**计算机感染病毒防范和处置措施**

在日常工作和生活中，计算机感染病毒是一种比较普遍的现象，但是很多人在计算机感染病毒后，不知道如何处置，甚至自己的计算机带病毒运行而毫不知情，直至在病毒症状爆发造成损失后才追悔莫及；有的人谈“毒”色变，唯恐电脑病毒破坏自己的计算机，删除文件，窃取信息，所以干脆不用了之。其实，对待电脑病毒既不用避而远之，也不要闻之色变，而应当用科学的方法来防范攻击、发现感染、消除隐患、拯救系统。

**一、乘虚而入的计算机病毒**

很多情况下，都是计算机感染病毒造成破坏了，人们才会自问一句“这些病毒是怎么进来的？”常言道，“苍蝇不叮无缝的蛋”，计算机病毒同样如此，但凡感染计算机病毒，无非是两种情况，一是操作系统或者应用软件存在漏洞而没有及时更新，造成病毒由网络感染入侵。二是计算机用户安全意识不强，访问陷阱网站、运行恶意程序，结果开门揖盗，把病毒请了进来。以下介绍7条病毒防范措施。

1.经常更新操作系统补丁和应用软件的版本。操作系统厂商会定期推出升级补丁，这些升级补丁除了提升操作系统性能外，很重要的任务是堵塞可能被恶意利用的操作系统漏洞。同理，把软件升级到最新版本，也会让很多病毒望而却步，因为新版本软件会优化内部代码，使病毒暂无可乘之机。

2.安装防火墙和杀毒软件。防火墙与杀毒软件就像大门的警卫，会仔细甄别出入系统的文件程序，发现异常及时警告并处置。比如你在访问恶意网站或运行可疑程序时，杀毒软件都会进行警告；当你下载或收到可疑文件时，杀毒软件也会先行扫描；当你的操作系统需要更新或应用程序需要升级时，杀毒软件也会提示。

3.经常备份重要的数据。越是重要的文件，越要多做备份，而且备份之间相距越远越好。就像我们在编辑文档时经常点击保存一样，一旦遇到突发情况，起码可以将损失降到最低，不至于全文皆丢。作为事后补救的措施，及时备份是一种很好的习惯和方法。

4.隐秘文件要加密。一定要树立“凡是上网即意味公开”的意识，坚守“涉密不上网，上网不涉密”的原则，没经过加密的文件在硬盘上存储或网络上传输是明文状态，窃取、截获、还原非常容易；不要对网络硬盘过于信任，凡在掌控范围以外的地方就是公之于众的地方；谨慎开启文字编辑软件的云盘备份功能，不然你编辑一份，就在云盘备份一份。最简单的加密方式就是用压缩软件对隐秘文件进行加密压缩，目前主流压缩软件采用椭圆曲线加密算法，加密强度较高，能够很好的保障文件隐秘安全。

5.使用复杂的密码。密码越复杂，被破解的几率越小，因此对自己的操作系统、邮箱、社交账号要设置长度12位以上字符、数字、特殊符号混杂的密码，且不要用相同密码、生日密码等易被猜解的密码，更不要将银行、社保等现实生活密码与网络密码混为一谈。

6.使用Ghost系统或系统还原。Ghost系统也称影子系统，就是在你刚刚安装系统完毕后，将纯净的系统制作一张系统光盘，一旦系统受损，可用影子系统快速恢复。系统还原就是操作系统会定期将系统的状态进行备份，备份的状态点被称为系统还原点，系统受损后直接点击还原点就能快速恢复系统上次的状态。

7.上网要提高安全意识这根弦。作为现实世界的镜像，互联网也充斥着现实中的阴暗角落。不要接收来历不明的文件，不要打开可疑的链接，不要暴露真实的身份信息，不要访问提示“危险”的网站，要相信杀毒软件给出的警示信息，切莫一意孤行造成损害。

**二、感染病毒的计算机表现**

由于不具备专业防病毒知识，很多人在计算机感染病毒后依然带“病”工作，结果造成严重损坏。因此，及早发现感染迹象，会降低病毒带来的损失，以下介绍6条计算机感染病毒后的症状。

1.计算机运行速度比正常计算机慢很多。由于病毒在计算机中“兴风作浪”，会占用计算机大量的计算资源、内存空间和网络带宽，让计算机不堪重负，越来越慢。比如说，原本打开一个应用程序，计算机反应迅速，而现在没干什么工作，想再运行程序，仅见硬盘狂转，风扇呼响，但程序却迟迟不见响应，反而鼠标迟钝，系统死机，这时就要考虑系统是否感染病毒了。

2.浏览器重定向无处不在。有时在打开浏览器页面时，浏览器会自己跳到一个网站上，这个网站你并无收藏或者设为主页，而且每打开一个新页面，见到的总是它，把这个网址从浏览器首页设置中移除，结果它自己又回来了，这时就要考虑计算机是否感染病毒了。

3.弹出窗口如雨后春笋，层出不穷。这种现象可以确定感染病毒了，这是一种恶作剧式损耗资源的病毒，点击一个任意程序就像打开一个大礼包，不断弹出窗口。有时浏览器会不断弹出加载了恶意广告的窗口，也是典型的感染迹象。

4.计算机自己开启。这可不是人工智能，是病毒程序在后台作祟。有些计算机病毒出于自身感染扩散、榨取计算资源的目的，会在特定的时间点或时间间隔启动计算机，进行恶意活动。如果你下班前明明已经关闭计算机，翌日上班确发现计算机处于开机状态，就要考虑是否感染计算机病毒了。

5.计算机病毒还会占用网络带宽。一些计算机病毒会将你的计算机作为“僵尸计算机”，意思是像僵尸一样没有思维并受到控制。这些“僵尸计算机”聚集在一起形成“僵尸网络”，它们会收到幕后不法分子的控制指令统一向某个单位的网络出口发起网络连接，就像塞车一样把受害单位的网络出口牢牢堵住和占用起来，扰乱正常网络通信，这就是DDOS网络洪泛攻击。还有一些计算机病毒会将你的计算机作为“矿机”，近些年虚拟货币越来越稀缺，价格也随之水涨船高，不法分子专门制作了“挖矿”病毒四处传播，由于虚拟货币依赖特定的数学算法计算产生，所谓的“挖矿”就是不断计算，试图生成虚拟货币，此类病毒会压榨计算资源和网络带宽资源，给正常使用带来不便。

6.计算机病毒对文件系统的破坏力最大，如果你的桌面图标突然不见了、硬盘盘符消失了、硬盘容量突然减少了，或者打开硬盘盘符显示的文件目录混乱、出现很多来历不明的文件，甚至都打不开硬盘了，这些就是破坏硬盘数据病毒的“杰作”；如果你发现在打开文件时莫名弹出一个窗口让你填写密码，仔细一看还附带转帐支付方式，这就是勒索病毒在搞鬼；还有你发现所有文件的后缀名都被统一改成了特定的文件后缀名，这就是文件感染病毒在捣乱，林林总总花样繁多，让人颇为无奈。

**三、拿什么拯救你，我的计算机**

中毒不可怕，就怕安全意识差，如果抱着无所谓的态度，最后只能是追悔莫及。这里向大家介绍一下计算机感染病毒后的处置措施：

1.发现计算机感染病毒迹象后，首先断开网络连接。断开网络连接，就斩断了病毒与外界联系的渠道，无论其试图网传你的文件还是感染其他计算机，都能被有效阻止。

2.打开杀毒软件对全盘进行扫描查杀。对于普通病毒，一般的扫描杀毒即可恢复系统状态，如果病毒比较棘手，导致系统死机、运行缓慢、甚至连杀毒软件都不能工作，这时需要重启操作系统。在计算机通电后，启动操作系统前，有的杀毒软件会提示是否进行扫描杀毒，这种杀毒方式称为BootScan。由于病毒依赖于操作系统才能运行，在系统未启动前，病毒没有被激活，只是普通的硬盘文件，可用该方式轻易清除病毒。如果你的计算机没有安装杀毒软件或者不具备BootScan功能，可将硬盘拆下后挂载到另外一台计算机上作为普通硬盘进行查杀操作。

3.清除完病毒后，导出重要的文件进行备份。把扫描过的硬盘挂载为普通硬盘，将其中的重要文件资料进行备份。备份时仅备份文档、照片等非程序数据文件，程序文件不要备份。

4.重新安装操作系统，彻底清理系统分区。一般而言，病毒都会驻留隐藏在系统分区，重新安装操作系统是最彻底的清除办法。重装完系统后要及时安装杀毒软件，更新系统补丁。然后将所有的帐号密码进行更换，包括邮箱帐号密码、社交帐号、网盘帐号等，并对所有曾经连接过感染主机的U盘、移动硬盘进行查杀扫描，彻底清除遗留病毒文件。

如果上述步骤执行过后，计算机系统仍然存在顽固病毒感染的情况，就得让专业人员来进行针对性清理查杀。

（来自国家保密局网站）