网络安全防御全面封阻主要网络威胁思科认证 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__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_644226.htm 如果你认真核对这份安全一览表，就很有希望让数据窃贼把目光转移到比较容易下手的对象。数据窃贼并不总是像电影《黑客帝国》里面那样躲在阴暗房间里不停地敲键盘的黑帽子黑客：有些数据中心的员工爱惹事生非，而且技术方面有本事欺骗“ 领导 ”，他们常常也负有责任。 那么你该怎样来对付呢？无论你仅仅负责自己的一台计算机，还是要管理一批成百上千台PC，PC都容易受到各种各样的威胁，其中包括： P2P客户程序 不安全的无线网络 网络钓鱼 间谍软件 病毒 不安全的在家办公环境 社会工程 本文教你如何阻止这些威胁。 对P2P文件共享说不 作为与其他媒体爱好者共享音乐和视频文件的一种简便方式，像Gnutella、BitTorrent、Kazaa和LimeWire这些对等文件传输客户程序几乎像病毒一样流行。可遗憾的是，它们还能够与周围街区、全国乃至全世界的陌生人共享敏感的公司和个人数据。 最近针对银行和联邦政府使用P2P文件共享情况的几项调查显示，当初为共享媒体编写的这类程序访问机密和秘密信息有多么容易。达特茅斯大学的塔克商学院曾对美国前三十家银行使用P2P文件共享的情况作了一项调查，结果发现，P2P文件共享搜索歌曲里面的歌词或者视频文件名，居然发现了各种类型的匹配信息，包括公司名称、地址及更多的信息。 安全公司Tiversa开展的一项调查发现，使用P2P客户程序LimeWire仅仅搜索了两三个小时，发现的机密文档就超过了200个。 为什么P2P文件共享会带来如此之大的潜在

危险呢？视客户程序而定，P2P文件共享通常按文件类型进行，而不是按文件夹进行。因而，P2P搜索之后，与机密信息放在同一文件夹里面的音乐或者视频文件就会把整个文件夹里面的内容暴露在面前。 更糟糕的是，有些P2P客户程序让人们便于共享整个驱动器，而不是单单共享指定文件夹。如今，P2P客户程序无处不在，包括孩子的PC或者其他家用PC，甚至还出现在公司PC上。 为了阻止P2P文件共享给工作环境带来的威胁，公司应当进行安全配置，阻止P2P客户程序。如果你在远程办公，请对工作文件夹进行文件加密，并且确保绝对不会安装P2P客户程序来监控工作文件夹。还要随时关注P2P方面的动态。 保护不安全的无线网络 无线网络很容易组建——特别是不安全的无线网络。你的办公室可能建有一个无线网络，采用WPA或者WPA2加密和Radius验证服务器加以保护；如果你在家或者在公共场所办公，但用的是不安全的无线网络，就有可能暴露敏感信息。那么，外头有哪几种威胁呢？ 如果餐馆或者其他零售店使用不安全的无线网络供销售点系统使用，那么泊在停车场的“ 无线窃听者 ”（wardriver）就能获得商业信用卡上的信用卡号码，然后伺机出售；或者使用它们擅自疯狂购物。 免费的无线热点大量出现在餐馆和咖啡馆。如果笔记本电脑上的网络共享没有被防火墙阻止，其他上网者就可以边吃东西，边偷偷窃取你的数据。 家庭无线网络具有双重的不安全性：它们可能是不安全的（缺乏WPA或者WPA2加密），还可能使用标准的服务集标识符（SSID）或者工作组名称；这样一来，入侵者轻而易举就能进入网络，访问系统上的任何共享文件夹。 100Test下载频道开通，各类考试题目直接下载。详细请访问