保护好你的Office工具 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/133/2021_2022__E4_BF_9D_E6_8A_A4_E5_A5_BD_E4_c97_133445.htm 计算机等级考试训练软件《百宝箱》微软office是世界上使用最广泛的办公和生产套件。因为绝大多数的人都依靠微软word、excel和powerpoint来完成日常的工作，微软office和它的组件成为了攻击者的目标，希望能从中找到漏洞。 在2006年 3月，微软发布了两条新的安全公报。一个被定为重要级，另一个为危机级。危机级安全公报ms06-012公布了在office中的一个漏洞，可能让攻击者完全控制被攻击系统。在2月份，一个与power point有关的重要漏洞(ms06-010)被公布。用户必须像保护自己的操作系统和浏览器一样将office加以保护。一台电脑整个安全性是与它的最薄弱点相当的，而office有可能就是那一点。下面的一些提示可以帮助你死锁office:确保宏保护开启:宏一直都有一定的危险性，如果来自未知或不可信的资源的宏被执行。宏保护的开启可以禁用宏的运行或是在运行前询问用户。这对于每个产品都是基本的，通常在选项中设置。给你的office升级和安装补丁:到现在为止，用户只有在微软office的官方网站查找下载新的补丁。建议使用自动升级或是用现成的软件通过windows升级网站扫描自己的电脑，以确定和安装操作系统、office和其它微软应用程序的补丁。不管你怎么作。请经常注意新的补丁并安装它们。遵行标准的电脑安全防范法:不管是什么样的攻击或入侵，常识性的电脑安全基础总是有用的。确保你的系统在防火墙的保护下，经常升级你的反病毒软件。删除隐藏的元数据:这么作更加是为了

保密而不是安全，但是很多用户都不知道隐藏在office文本后台的硬盘信息，特别是word。甚至当你把一些敏感信息删除了，比如存有银行帐号或社会保险码的文档，但是这些信息却仍然保存在隐藏的元数据中。在word的选项中，你可以把快速存档禁用。或者设置保密选项中选择“ 保存时删除文件属性中的个人信息 ”。也有一些工具可以删除隐藏数据，比如微软出品的免费软件remove hidden data add-in。 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