合理设置不让坏习惯威胁Windows系统安全Microsoft认证考试
 在频繁操作电脑的过程中，我们时常会养成一些不好的操作习惯，这些习惯看上去可以提供工作效率，但透过这些操作习惯一看，有很多都是威胁系统安全的操作，例如从Internet网络中下载获得REG文件后，多数人眼睛一闭就是直接双击，将其导入到系统注册表中，殊不知这样的操作严重时能导致系统崩溃.再比如说，在系统管理员权限状态下，随意打开IE浏览器上网冲浪，可能会导致系统遭遇木马或其他恶意代码的破坏或袭击。由于操作习惯不是一朝一夕就能改变的，为了不让坏习惯威胁Windows系统安全，我们可以通过合理设置，降低不良操作习惯的安全威胁程度。 1、降低双击REG文件的威胁 有时，为了实现某种功能目的，我们从网上下载得到相关的REG文件，再通过双击鼠标的方法将其导入到系统注册表，就可以达到目的了。但是，现在Internet网络中存在许多恶意的REG文件，要是贸然地对它们执行双击操作的话，Windows系统可能就会遭遇到非法攻击。为了降低这种操作习惯的安全威胁，我们可以通过手工设置，更改REG文件的打开方式，让Windows系统在收到双击操作命令之后，先调用写字板等文本编辑程序打开REG文件，这样一来我们就能识别出REG文件中是否存在危害系统安全的恶意代码了，下面就是该方法的具体实施步骤： 首先依次单击“ 开始 ”/“ 运行 ”命令，在弹出的系统运行对话框中，输入字符串命令“ cmd ”，单击回车键后，将系统屏幕切换到MS-DOS工作窗

口. 其次在该窗口的命令行提示符下，输入字符串命令“ ftype regfile=write.exe %1 ”，单击回车键后，Windows系统就会成功改变REG文件的导入方式，日后我们再次用鼠标双击该文件时，Windows系统将会使用写字板程序来打开REG文件中的内容，在该文本编辑窗口中我们会一目了然地看到其中是否存在危害系统的恶意代码了。要是发现其中没有恶意代码存在，我们只要再用鼠标右键单击目标REG文件，从弹出的快捷菜单中执行“ 合并 ”命令，就能将该文件中的内容导入到本地系统注册表中了。 当然，要是从Internet网络中下载得到的是BAT文件，我们也可以采用同样的方法更改它的打开方式，以便确保Windows系统的运行安全性。我们可以在MS-DOS工作窗口的命令行提示符下，执行字符串命令“ ftype batfile=write.exe %1 ”，这样一来日后用鼠标双击BAT文件时，首先打开的是文本编辑窗口。如果发现目标BAT文件符合运行要求，我们只要在MS-DOS工作窗口的命令行提示符下，输入该BAT文件的路径，单击回车键就可以了。 2、降低双击IE图标的威胁 为了获取最大的操作权限，很多上网用户往往喜欢用系统管理员账号登录Windows系统，然后在系统管理员权限状态下，随意打开IE浏览器上网冲浪，其实这也是很危险的操作习惯，这是因为IE浏览器自身存在很多安全漏洞，一些黑客程序常常会通过这些漏洞对计算机系统进行非法攻击，或者通过这些漏洞想方设法地窃取本地计算机的系统管理员权限。为了降低双击IE图标的威胁，我们可以想办法让Windows系统强行要求IE浏览器必须以标准用户账号运行，同时需要输入密码才能打开IE浏览器进行上网访问.要做到这一点，我们可以按照下面的操作来进行： 首先用

鼠标右键单击本地计算机系统桌面中的“ 计算机 ”图标，从弹出的快捷菜单中执行“ 管理 ”命令，打开对应系统的计算机管理窗口，在该窗口的左侧显示区域，依次点选“ 系统工具 ”/“ 本地用户和组 ”/“ 用户 ”分支选项. 其次用鼠标右键单击“ 用户 ”分支选项，并执行右键菜单中的“ 新用户 ”命令，在其后出现的新用户创建对话框中，创建一个新的标准账号名称，同时设置好合适的访问密码，假设在这里我们新创建了一个“ aaa ”标准账号，同时将该账号的密码设置为了“ 111 ”. 下面为IE浏览器创建一个快捷方式，并将该快捷方式直接拖放到系统桌面中，同时用鼠标右键单击IE快捷方式，从弹出的快捷菜单中执行“ 属性 ”命令，打开目标快捷方式的属性设置窗口，在该窗口的“ 目标 ”文本框中，直接输入字符串内容“ C:\Windows\System32\runas.exe /user:aaa "C:\Program Files\Internet Explorer\IEXPLORE.EXE" ”，单击“ 确定 ”按钮完成上述更改操作. 为了保证系统的绝对安全，我们现在再打开本地计算机的“ 开始 ”菜单，从中删除IE浏览器的相关项目，以及其他位置处的相关快捷方式，只保留系统桌面上的那个IE快捷方式。 经过这样的设置，我们日后在系统特权状态下，用鼠标双击系统桌面中的IE快捷方式时，系统会先要求我们输入“ aaa ”账号的密码，等到密码输入正确后，IE浏览器就会以“ aaa ”账号权限启动运行，在该权限状态下，黑客或非法攻击者即使利用了漏洞来攻击本地计算机，但无奈它们的攻击权限有限，而不会威胁本地计算机系统的安全运行。 3、降低运行注册表威胁 稍微懂得一点电脑知识的用户，常常会在本地计算机系统中随意运行注册表编辑程序，来自由更改系统相关注册表键值，殊不知如果某个

键值更改不当的话，轻则导致某个系统功能不能正常使用，严重的话会导致计算机系统发生瘫痪现象。其实，通过下面的设置操作，我们可以让Windows系统在用户执行“ regedit.exe ”程序时，自动弹出警告提示，告诉用户高危程序不要随意运行： 首先打开写字板程序，并在程序编辑窗口中输入具体的警告提示内容，假设这里输入的内容为“ 您当前运行的是高危程序，请一定要谨慎操作 ”，并将上述内容保存为“ F:\jinggao.txt ”. 其次再打开写字板文件编辑窗口，在其中输入下面的代码内容： start F:\jinggao.txt ping -n 5 127.0.0.1 &gt. nul taskkill /im write.exe 在确认上面的代码内容正确无误后，再依次单击“ 文件 ”/“ 保存 ”命令，将它保存为“ F:\jinggao.bat ”文件.Windows系统日后一旦执行了该批处理文件后，系统屏幕上就会出现5秒钟的“ 您当前运行的是高危程序，请一定要谨慎操作 ”文字提示. 下面依次单击“ 开始 ”/“ 运行 ”命令，在弹出的系统运行对话框中，输入“ regedit ”字符串命令，单击“ 确定 ”按钮后，打开对应系统的注册表编辑窗口，在该编辑窗口的左侧显示区域，依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options分支选项，在目标分支选项的右侧显示区域，用鼠标右键单击空白位置，并依次点选快捷菜单中的“ 新建 ”/“ 项 ”命令，再将新项取名为“ regedit.exe ”. 选中“ regedit.exe ”子项，再按相同的操作方法在该子项下面创建一个字符串键值，同时将该字符串键值取名为“ debugger ”，再用鼠标双击该键值，从其后出现的数值设置对话框中，将“ debugger ”数值设置为

“ F:\jinggao.bat ”，最后单击“ 确定 ”按钮完成注册表设置操作。 日后，当有其他用户在本地计算机系统中运行注册表程序时，系统屏幕上就会自动出现“ 您当前运行的是高危程序，请一定要谨慎操作 ”这样的警告提示信息了，五秒钟之后该提示信息会自动消失，相信出现这样的警报提示后，普通人就不敢随意运行注册表编辑这样的高危程序了。 