播媒介，并很有可能与网络传播造成同等的危害。

专家提示:使用手机上网功能时，应尽量以浏览信息为主，尽可能的减少从网上下载信息和文件，即便是有这方面的需求，也最好从一些正规网站上下载。收到带有病毒的短信或邮件立即删除，键盘被锁死应立即取下电池，然后重新开机进行删除。可先用光华反病毒软件手机版查杀病毒，如仍旧不能恢复正常的，请及时将手机送厂维修，避免病毒二次传播。

病毒的种类繁多，特性不一，只要掌握了其流通传播方式，便不难进行监控和查杀。

计算机病毒具有自我复制和传播的特点，因此，要彻底解决网络安全问题，必须研究病毒的传播途径，严防病毒的传播。分析计算机病毒的传播机理可知，只要是能够进行数据交换的介质都可能成为计算机病毒传播途径。就当前的病毒特点分析，传播途径有两种，一种是通过网络传播，一种是通过硬件设备传播。首先，我们来看看网络传播的途径和解决方案。

网络传播，又分为因特网传播和局域网传播两种。网络信息时代，因特网和局域网已经融入了人们的生活、工作和学习中，成为了社会活动中不可或缺的组成部分。特别是因特网，已经越来越多地被用于获取信息、发送和接收文件、接收和发布新的消息以及下载文件和程序。随着因特网的高速发展，计算机病毒也走上了高速传播之路，已经成为计算机病毒的第一传播途径。

一、因特网传播:

Internet既方便又快捷，不仅提高人们的工作效率，而且降低运作成本，逐步被人们所接受并得到广泛的使用。商务来往的电子邮件，还有浏览网页、下载软件、即时通讯软件、网络游戏等等，都是通过互联网这一媒介进行。如此频繁的使用率，注定备受病毒的“青睐”。

通过电子邮件传播:

在电脑和网络日益普及的今天，商务联通更多使用电子邮件传递，病毒也随之找到了载体，最常见的是通过Internet交换Word格式的文档。由于Internet使用的广泛，其传播速度相当神速。电子邮件携带病毒、木马及其他恶意程序，会导致收件者的计算机被黑客入侵。email协议的新闻组、文件服务器、FTP下载和BBS文件区也是病毒传播的主要形式。经常有病毒制造者上传带毒文件到FTP和BBS上，通常是使用群发到不同组，很多病毒伪装成一些软件的新版本，甚至是杀毒软件。很多病毒流行都是依靠这种方式同时使上千台计算机染毒。

BBS是由计算机爱好者自发组织的通讯站点，因为上站容易、投资少，因此深受大众用户的喜爱，用户可以在BBS上进行文件交换(包括自由软件、游戏、自编程序)。由于BBS站一般没有严格的安全管理，亦无任何限制，这样就给一些病毒程序编写者提供了传播病毒的场所。各城市BBS站间通过中心站间进行传送，传播面较广。随着BBS在国内的普及，给病毒的传播又增加了新的介质。

解决方案:光华反病毒软件特别设计了“邮件监视”功能、“邮件过滤设臵”插件，来支持各种类邮件客户端，在收发邮件时进行双向过滤，彻底查杀正文、附件、超文本中隐藏的一切病毒，并自动过滤垃圾邮件。

光华反病毒专家提示:培养良好的安全意识。对来历不明的陌生邮件及附件不要轻易打开，即使是亲朋好友的邮件也要倍加小心。

通过浏览网页和下载软件传播:

很多网友都遇到过这样的情况，在浏览过某网页之后，IE标题便被修改了，并且每次打开IE都被迫登陆某一固定网站，有的还被禁止恢复还原，这便是恶意代码在作怪。当你的IE被修改，注册表不能打开了，开机后IE疯狂地打开窗口，被强制安装了一些不想安装的软件，甚至可能当你访问了某个网页时，而自己的硬盘却被格式化……那么很不幸，你肯定是中了恶意网站或恶意软件的毒了。

当您浏览一些不健康网站或误入一些黑客站点，访问这些站点的同时或单击其中某些链接或下载软件时，便会自动在您的浏览器或系统中安装上某种间谍程序。这些间谍程序便可让您的浏览器不定时地访问其站点，或者截获您的私人信息并发送给他人。

解决方案:在登陆互联网时，打开《光华反病毒软件》中有关于互联网监视的几项功能，确保您的计算机享有实时防护的服务，遇到病毒及时反映并做出正确的处理。

光华反病毒软件的网页监视功能，可以有效阻挡非法网站中藏匿的恶意代码，轻松确保IE原有设臵不被篡改。

“屏蔽恶意网站”功能，使用内臵默认和自由添加两个方式确定恶意网站列表，识别恶意网站地址，有效封杀通过恶意网站进行感染的病毒和木马。同时，随着光华反病毒软件的每日自动升级，恶意网站列表将不断更新，所以不必担心列表中的网站数量有限。

“绿色上网功能”，可以屏蔽上网过程中出现的各种恶意组件，免受间谍软件、广告软件的打扰真正实现您自由自在的网络游弋。

拒绝恶意软件:在光华反病毒软件中点击菜单“工具→插件→绿色上网”，打开绿色上网插件窗口。同样，针对不同类型的恶意软件，光华为我们进行了详细的分类，有国内、国外、聊天、安全、游戏等等。我们在相应的分类上点选自己想屏蔽的组件，即可屏蔽上网过程中出现的各种恶意组件，免受间谍软件、广告软件的打扰。

“光闭IE广告窗口”即可禁止某些网站的弹出广告，让你用IE上网时更加省心。

光华反病毒专家提示:不要随便登陆那些很诱惑人的小网站，因为这些网站很可能有网络陷阱。不要轻易下载小网站的软件与程序，下载的软件需先进行安全检查，确认无安全无病毒后再安装使用，确保您的计算机始终处于安全的环境下。

通过即时通讯软件传播:

即时通讯(Instant Messenger，简称IM)软件可以说是目前我国上网用户使用率最高的软件，它已经从原来纯娱乐休闲工具变成生活工作的必备利器。由于用户数量众多，再加上即时通讯软件本身的安全缺陷，例如内建有联系人清单，使得病毒可以方便地获取传播目标，这些特性都能被病毒利用来传播自身，导致其成为病毒的攻击目标。事实上，臭名昭著、造成上百亿美元损失的求职信(Worm.Klez)病毒就是第一个可以通过ICQ进行传播的恶性蠕虫，它可以遍历本地ICQ中的联络人清单来传播自身。而更多的对即时通讯软件形成安全隐患的病毒还正在陆续发现中，并有愈演愈烈的态势。截至目前，通过QQ来进行传播的病毒已达上百种。

P2P，即对等互联网络技术(点对点网络技术)，它让用户可以直接连接到其它用户的计算机，进行文件共享与交换。每天全球有成千上万的网民在通过P2P软件交换资源、共享文件。由于这是一种新兴的技术，还很不完善，因此，存在着很大的安全隐患。由于不经过中继服务器，使用起来更加随意，所以许多病毒制造者开始编写依赖于P2P技术的病毒。

解决方案:当您使用QQ、MSN、UC、ICQ、IRC、雅虎通等即时通讯软件接收文件时，光华反病毒软件的“聊天监视”将实时过滤病毒，一旦发现异常，第一时间提出警示，保护您在聊天的时候不会被病毒感染。开启聊天监视还可以有效地避免您的QQ、MSN、雅虎通等聊天工具帐号、密码被盗。

光华反病毒专家提示:收到好友发过来的可疑信息时，千万不要随意点击，应当首先确定是否真的是好友所发。要防范通过IRC传播的病毒，还需注意不要随意从陌生的站点下载可疑文件并执行，而且轻易不要在IRC频道内接收别的用户发送的文件，以免计算机受到损害。

通过网络游戏传播:

网络游戏已经成为目前网络活动的主体之一，更多的人选择进入游戏来缓解生活的压力，实现自我价值，可以说，网络游戏已经成了一部分人生活中不可或缺的东西。对于游戏玩家来说，网络游戏中最重要的就是装备、道具这类虚拟物品了，这类虚拟物品会随着时间的积累而成为一种有真实价值的东西，因此出现了针对这些虚拟物品的交易，从而出现了偷盗虚拟物品的现象。一些用户要想非法得到用户的虚拟物品，就必须得到用户的游戏帐号信息，因此，目前网络游戏的安全问题主要就是游戏盗号问题。由于网络游戏要通过电脑并连接到网络上才能运行，偷盗玩家游戏账号、密码最行之有效的武器莫过于特洛伊木马(Trojan horse)，专门偷窃网游账号和密码的木马也层出不穷，这种攻击性武器无论是菜鸟级的黑客，还是研究网络安全的高手，都视为最爱。

解决方案:开启光华反病毒软件实时监视中的“网络游戏保护”，能有效的避免盗号程序的植入。光华反病毒软件的反木马功能也非常强大，它扫描系统端口，有效查杀网络游戏盗号木马等5万种以上。

在保护玩家游戏账号、密码上，光华反病毒更有其独创的“Online”技术，只要上网，系统自动进入在线防护状态，保护在线游戏的安全。

《光华反病毒》软件还提供了隐私保护功能，您可以将您常用的用户名、密码以及私密信息、各类帐号在这里做一下登记，这样就可以防止间谍软件将您的被保护信息以任何形式被窃取，为你的隐私加了一层保护壳。

二、局域网传播

局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。组成网络的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此，有可能在很短的时间内感染整个网络中的计算机。局域网络技术的应用为企业的发展作出巨大贡献，同时也为计算机病毒的迅速传播铺平了道路。同时，由于系统漏洞所产生的安全隐患也会使病毒在局域网中传播。

解决方案:打开《光华反病毒》将需要检测的文件直接拖拽到主程序界面上便可以快速查毒，方便快捷。对由于系统漏洞产生的隐患，也可以通过光华反病毒软件的“系统漏洞修护”功能进行完善。“系统漏洞修护”功能，可以找出目前您计算机系统存在的所有升级补丁，同时通过下载相应的更新补丁程序进行系统升级，使您系统达到最新状态，提高系统的安全性和稳定性，从而有效地避免病毒、黑客和恶意程序的攻击。

三、通过不可移动的计算机硬件设备传播

此种传播方式，是通过不可移动的计算机硬件设备进行病毒传播，其中计算机的专用集成电路芯片(ASIC)和硬盘为病毒的重要传播媒介。通过ASIC传播的病毒极为少见，但是，其破坏力却极强，一旦遭受病毒侵害将会直接导致计算机硬件的损坏，检测、查杀此类病毒的手段还需进一步的提高。

硬盘是计算机数据的主要存储介质，因此也是计算机病毒感染的重灾区。硬盘传播计算机病毒的途径是:硬盘向软盘上复制带毒

文件、带毒情况下格式化软盘、向光盘上刻录带毒文件、硬盘之间的数据复制，以及将带毒文件发送至其它地方等。

解决方案:定期用《光华反病毒软件》查毒，发现病毒后立即解除，并及时把反病毒软件升级到最新版本，以确保能有效查杀最新病毒。《光华反病毒软件》，能彻底清除18万种病毒和木马，查杀2024种以上压缩可执行文件中深藏的病毒，对未知病毒的查处率高达90%以上。同时，《光华反病毒》全球首创的Online技术，实时在线，实时自动升级，第一时间将最新升级文件主动分发到您的系统中，让您跟上全球安全技术更新的步伐。

光华反病毒专家提示:定期使用正版杀毒软件查杀病毒非常重要。如果暂时没有正版的反病毒软件，您也可以登陆《光华反病毒软件》官方网站()，在这里您可以使用“光华免费在线杀毒”，彻底检查您的计算机安全。“光华免费在线杀毒”具备正版《光华反病毒软件》的病毒查杀功能，其中包括对文件、邮件、压缩文件等的查杀防护，能彻底查杀18万多种病毒、木马、恶意脚本及有害数据。

四、通过移动存储设备传播

更多的计算机病毒逐步转为利用移动存储设备进行传播。移动存储设备包括我们常见的软盘、磁带、光盘、移动硬盘、U盘(含数码相机、MP3等)、ZIP和JAZ磁盘，后两者仅仅是存储容量比较大的特殊磁盘。软盘主要是携带方便，早期在网络还不普及时，软盘是使用广泛、移动频繁的存储介质，因此也成了计算机病毒寄生“温床”。光盘的存储容量大，所以大多数软件都刻录在光盘上，以便互相传递;同时，盗版光盘上的软件和游戏及非法拷贝也是目前传播计算机病毒主要途径。随着大容量可移动存储设备如Zip盘、可擦写光盘、磁光盘(MO)等的普遍使用，这些存储介质也将成为计算机病毒寄生的场所。

随着时代的发展，移动硬盘、U盘等移动设备也成为了新攻击目标。而U盘因其超大空间的存储量，逐步成为了使用最广泛、最频繁的存储介质，为计算机病毒寄生的提供更宽裕的空间。目前，U盘病毒逐步的增加，使得U盘成为第二大病毒传播途径。

解决方案:当把移动设备接入系统中时，光华反病毒软件会自动提示是否对该设备进行病毒扫描。移动设备使用中，打开光华反病毒的监视功能，便可有效的对移动存储设备进行病毒检测，一旦发现可疑文件或病毒，软件将弹出警示框。为了安全起见，使用移动存储器前应先使用《光华反病毒》进行病毒查杀，确认安全无病毒后再开始使用。

光华反病毒专家提示:在学校里的公用机房、网吧等特定公共场所使用U盘(闪存)等移动设备的用户要特别谨慎小心，以防感染木马，造成自己的信息失密并被窃取。

五、无线设备传播

目前，这种传播途径随着手机功能性的开放和增值服务的拓展，已经成为有必要加以防范的一种病毒传播途径。随着智能手机的普及，通过彩信、上网浏览与下载到手机中的程序越来越多，不可避免的会对手机安全产生隐患，手机病毒会成为新一轮电脑病毒危害的“源头”。手机、特别是智能手机和3G网络发展的同时，手机病毒的传播速度和危害程度也与日俱增。通过无线传播的趋势很有可能将会发展成为第二大病毒传播媒介，并很有可能与网络传播造成同等的危害。

解决方案:北京日月光华软件公司从2024年3月即开始立项开发手机杀毒软件，并于2024年5月推出了第一个测试版本，2024年9月开始提供网上试用下载版本(下载地址为:http:///admin/call.asp)，成为全球首家推出手机杀毒产品的领军企业。

《光华反病毒软件 手机版》支持手机型号齐全，占用空间仅43K，查杀病毒全面，可以查杀手机病毒、蠕虫、木马等有害程序100余种，其中不仅包括Cabir全系列，还有著名的Lasco系列、Skulls系列病毒。该软件目前支持S60、S80、UIQ、Windows Mobile四种系统。

光华反病毒专家提示:使用手机上网功能时，应尽量以浏览信息为主，尽可能的减少从网上下载信息和文件，即便是有这方面的需求，也最好从一些正规网站上下载。收到带有病毒的短信或邮件立即删除，键盘被锁死应立即取下电池，然后重新开机进行删除。可先用光华反病毒软件手机版查杀病毒，如仍旧不能恢复正常的，请及时将手机送厂维修，避免病毒二次传播。

病毒的种类繁多，特性不一，只要掌握了其流通传播方式，便不难进行监控和查杀。使用功能全面的病毒防护工具将能有效的帮助您避免病毒的侵入和破坏。作为国内唯一一家通过微软全球认证的反病毒软件——《光华反病毒》软件——具备了查、杀、防三项合一的能力，正为我们创造新一代网络安全的解决方案!

**第五篇：电脑病毒有哪些种类**

电脑病毒有哪些种类你知道吗?马上断开连接，这样能将自己的损失降低的同时，也避免了病毒向更多的在线电脑传播。请先不要马上重新启动系统或是关机，一起来看看电脑病毒有哪些种类，欢迎查阅!

什么是病毒?

计算机病毒，根据《中华人民共和国计算机信息系统安全保护条例》，病毒的明确定义是;指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

病毒必须满足两个条件

1、它必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。

2、它必须能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机也可以感染网络服务器。

此外，病毒往往还具有很强的感染性，一定的潜伏性，特定的触发性和很大的破坏性等，由于计算机所具有的这些特点与生物学上的病毒有相似之处，因些人们才将这种恶意程序代码称之为;计算机病毒。一些病毒被设计为通过损坏程序、删除文件或重新格式化硬盘来损坏计算机。有些病毒不损坏计算机，而只是复制自身，并通过显示文本、视频和音频消息表明它们的存在。即使是这些良性病毒也会给计算机用户带来问题。通常它们会占据合法程序使用的计算机内存。结果，会引起操作异常，甚至导致系统崩溃。另外，许多病毒包含大量错误，这些错误可能导致系统崩溃和数据丢失。令人欣慰的是，在没有人员操作的情况下，一般的病毒不会自我传播，必须通过某个人共享文件或者发送电子邮件等方式才能将它一起移动。典型的病毒有黑色星期五病毒、比特币勒索病毒等等。

电脑病毒彻底清理的方法

手动清理

1如果我们感觉我们电脑受到了电脑病毒的威胁，我们可以通过手机杀毒的方式，对我们的电脑进行相关的手机清理病毒，首先，点击开始菜单栏，进入到运行的界面。在电脑的运行中输入相关的命令，我们可以按回车运行该命令，进入到相关的页面中，在当前页面中我们可以根据我们需求输入相关的命令。然后跳转到相关的打开功能界面中，在当前界面中我们可以找到windows的相关文件夹中。通过进入到功能的界面，设置相关的内容即可。

安全软件杀毒

当我们的电脑出现不可避免的电脑病毒后，采用手动无法根除后，可以适当的选择电脑的安全软件去解决相关的问题，首先，进入到腾讯电脑管家的杀毒页面。

进入到杀毒界面后，我们可以选择当前页面的闪电查杀功能，腾讯电脑管家会根据我们选择的杀毒方式查杀我们电脑中的病毒，如果最后腾讯电脑管家并没有检查出我们电脑中存在病毒的话，会根据我们的电脑安全给出提示，确定电脑完全安全后，我们点击当前页面的完成提示按钮即可。

电脑病毒有哪些种类

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找