常见的电脑杀毒认识误区

我们对任何事物的认识总是有限的，再加上获取相关信息的渠道不通畅，造成我们对某个事物的认识出现了主观、偏颇甚至是错误的判断。在电脑安全领域同样如此。你要是不经常关注这方面的新信息，往往会想当然地做出一些在专业人士眼中的“傻”事。

误区1 病毒不感染只读文件

某些人认为把文件属性设置为只读，让文件变成“不可写”状态就能有效地抵御病毒的侵害。如果有这么简单的话，那杀毒软件厂商也不用费尽心思更新病毒库了，只要把系统所有软件都改成只读就可以了，这样不就可以“百毒不侵”了？

你以为你是电脑的最高控制者，其实不然。你可以轻易修改文件的属性，病毒同样可以，实现起来非常简单。而且很多系统重要文件是无法改为只读属性的。

误区2 病毒不感染数据文件

通常是这样。因为病毒是一段程序，而数据文件，像一般的文本文件、图片文件等是不包含程序代码，也就不会感染病毒。不过有些病毒是专门破坏系统里的各种文件，所以备份重要的数据文件还是非常必要的。

但例外的是，若数据文件包含了可执行代码，那么它就能够被病毒感染了。这方面最好的一个例子就是我们常用的 Word 文件（后缀名为.doc 和.dot）。虽然 Word 文件是数据文件，但 Word 中可以包含一段程序，因此它们能够容纳病毒，并且因为是可执行文件，所以很容易受病毒感染。

误区3 装上能实时杀毒的防火墙，就万事大吉了

这是很多用户所持的一种错误观念，以为只要买了杀毒软件，特别是只要安装了有实时杀毒功能的病毒防火墙，就能挡住所有病毒——这是大错而特错的。

从 1999 年 4 月 26 日 CIH 病毒大发作的情况来看，安装了病毒防火墙，并且在之前至少升级过一次的用户，都没有受到该病毒的攻击。而那些虽然安装并且运行病毒防火墙，却长时间没有升级过的用户，有很大一部分人不幸成为 CIH 病毒的牺牲品。所以请把杀毒软件的自动更新功能打开，并且每次使用电脑时，都保持网络连通，以便于杀毒软件能够随时进行更新。

误区4 使用杀毒软件就可以免受病毒侵扰

现在的病毒制造者越来越厉害，使得病毒的变种和类型越来越多，目前市场上的杀毒软件，都只能在病毒泛滥后才“一展身手”，并不能保证系统万无一失，免受病毒侵害。所以如果你不小心感染了一种新病毒，已有的杀毒软件很有可能“束手无策”。在杀毒软件厂商找到解决办法更新病毒库之前，病毒早已对系统造成破坏，造成工作延误、电脑“罢工”或其他更为严重的后果。所以杀毒软件并非万能。

误区5 病毒会感染写保护磁盘

由于病毒可以感染只读文件，不少人“顺理成章”地认为病毒也能感染在带有写保护的软盘或储存卡上的文件。事实上，软盘或储存卡的写保护功能是通过硬件来实现的，必须靠手工进行打开或关闭开关的操作，而非通过软件的形式修改某个属性实现的。所以当写保护开关打开时，驱动设备只能读取资料，而不能写入新资料或更改原有资料，所以这时病毒是无能为力的。

误区6 备份数据时，数据中含有病毒，那么备份是无用的

这个问题要分开来看。如果是备份在移动硬盘或优盘上，备份中含有引导型病毒。这种情况下，只要不用这个移动硬盘或优盘启动电脑，它将和无毒备份一样安全；如果备份中的数据文件中没有病毒，可执行文件含有病毒，那么可执行文件就等于白备份了，但备份中的数据文件还是可用的。

误区7 正版软件不可能带病毒，可安全使用

电脑用户常被告知，“为了防范病毒的侵害，不要使用来历不明的软件”。这话不错，所谓“来历不明的软件”确实是电脑病毒传播主要途径之一。那么使用有“来历”的软件是否就可以高枕无忧呢？非也！实际上媒体已经多次报道过“正版软件”、“商品软件”在出厂前没有严格进行杀毒，以至于带有病毒的问题。所以，使用有“来历”软件时也不可掉以轻心，甚至新购买的电脑包括原装电脑，在使用前都要进行病毒检测。如确实由于原版软件带有病毒而造成重大损失，应寻求法律保护。

误区8 不用优盘，不会染毒

这是最典型的“因噎废食”的例子。按照这个逻辑，不用电脑不就更不会感染病毒吗？的确，优盘是传播病毒的主要途径之一。有时候要从同事的电脑上拷个文件，但文件太大，从网上传不方便，索性拿同事的优盘拷。但同事的优盘或者电脑一旦有病毒，很有可能就会感染你的电脑。但实际上，现在感染病毒的途径太多了，就连打开一个网页，都会感染病毒，病毒有时候真的是无处不在，只要你一不小心，就会“中招”。所以不能因为害怕感染病毒而拒绝优盘，而是要做好完备的防范措施，及时更新杀毒软件。使用他人优盘或移动硬盘之前，最好先用杀毒软件扫描一下。

误区9 文件损坏多为病毒所致

文件的损坏有多种原因，电源电压波动、掉电、非正常重启、关机、硬件错误、其他软件造成的死机、灰尘、烟灰、茶水，甚至一个喷嚏都可能造成硬件故障，导致数据丢失。以上这些对文件造成的损坏，会比病毒造成的损失更常见、更严重。

误区10 杀毒软件能清除所有已知病毒

目前的杀毒软件确实可以查杀所有已知病毒，但并不表示被病毒感染的文件还能恢复原样。病毒的感染方式很多，有些病毒会强行覆盖执行程序的某一部分，将自身代码嵌入其中，以达到不改变被感染文件长度的目的，被这样的病毒覆盖掉的代码是无法复原的，也就是说，这个程序被病毒篡改了，无法实现原来的功能。因此要杀掉这种病毒只能把原文件也一同删除。

（史瑀）

电脑蓝屏后你该做的几件事

1.重启电脑

有时只是某个程序或驱动程序一时犯错，重启后它们会“改过自新”。

2.检查新硬件

首先，应该检查新插上去的硬件是否插牢，这个被许多人忽视的问题往往会引发许多莫名其妙的故障。如果确认没有问题，将其拔下，然后换个插槽再试试，并安装最新的驱动程序。同时还应对照微软网站的硬件兼容列表检查一下硬件是否与操作系统兼容。如果你的硬件没有在表中，那么就得到硬件厂商网站进行查询，或拨打他们的咨询电话。

3.使用新驱动和新服务

如果刚安装完某个硬件的新驱动，或安装了某个软件，而它又在系统服务中添加了相应项目（比如：杀毒软件、CPU 降温软件、防火墙软件等），在重启或使用中出现了蓝屏故障，请到安全模式卸载或禁用它们。

4.检查病毒

比如冲击波和震荡波等病毒有时会导致 Windows 蓝屏死机，因此查杀病毒必不可少。此外，一些木马间谍软件也会引发蓝屏，所以最好再用相关工具进行扫描检查。

5.检查 BIOS 和硬件兼容性

对于新装的电脑经常出现蓝屏问题，应该检查并升级 BIOS 到最新版本，同时关闭其中的内存相关项，比如：缓存和映射。另外，还应该对照微软网站的硬件兼容列表检查自己的硬件。还有就是，如果主板 BIOS 无法支持大容量硬盘也会导致蓝屏，需要对其进行升级。

6.检查系统日志

在“开始→运行”中输入“EventVwr.msc”，回车后打开“事件查看器”，注意检查其中的“系统日志”和“应用程序日志”中标明“错误”的项。

7.查询停机代码

把蓝屏中密密麻麻的英文记下来，接着到其他电脑中上网，进入微软帮助与支持网站：http://support.microsoft.com，在左上角的“搜索（知识库）”中输入停机代码，比如：0x0000001E，接着在下面首先选择“中文知识库”，如果搜索结果没有适合信息，可以选择“英文知识库”再搜索一遍。一般情况下，会在这里找到有用的解决案例。另外，在百度、Google 等搜索引擎中使用蓝屏的停机码或后面的说明文字作为关键词搜索，往往也会有意外收获。

8.最后一次正确配置

一般情况下，蓝屏都出现于更新了硬件驱动或新加硬件并安装其驱动后，这时 Windows 2000/XP 提供的“最后一次正确配置”就是解决蓝屏的快捷方式。重启系统，在出现启动菜单时按下 F8 键就会出现高级启动选项菜单，接着选择“最后一次正确配置”。

9.安装最新的系统补丁和 Service Pack

有些蓝屏故障是 Windows 本身存在缺陷造成的，因此可通过安装最新的系统补丁和 Service Pack 来解决。

世界头号黑客的十大电脑安全建议

世界头号黑客凯文·米特尼克，1964 年生于美国加州的洛杉矶。13 岁时他对电脑着了迷，掌握了丰富的计算机知识和高超的操作技能，但却因为用学校的计算机闯入了其他学校的网络而被勒令离校。从此他便开始了不断入侵大公司和国家机密机构网络的黑客生涯。在获刑 4 年刑满释放后，他改邪归正，目前投身于计算机安全咨询和写作中。下面是他给普通人的十条电脑安全建议。

1.经常备份重要资料。谨记你的系统永远不可能无懈可击，灾难性的数据损失会随时发生在你身上——只需一条“虫子”或一只“木马”就已足够。

2.使用很难猜的密码。不要随意使用几个与你有关的数字，如生日、电话号码、汽车牌号等等。在任何情况下，都要及时修改默认密码。

3.电脑应安装防毒软件，并让它每天更新升级。

4.电脑的操作系统要时时更新，时刻留意软件制造商发布的各种安全补丁，及时下载安装。

5.上网浏览时，一些网页上有黑客“诱饵”，对此要保持清醒，拒绝点击，同时将电子邮件客户端的自动脚本功能关闭。

6.电脑在发送敏感邮件时应使用加密软件。此外，也可用加密软件保护你的硬盘上的数据。

7.电脑上应安装一个或几个反间谍程序，并且要经常运行检查。

8.电脑应装有个人防火墙并进行正确设置，以阻止其他电脑、网络与你的电脑建立连接。应指定哪几个程序可以自动连接到网络。

9. 关闭所有你不使用的系统服务，特别是那些可以让别人远程控制你电脑的服务，如 RemoteDesktop、RealVNC 和 Net-BIOS 等。

10.使用无线上网也应注意安全。应对你自己的无线网络设置至少 20 个字符的密码。也不要加入任何没有经过加密设定的无线网络。要想在一个充满敌意的因特网世界里保护自己，的确是一件不容易的事。你要时刻想到，在地球另一端的某个角落里，有人正在嗅探你的系统漏洞，并利用这些漏洞窃取你最敏感的秘密。