可以保障Win7安全的七方法Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_8F_AF_E4_BB_A5_E4_BF_9D_E9_c100_644006.htm 软件制造商为了提高软件的可用性经常会以牺牲安全性为代价，微软也不例外。 与Windows Vista相比，微软的下一代操作系统Windows 7具有更强的安全性。如今对用户产生威胁的因素通常是由于恶意软件的攻击和用户缺乏保护意识造成的。 下面所列举的七种方法通过简单的安装设置就可以完成： 1、Install anti-spam and anti-malware software(安装反病毒木马软件) 对用户而言，威胁通常来自于木马、恶意软件、假冒的病毒扫描程序。不管你是计算机专家还是菜鸟，装备一款合适的杀毒软件是十分有必要的，同时记住保持杀毒软件的更新，防范新的恶意程序攻击。 本周，微软官方向用户推荐了十款Windows 7适用杀毒软件，它们是：AVG、诺顿、卡巴斯基、McAfee、Trend Micro、Panda Security、F-Secure、Webroot、BullGuard、G-Data 2、Enable the SmartScreen Filter in Internet Explorer 8(开启IE8智能过滤功能) 浏览器正逐渐成为最容易被攻击的目标，Windows 7的浏览器IE8安全菜单中有项智能截屏过滤功能，用户开启此项功能后，可以与微软的网站数据库链接起来，对比审核所访问的网站是否安全，大大降低了误入不明网站中毒的可能性。 3、Enable BitLocker(磁盘加密位元锁) Windows 7中的磁盘加密位元锁可以用来加密任何硬盘上的信息，包括启动、系统甚至移动媒体，鼠标右键就可以在选项中加密Windows资源管理器中的数据。用户可以在设置菜单中选择希望加锁的文件，被加密的文件可以被设置

为只读，且不能被重新加密。 在保存好Bitlocker信息后关闭电脑，BitLocker的恢复信息存储在计算机的属性文件中，大多数情况下自动备份用户的密码恢复到Active Directory。所以要确保可以访问这些属性，防止丢失密码后无法恢复文件。 4、Raise the UAC slider bar(提升安全级别) Windows 7的用户帐户控制得到较大的改进，在区别合法和非法程序时表现得十分精确、迅速。根据用户的登录方式(管理员或普通用户)默认UAC安全级别设置，可以选择不同敏感度的防御级别。 Windows 7中设计了一个简单的用户帐户控制滚动条，方便管理员或标准用户设置它们的UAC安全级别。 建议将UAC安全级别设置为“ 始终通知 ”，请放心Windows 7中遇到的安全通知要比Vista少很多。 虽然UAC功能提供了一个必要的防御机制，但是为了系统的稳定性，请谨慎使用管理员帐户。 5、Patch everything(及时升级) 在Windows 7的默认设置中，Windows升级服务将自动下载并安装重要的Windows系统和应用程序的升级包。 有一项研究表明，微软的软件是世界上补丁最多的产品。但是系统并没有提醒你，及时更新其他的非系统软件，比如浏览器、媒体播放器等。黑客们现在都喜欢从这些方面对电脑进行攻击。 上周发生的针对IE浏览器发动的零日攻击就是一个典型的例子。尽量保证系统中运行的程序都已升级到新的版本，将漏洞存在的可能降到最低。 6、Take an inventory(清理垃圾文件) 用户使用一段时间后，会觉得电脑速度变得慢了，这通常是由于系统中产生了大量的垃圾文件。清理掉无用的垃圾文件，相当于给自己的电脑减肥。 清理的方法有很多，在Windows 7中有一个工具：Microsofts Autoruns。Autorun中记录了每一个在系统中运行

过的程序和服务，你可以通过点击鼠标将无用的文件删除。在这里需要注意的是，如果遇到你不认识的程序，先做一个调查再进行操作，防止不小心删除了重要的数据。 7、Back up your data(备份数据) 道高一尺，魔高一丈。有的时候真的是防不胜防，即使做了很多努力，当病毒来临时防御措施仍可能变的不堪一击。及时备份重要数据才是王道，这样就算遇到了极具杀伤性的病毒，也可以通过恢复数据轻松解决。