

安全小技巧个人电脑防黑客入侵八准则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\\_ti2020/561/2021\\_2022\\_\\_E5\\_AE\\_89\\_E5\\_85\\_A8\\_E5\\_B0\\_8F\\_E6\\_c100\\_561504.htm](https://www.100test.com/kao_ti2020/561/2021_2022__E5_AE_89_E5_85_A8_E5_B0_8F_E6_c100_561504.htm) 在这个网络时代，每个人都可以轻易地从网络上得到各种简单易用的黑客工具，于是，“黑客”就诞生了。这些人多半是一些无所事事的网虫，天生就有破坏的欲望。于是无聊表现欲促使他们拿着从网上找来的各种“炸弹”之类的东西开始在浩大的网络中寻找可以炫耀一下自己本事的猎物。当你在网络上冲浪，或是正在同别人聊天时，机器突然死机了或是蓝屏了，网页不能浏览了，QQ登录不上去了，这时你就该想想自己是不是中毒了，或是被黑了。那么为防止我们的个人电脑被黑客攻击，我们使用电脑时该遵循些什么样的安全准则呢？

一、密码安全准则 不要使用简单的密码。不要简单地用生日、单词或电话号码作为密码，密码的长度至少要8个字符以上，包含数字、大、小写字母和键盘上的其他字符混合。对于不同的网站和程序，要使用不同口令，以防止被黑客破译。要记录好你的ID和密码以免忘记，但不要将记录存放在上网的电脑里。不要为了下次登录方便而保存密码；还有，要经常更改密码和不要向任何人透露您的密码。

二、电子邮件安全准则 不要轻易打开电子邮件中的附件，更不要轻易运行邮件附件中的程序，除非你知道信息的来源。要时刻保持警惕性，不要轻易相信熟人发来的E-mail就一定没有黑客程序，如Happy99就会自动加在E-mail附件当中。不要在网络上随意公布或者留下您的电子邮件地址，去转信站申请一个转信信箱，因为只有它是不怕炸的。在E-mail客户端软件中限制邮件大小和过滤

垃圾邮件；使用远程登录的方式来预览邮件；最好申请数字签名；对于邮件附件要先用防病毒软件和专业清除木马的工具进行扫描后方可使用。

**三、IE的安全准则** 对于使用公共机器上网的网民，一定要注意IE的安全性。因为IE的自动完成功能在给用户填写表单和输入Web地址带来一定便利的同时，也给用户带来了潜在的泄密危险，最好禁用IE的自动完成功能。IE的历史记录中保存了用户已经访问过的所有页面的链接，在离开之前一定要清除历史记录；另外IE的临时文件夹（\Windows\Temporary Internet Files）内保存了用户已经浏览过的网页，通过IE的脱机浏览特性或者是其他第三方的离线浏览软件，其他用户能够轻松地翻阅你浏览的内容，所以离开之前也需删除该路径下的文件。还要使用具有对Cookie程序控制权的安全程序，因为Cookie程序会把信息传送回网站，当然安装个人防火墙也可对Cookie的使用进行禁止、提示或启用。

**四、聊天软件的安全准则** 在使用聊天软件的时候，最好设置为隐藏用户，以免别有用心者使用一些专用软件查看到你的IP地址，然后采用一些针对IP地址的黑客工具对你进行攻击。在聊天室的时候，还要预防Java炸弹，攻击者通常发送一些带恶意代码的HTML语句使你的电脑打开无数个窗口或显示巨型图片，最终导致死机。你只需禁止Java脚本的运行和显示图像功能就可以避免遭到攻击了，但这时你就没法访问一些交互式网页了，这需要你个人权衡。

**五、防止特洛伊木马安全准则** 不要太容易信任别人，不要輕易安装和运行从那些不知名的网站（特别是不可靠的FTP站点）下载的软件和来历不明的软件。有些程序可能是木马程序，如果你一旦安装了这些程序，它们就会在你不知情的情况下更改你

的系统或者连接到远程的服务器。这样，黑客就可以很容易进入你的电脑。笔者并不是让大家不信任来自Internet的任何东西，因为即使是很大的网站，都有可能遭到黑客的破坏。

六、定期升级你的系统 很多常用的程序和操作系统的内核都会发现漏洞，某些漏洞会让入侵者很容易进入到你的系统，这些漏洞会以很快的速度在黑客中传开。如近期流传极广的尼姆达病毒就是针对微软信件浏览器的弱点和Windows NT/2000、IIS的漏洞而编写出的一种传播能力很强的病毒。因此，用户一定要小心防范。软件的开发商会把补丁公布，以使用户补救这些漏洞。建议用户订阅关于这些漏洞的邮件列表，以便及时知道这些漏洞后打上补丁，以防黑客攻击。当然最好使用最新版本的浏览器软件、电子邮件软件以及其他程序，但要是测试版本。

七、安装防火墙 不要在没有防火墙的情况下上网冲浪。如果你使用的是宽带连接，例如ADSL或者光纤，那么你就会在任何时候都连上Internet，这样，你就很有可能成为那些闹着玩的黑客的目标。最好在不需要的时候断开连接，如可以在你的电脑上装上防黑客的防火墙一种反入侵的程序作为你的电脑的门卫，以监视数据流动或是断开网络连接。

八、禁止文件共享 局域网里的用户喜欢将自己的电脑设置为文件共享，以方便相互之间资源共享，但是如果你设了共享的话，就为那些黑客留了后门，这样他们就有机可乘进入你的电脑偷看你的文件，甚至搞些小破坏。建议在非设共享不可的情况下，最好为共享文件夹设置一个密码，否则公众以及你的对手将可以自由地访问你的那些共享文件。

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)