谨慎使用无线网络五项WiFi热点安全建议思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E8_B0_A8_E6_85_8E_E4_BD_BF_E7_c101_590378.htm 笔记本电脑是大多数移动办公人员的主要业务工具，通过免费的公共Wi-Fi热点把这些设备连接在Internet上已经成为常见的作法。那么，这些移动办公人员遵守移动计算安全准则的情况又如何呢? 为此，我们直接去采访使用者。我们访问了机场、餐馆和咖啡馆，询问人们为保护自己的笔记本电脑所采取的安全措施的情况。 我们询问了笔记本电脑是个人财产还是工作单位提供的，是用于个人事务还是工作项目，用户参加过何种安全培训，以及其他有关Wi-Fi使用和一般笔记本电脑安全的情况。由于我们没有追问除用户名字以外的个人详细信息，人们在回答时似乎相当坦诚。 调查的结果会让任何安全专业人员都吓出一身冷汗。许多用户不知道自己的笔记本电脑具有哪些安全特性，并且对计算安全只有模糊的概念。让我们先从展现出最好Wi-Fi行为的最终用户开始，然后再讲真正恐怖的故事。 淡薄的安全意识 Timothy: B 每一位拥有笔记本电脑员工的IT经理都会很高兴把Timothy树立为明智地使用笔记本电脑的榜样。坐在洛杉矶机场，把笔记本电脑连接在手机上，Timothy做了绝大部分的正确事情来保护笔记本电脑的安全。 身为一家医疗设备制造商技术员的Timothy说：“ 公司的所有现场服务工程师都必须获得A 认证。IT设备安装安全软件，我们偶尔收到有关安全的备忘录，但我们都懂得安全问题，并且非常小心。 ”在使用公共Wi-Fi热点网络时，移动办公人员更要加强安全意识 由于洛杉矶机场不提供免费Wi-Fi

，Timothy通过手机使用Sprint的蜂窝数据网连接网络。不过在有免费Wi-Fi可供使用的地方，例如在丹佛机场，他就直接利用Wi-Fi网络。 Timothy说，他在查看公司的电子邮件时，接入一条回连公司网络的VPN，不过他当时没有使用它。他的雇主提供了Dell Latitude D520来运行Windows XP，不过Timothy承认他也使用这台机器处理个人事务。 Timothy的笔记本电脑还设置了加载Windows前要求输入的口令。他不知道这个口令是系统级口令还是用于整个硬盘加密产品的口令。 Kurt: B 接下来要讲的是地区餐馆连锁店CFO Kurt。Kurt喜欢免费Wi-Fi(如果他能得到的话)，并拒绝考虑为自己或他的用户购买任何类型的蜂窝数据网。他说：“ 如果我在旅行时可以利用免费Wi-Fi满足需求的话，那么其他人也可以这样做。 ”坐在Dallas Ft. Worth机场的Kurt购买了使用T-Mobile Wi-Fi接入服务的单日使用卡。他用Dell Latitude 630(公司配发的设备)运行Windows XP。 Kurt说：“ 我们使用Blackberry或智能手机查看电子邮件，因此笔记本电脑的连接并不那么关键。 ”他确实使用公司的笔记本电脑处理个人事务，但是当问及是否通过公共Wi-Fi使用在线银行时，他立即给出了断然的否定回答。Kurt说：“ 如果需要的话，我可以通过VPN访问公司的财务服务器，但那是我工作时使用的连接。 ”他拒绝考虑使用来自一家主要移动电话提供商的蜂窝数据网络，认为那只是“ 看起来光鲜 ”而已。当用户寻找免费Wi-Fi网络时，他们把自己暴露在形形色色的侦听黑客技术面前，尤其当他们意外连接在Ad Hoc网络上时。 实际上，在1个月内购买两张T-Mobile上网单日卡以及支付3天的饭店Internet接入费用，将让Kurt付出与每月蜂窝数据网络费同样的费用。而每

月在笔记本电脑连接上花费60美元的用户将从蜂窝数据网固定的、可预测的价格模型中受益，而且至少比搜索开放的公共Wi-Fi网络更安全一点。 Rebecca: D 在一家名为“ Panera Bread ”的连锁店中，Rebecca一边啜茶，一边摆弄着她那台运行Windows XP的Acer 1640Z笔记本电脑。她为自己的两项工作(一家医院和兼职的本地学院)中使用个人笔记本电脑。 她使用公共Wi-Fi收发电子邮件和上网冲浪。她说她没法从远程位置直接连接学院的网络，但的确通过学院的Web界面访问几种系统。 当问及与医院的连接时，她说：“ 我使用像Citrix这样的产品。 ”她说，医院IT部门安装了Citrix软件和一些安全程序，不过她不知道它们是做什么的。 在这里我们看到一台往来于两个要求小心处理客户记录的管制非常严格的行业医院和大学之间的笔记本电脑，这台笔记本电脑物理或远程连接在这两个单位的网络上。Rebecca的笔记本电脑没有采取物理安全措施，如系统启动口令或任何级别的硬盘加密。一想到如果笔记本电脑被盗其他人会很容易地访问保存在笔记本电脑上的信息，或利用10多种Wi-Fi嗅探工具很容易地截获数据时，就会让我们感到不寒而栗。 Brad: D 再来说说Brad。当Brad坐在Panera Bread餐馆中利用公共Wi-Fi上网时，他骄傲地炫耀自己那台刚买了9个月、运行Windows XP系统的Dell E1405笔记本电脑。他自己购买了这台计算机，但也把它当做他所工作的教堂中的主计算机来使用。这意味着他在Panera Bread餐馆中用笔记本电脑所做的一切都会随他进入办公室，直接进入办公室的网络中。 Brad说：“ 我在笔记本电脑上做各种事情。电子邮件、博客、Web调查、在线查看银行账户，所有个人的和教堂工作的事。 ”但是，当他稍后说自己从

来不让浏览器保存所访问的网站用户名和口令时，可能才意识到一点刚才这段话的安全含义。 Jay: C Jay坐在达拉斯Cafe Express餐馆(一个繁忙的Wi-Fi热点)里，用他的运行OS X 10.5系统的老MacBook读电子邮件。作为一位个体音乐家兼活动策划师，Jay很少担心公共Wi-Fi存在的安全问题，因为“ 它是台Mac ”。 这台机器的正式身份是一台工作计算机，当他离开家庭办公室时使用这台设备处理所有个人和工作事务。 为了证明他确实担心丢失自己的笔记本电脑，Jay提出要让我们看看放在电脑包中的Kensington笔记本电脑锁。不幸的是，这个电脑包中实际上只有两条备用的音频设备RCA线。但Jay比我们遇见的其他任何人都要更担心笔记本电脑的物理安全，这点值得赞扬。 如何携带笔记本电脑安全出行 使用笔记本电脑标签服务或跟踪服务，或同时使用两者。 在乘坐公共交通时，始终把笔记本电脑放在腿上。在2005年，仅芝加哥市就有4400多台笔记本电脑被丢在了出租车中。 经验教训总结 简单地说，我们采访的笔记本电脑用户在使用公共Wi-Fi网络时，似乎都不担心安全问题。那些拥有办公笔记本电脑的用户在处理个人事务时仍使用它们，那些把个人笔记本电脑用于工作的用户也没有采取什么安全措施。 没有人主动提到他们使用防火墙，尽管在问及时一些人知道他们使用防火墙。没有人意识到在我们谈话过程中，他们的通信可能遭受到大量的偶然和有目标的Wi-Fi黑客行为的攻击。 由于在新闻报道中大多数数据泄露都始于某一类丢失的笔记本电脑，因此我们期待着听到一些人告诉我们全盘加密了自己的笔记本电脑硬盘。但没有人这样说(尽管Timothy可能使用了全盘加密)，也没有人使用任何类型的数据文件夹加密措施。 我们采访的笔

记本电脑用户中，没人使用任何类型的笔记本电脑标签技术或跟踪服务来大大增加拿回丢失的笔记本电脑的可能。由于每周有近12000台笔记本电脑在美国机场丢失或被盗，因此一位经常外出的人可能丢失笔记本电脑的概率很大。 标签跟踪技术利用唯一的ID以及免费电话号码和URL给笔记本电脑贴上一个永久的标签。当有人发现丢失的笔记本电脑时，这项服务将帮助笔记本电脑回到所有者手中，并奖励发现者。由于商务笔记本电脑的价格仍在1000美元到1500美元，因此取回笔记本电脑可以节省一大笔钱。 跟踪服务也有助于取回笔记本电脑，但它的重点放在那些小偷偷走的笔记本电脑上。一旦笔记本电脑连接在网络上，隐藏的软件会“ 给家里打电话 ”，报告笔记本电脑的位置。当报告被偷时，跟踪服务确定笔记本电脑的位置并通知所有者或当地警方。这个领域的市场领先者Absolute.com声称找回了 5000多台被偷的笔记本电脑，包括2007年1周内找回的200多台笔记本电脑。 宣扬“ 禁限 ”作为这项调查的一部分，我们采访了一家主要金融服务机构的安全经理John，询问公司提供的笔记本电脑的使用规定。这些规定是我们见过的最严格的规定，肯定会让我们采访过的笔记本电脑用户感到吃惊。 John说：“ 永远不许使用公共Wi-Fi。我们只使用蜂窝数据网，以获得更多一些的安全保障。我们封锁上了笔记本电脑上的USB端口和CD-DVD光驱。如果你可以加载程序，你就有可能会被感染。当笔记本电脑受到感染时，你将把感染的病毒带进办公室。 ”
在Starbucks咖啡馆，我们发现了一位赞成John的“ 禁限 ”理论的最终用户。他在Starbucks里使用个人的老款Gateway笔记本电脑。他边把电源线插入到墙上的电源插座上边说：“ 不

管在任选地方，我都从不使用无线上网。在家不用，在办公室不用，在公共场所肯定更不用了。”当然，不加选择地使用公共Wi-Fi与走“禁限”之路之间存在着中间地带。用户可以通过遵守为人们接受的最佳安全实践(包括防火墙、加密、VPN和笔记本电脑丢失或被盗时保护数据的物理安全措施)，来实现安全的网上冲浪。 五项Wi-Fi安全建议 始终使用个人防火墙和最新的安全软件。 避免使用所有开放的接入、Ad Hoc Wi-Fi网络。 在连接到公共Wi-Fi时，使用企业VPN用于回连到公司的链路。 确保所有的传输流都得到加密。不要使用普通的POP3、IMAP或SMTP来收发电子邮件，而要使用POP3 over SSL(POP3S)、IMAP over SSL(IMAPS)和SMTP over SSL(SMTPS/SMTPTLS)。 在防窃听方面，蜂窝数据网可提供比Wi-Fi略高的技术障碍，但仍要使用防火墙并采取其他措施。 不要使用唯恐别人不知“内有贵重笔记本电脑”的显眼标识的笔记本电脑包。 为避免看到来自丢失的笔记本电脑中的数据出现在CNN上，请使用全硬盘的加密。 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 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