计算机软件水平,计算机软件水平考试,软件水平,软件水平考试,计算机水平考试,计算机软件考试,全国软件水平考试,邮件
 电子邮件是我们日常联络使用最多的工具之一，因此邮件成为病毒传播的一种主要方式，危害甚大。但是这种危害，并非不可防范，只要我们了解一些常识，掌握必要的知识，带毒邮件就再无“ 用武之地 ”了！ 一、安装杀毒软件 要对付病毒，单纯的靠手工防范是不现实的，也是不科学的。因此，首先必须安装一款杀毒软件。现在基本上所有的主流杀毒软件都提供了邮件监视功能，在接收、发送邮件的时候，会自动检查监视邮件的内容是否包含病毒，对于带病毒的邮件会按照设置自动进行处理，从而避免病毒的运行和传播。 二、做好升级工作 升级包括两部分，一是杀毒软件的升级，二是系统的升级。对于杀毒软件的升级，相信其重要性不言而喻，只有采用最新的病毒库才能最大限度的防范病毒，尤其是应对新病毒、各种病毒的变种等。对于系统的升级，同样也很重要。因为很多病毒就是因为系统存在漏洞才发布的，如果我们能够提前打好补丁，避免系统漏洞的存在，这样病毒自然无从发作了。 三、辨别邮件主题 由于病毒邮件一般都是自动发送或批量发送，因此其主题都会表现出一定的特征。例如“ 老同学，好久不见了 ”、“ 请你检查一下 ”，主题关键字表现出很高的迷惑性，诱惑用户查看邮件。 四、检查邮件附件 如果邮件包含附件，并且邮件中的正文还显示“ 附件中是我的照片，快看看啊！ ”之类的话，那么这时你一定得小心，不能听信其所说，

看到附件的图标是图片文件、文本文件就以为是安全的。要知道这类文件的全名常常就是1.jpg.exe、1.txt.exe，因此最好先进入文件夹选项窗口，设置显示扩展名，确认没有exe后缀再打开。另外对于伪装成图片文件的病毒，我们可以先预览一下，如果能预览到其图片内容，那么再打开中招的可能就会下降许多。 五、禁用地址簿 为了联系的方便，很多人习惯把联系人添加到地址簿，这样发送邮件时直接选择就可以了。但是要知道，如果自己被病毒感染，那么发作的病毒就会自动给地址簿中所有的联系人发送一封带病毒的邮件，这样循环往复造成的危害极大。因此我们可以把联系人信息放在一个文件文件中，撰写邮件的时候直接从文本文件中复制过来即可。虽然这样操作会有一点不方便，但是对于一些商业用户或者使用电子邮件比较频率的企业内部来说，还是非常有必要的。 六、禁用信纸模板 很多用户从漂亮的角度，会选择一些信纸模板，但是漂亮是有代价的。因为这些模板为实现某些效果，常常调用脚本文件，这些脚本文件非常容易感染JS/VBS等类型的病毒，如果用户使用感染了病毒的信纸发送邮件就带有病毒了。 七、正确处理垃圾邮件 邮件病毒邮件都是垃圾邮件，用户发现后常常选择直接将其删除。但是直接删除后，邮件并没有消失，而是被保存到废件箱或垃圾邮件中，对此我们民须将它们从废件箱中清空，然后再右击废件箱，选择清空废件箱操作，这样才能彻底将其中删除。 八、启用自动过滤 不管是基于web接收，还是使用客户端Foxmail之类的收发工具，一般都提供了自动过滤功能。对此，我们需要将其启用，这样不仅可以防范垃圾邮件，还可以过滤掉一些带病毒的邮件。另外也需要将一些来自陌生地

址的发信人添加到黑名单中，避免相同地址的邮件再次出现。 九、使用纯文本格式查看 由于邮件一般有HTML和TXT两种方式查看，使用HTML方式查看邮件虽然能够看到邮件的原貌，但是由于HTML文件可以加载JS代码，容易产生破坏，相比之下TXT文件则没有这种问题。我们可以将邮件的默认查看设为TXT格式，待大概了解邮件正文内容，发现没有异常后再切换到HTML方式浏览。 十、认真学习病毒防范知识 由于病毒的信息变化很快，如果我们不能够加强这方面知识的吸取，那么很容易被病毒迷惑住。因此，要尽可能的了解各种病毒信息，掌握其特征，做到知已知彼，方可做到百战不殆。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com