

Windows安全预防病毒的八个忠告 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/493/2021_2022_Windows_E5_AE_89_c67_493531.htm 纵观全球病毒的发展，不难发现蠕虫

病毒着实让杀毒市场火了一把。蠕虫病毒信手拈来，如库尔尼科娃、Sircam、红色代码、蓝色代码、本拉登等等，一个比一个厉害，一个比一个恶毒，令人防不胜防，只要你上网，不经意之间就有可能染上病毒而浑然不知。现在人们还没有养成定期进行系统升级、维护的习惯，这也是最近受病毒侵害感染率高的原因之一。只要培养良好的预防病毒意识，并充分发挥杀毒软件的防护能力，完全可以将大部分病毒拒之门外。

1、安装防毒软件：鉴于现今病毒无孔不入，安装一套防毒软件很有必要。首次安装时，一定要对计算机做一次彻底的病毒扫描，尽管麻烦一点，但可以确保系统尚未受过病毒感染。另外建议你每周至少更新一次病毒定义码或病毒引擎（引擎的更新速度比病毒定义码要慢得多），因为最新的防病毒软件才是最有效的。定期扫描计算机也是一个良好的习惯。

2、注意软盘、光盘媒介：在使用软盘、光盘或活动硬盘其他媒介之前，一定要对之进行扫描，不怕一万，就怕万一。

3、下载注意点：下载一定要从比较可*的站点进行，对于互联网上的文档与电子邮件，下载后也须不厌其烦做病毒扫描。

4、用常识进行判断：来历不明的邮件决不要打开，遇到形迹可疑或不是预期中的朋友来信中的附件，决不要轻易运行，除非你已经知道附件的内容。

5、禁用Windows Scripting Host.许多病毒，特别是蠕虫病毒正是钻了这项“空子”，使得用户无需点击附件，就可自动打开一

个被感染的附件。 6、使用基于客户端的防火墙或过滤措施，以增强计算机对黑客和恶意代码的攻击的免疫力。或者在一些安全网站中，可对自己的计算机做病毒扫描，察看它是否存在安全漏洞与病毒。如果你经常在线，这一点很有必要，因为如果你的系统没有加设有效防护，你的个人资料很有可能会被他人窃取。 7、警惕欺骗性或文告性的病毒。这类病毒利用了人性的弱点，以子虚乌有的说辞来打动你，记住，天下没有免费的午餐，一旦发现，尽快删除。更有病毒伪装成杀毒软件骗人。 8、使用其它形式的文档，比如说办公处理换用。wps或。pdf文档以防止宏病毒。当然，这不是彻底避开病毒的万全之策，但不失为一个避免病毒缠绕的好方法。 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