

实用招数轻松防治U盘病毒 PDF转换可能丢失图片或格式，  
建议阅读原文

[https://www.100test.com/kao\\_ti2020/460/2021\\_2022\\_\\_E5\\_AE\\_9E\\_E7\\_94\\_A8\\_E6\\_8B\\_9B\\_E6\\_c100\\_460843.htm](https://www.100test.com/kao_ti2020/460/2021_2022__E5_AE_9E_E7_94_A8_E6_8B_9B_E6_c100_460843.htm) U盘对病毒的传播要借助autorun.inf文件的帮助，病毒首先把自身复制到u盘，然后创建一个autorun.inf，在你双击u盘时，会根据autorun.inf中的设置去运行u盘中的病毒，我们只要可以阻止autorun.inf文件的创建，那么U盘上就算有病毒也只能躺着睡大觉了，大家可能也想到这个，但是不管给autorun.inf设置了什么属性，病毒都会更改它，我提到的方法就是，在根目录下，删除autorun.inf文件，然后，根目下建立一个文件夹，名字就叫autorun.inf，这样一来，因为在同一目录下，同名的文件和文件夹不能共存的原理，病毒就无能为力，创建不了autorun.inf文件了，以后会不会出新病毒，自动去删文件夹，然后再建立文件就不知道了，但至少现阶段，这种方法是非常有效的。现状分析：事实表明，目前已经有新的病毒能够有意识地检测autorun.inf的存在，对于能直接删除的则删之，对于“无法删除”的则用重命名的方式毁之；还有一种很早就出现的以文件名诱骗用户点击的病毒（如：重要文件.exe，小说.exe）。对于以上这两种传播方式的病毒，仅仅建立autorun.inf文件夹是抵御不了的。应对策略：1、在插入U盘时按住键盘shift键直到系统提示“设备可以使用”，然后打开优盘时不要双击打开，也不要右键菜单的打开选项打开，而要使用资源治理器（开始-所有程序-附件-windows资源治理器）将其打开，或者使用快捷键winkey E打开资源治理器后，一定通过左侧栏的树形目录打开可移动设备！（要养

成这样的良好习惯) 2、假如盘内有来路不明的文件，尤其是文件名比较诱惑人的文件，必须多加小心；需要非凡提示的是，不要看到图标是文件夹就理所当然的是文件夹，不要看到图标是记事本就理所当然的是记事本，伪装图标是病毒惯用伎俩。 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](http://www.100test.com)