高深黑客眼中的个人安全防范问题思科认证 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__E9_AB_98_E6_B7_B1_E9_BB_91_E5_c101_644231.htm 在病毒横行，马儿随意吃草的年代，网民们谈论最多的就要属系统破坏，病毒入侵了。说实话，自己每次出差之前，都要给家人的和邻居们的计算机做一下检查。你也许会说，这不是吃饱了撑的么!没错，我是吃饱了，但绝对不是撑的没事做，因为经常在外出差办事，接到家里打来的电话，通常都是三句：“ 中招了，电脑开不了了! ”、“ 电脑现在好慢哦!怎么办啊? ”第3句话基本上就是问我什么时候回来。能用电脑的人不一定会使用好，装了个杀毒软件就能防范所有病毒么?想抵御黑客攻击，靠防火墙软件就可以么?作为黑客，我不得不说，没那么简单，那么对于大多数人来说，应该做什么样的防范，才能把黑客、病毒、恶意软件统统关在门外呢? 一、删除垃圾文件，把木马和病毒消灭在温床里 一般大家在浏览网站信息的时候，都会在本地机器上残留一些文件，而病毒也经常潜伏在里面，尤其是一些广告代码，恶意脚本和以及木马程序。这些文件集中在C 盘的Documents and Settings文件夹下的子文件夹(你经常用的登陆帐号，例如admin，就是你在装机器的时候，填写的那个登陆帐户的名字)下面的local setting里面的temp文件夹。我们只要Ctrl A 全选之后，删除就可以了。 注意：local setting文件夹默认是隐藏属性，所以，你必须要让系统显示所有隐藏文件，这点我就不说怎么做了，我想大家都应该会。 二、关闭自动播放，避免间接感染 DC、DV以及Mp3，Mp4等娱乐休闲设备大兴其道的同时，也给我们本已脆弱

的系统增加了几分凶险。很多人都是习惯性的将这些移动存储设备连接电脑后，直接传输文件、图片和视频，其实这个习惯很容易让你中招。曾经有一次，邻居的电脑发现双击打不开硬盘驱动器，弹出一个“ 选择打开方式 ”的对话框，其实是中了autoruan病毒。这类病毒的传播媒介主要是移动存储设备，由于经常要在磁盘内交换数据，很有可能会感染病毒。很多人都知道硬盘有加密区，移动存储设备也一样有，用于存放设备及厂家标识信息的，而且都不大，几十K，最大也不超过几百K。有些病毒和恶意代码程序就是专门针对移动存储设备的加密区而写的，即使你把U盘格式化，他们也依然存在。这无论对于个人还是企业，都有一定的威胁。据我所知，有些大公司和企业为了不让自己的机密信息通过U盘传播出去，就制定了不允许在公司内部使用U盘拷贝文件的规定。个人用户为了读取数据文件的方便，还是要使用移动存储设备的，那么我们怎么做才能把安全风险降到最低呢?闭Windows系统的自动播放服务，具体操作方法是：在运行里面，输入gpedit.msc，打开组策略，在用户配置下的管理模板中打开“ 系统 ”选项，在里面双击“ 关闭自动播放 ”，选择“ 已启用 ”，并选择“ 所有驱动器 ”，这样就可以关闭自动播放服务了。对于一些初级用户，如果想省事，使用大成的U盘免疫系统，也是不错的选择。 三、家用摄象头的安全隐患 个人隐私对于任何人来说，都是再重要不过的了，可是现在的黑客，为了Money，可谓是无恶不作。如果你碰巧有个摄像头，又恰巧被人安装木马，键盘记录器等小工具，那么恭喜你，你的机器既成为了人家手中的肉鸡，又有可能通过你的摄像头掌握你一切的活动，甚至有些变态的在澡堂和

换衣间安装针孔摄象头，来捕获一些信息出售了。 摄象头成本低廉，在电信、移动、网通这些“ 吸血鬼 ”狂喝我们纳税人血液的时候，Voip的诞生，网络通讯软件的广泛应用给我们省了不少Money。但是同时也造成了一些安全隐患，在你同别人视频的时候，如果对方在你机器中下了有针对性的木马，那么你所有的活动都将收入人家的眼底。前些时候网上抄的很凶的视频泄密，是真实存在的，只要在木马中加一小段代码，就可以实现远程遥控的你摄像头。使用工具的伪“ 黑客 ”们可以捕获你和对方的谈话信息，捕获你的屏幕，甚至利用你的摄象头来监视你，这是绝对可以实现的，而且你还不知道。那你也许会问，把摄像头关了，不就可以了么?答案是否定的，同样在木马或病毒中加上一小段脚本，就可以远程开关你的摄像头，你在房间的一举一动都能看的清清楚楚。 有句话说的好，不怕贼偷就怕贼惦记。对家用摄像头带来的安全隐患，没有特别好的处理方法，通常都是聊天完毕，立即拔掉摄象头即可避免这样的情况。但对于彻夜不关机的懒人来说，就需要在睡觉的时候给摄像头盖上一块布，或者对着一盆花。 四、如何防止个人信息泄露 通常个人电脑中发生的密码泄露，游戏帐号泄露等事件都是病毒、木马以及恶意程序造成的，这些程序在你的电脑中植入小小的键盘记录器，来记录你的个人信息。在子明的黑客故事系列的第三篇，黑客窃取银行中就有对键盘记录器的详细介绍。www. Ｅxamda.CoM考试就到百考试题 对付键盘记录器的一些个人建议：在输入密码时，前面先多做几次出错。在选择输入框的同时利用鼠标不断变换位置，尽量不要先输入头一位。现在网络银行和QQ 登陆帐户都启用了软键盘功能，以前的软

键盘输入之后，光标位置不变，而现在的就不错，每次打开输入一次，键盘上的字母和数字就会重新变换一次位置，这就造成了Hook(钩子)的失效，那是不是这些黑客就无法破解了呢?答案是一定否定的，但是对于个人用户，这些是足够的了。 总结：个人用户在更新系统补丁的同时，一定要及时升级杀毒软件，不要以为杀毒软件能自动完成查杀，它也只能查杀病毒特征库中已知的病毒，对于那些黑客自己编写，尚未流通的病毒是无效的。最好的预防办法就是少一些好奇，尽量不要浏览不明网站和下载不明程序，尤其那些地址看上去非常怪异的，实在想浏览可以利用搜索引擎中的快照功能。对于Emule，vagaa等P2P软件，也要多加小心，因为这些软件也是更多病毒的温床。最重要的是多为自己增加几分网络安全意识，网络安全防范，防的不是别人，要防的其实是自己，少一些好奇，少一些无知，少一些贪欲，这才是你最好的防范。黑客想进门也不那么容易了。 