教你八招无线网络安全性技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/231/2021_2022__E6_95_99_E4_BD_A0_E5_85_AB_E6_c101_231479.htm 无线网络的攻击通常是指黑客非法接入受害人的无线网络。这样的情况大多发生在用户没有在其无线接入点（AP）采用适当的安全性策略的情况下。不在无线接入点应用安全性策略的危害在于：恶意广告和垃圾邮件将会侵入用户的终端，黑客将可以入侵用户系统窃取用户名和密码等机密信息。而且，病毒和木马的入侵还将会因此而散播开来，因此用户有责任在自己使用的无线接入点上部署和升级安全性策略。本文则阐述了八种无线家庭网络的安全性技巧。 技巧1：修改默认的管理员（用户）密码 修改默认的管理员（用户）密码很重要。因为最简单的攻击发生在：每个购买同一批出厂的无线接入设备（无线路由器）的用户，都被默认设定了相同的初始密码，如果不做修改则很容易被他人盗用。技巧2：开启WPA/WEP加密服务 在默认状态下，无线接入点设备通常都是没有开启加密服务。而事实上，厂商在无线设备中已经注入了WPA（有线等效协议）/WEP（Wi-Fi保护接入协议），强制用户的主机在提供了密码后才能够接入无线接入点。 因此，用户应该开启WPA/WEP加密服务以提高接入点的安全性防护能力。 技巧3：改变初始SSID 服务集标志符(Service Set Identifier,简称SSID)用来标识不同的无线网络。许多用户都将他们无线设备的SSID保留为默认的设置，例如Linsys、NetGear等。 然而，改变初始的SSID值可以提高网络的安全性，这样入侵者需要更多的时间才能够捕捉到一些共同的漏洞（例如技巧1中提

到的没有改变的初始密码）。而且，建议用户最好不要用他们的家庭地址等信息作为SSID，这样有可能会和他们的邻居产生重叠，进而可能收到对方的攻击，因为设置成相同SSID的用户相当于在一个局域网内，可以彼此通信。