Securely protect information on Wi-Fi network

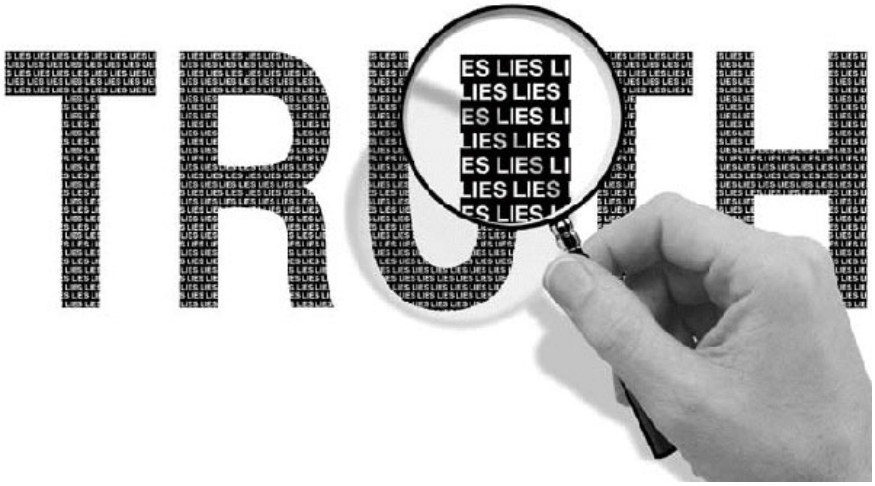
Wi-Fi networks are not yet a safe environment. On private networks, users can enable secure encryption to prevent illegal users from connecting and capturing traffic. However, depending on the security method used, user data can still be stolen. And

TipsMake.com - Wi-Fi networks are not yet a safe environment. On private networks, users can enable secure encryption to prevent illegal users from connecting and capturing traffic. However, depending on the security method used, user data can still be stolen. And although public networks can use web-based authentication, most of these networks do not have a true security encryption method. So anyone in range can 'eavesdrop' on hotspot traffic.

The article will clarify how Wi-Fi spies are and suggest some solutions to protect users when using private and public Wi-Fi networks.

Wi-Fi spy

To better understand what a Wi-Fi spy is, we should find out what can be done on the captured Wi-Fi traffic. When an intruder catches traffic packets over Wi-Fi, he can know the password and content of the services or websites that the victim logged in when not using SSL encryption technique, usually the connect POP3 / IMAP and FTP email. He can also block login (hjack) to websites like Facebook and Twitter or collect transfer files on private networks.



Fortunately, Wi-Fi spies will not easily reach their goals if the service or website uses SSL encryption technology, such as bank websites. But they can still use vulnerabilities on SSL. This is another topic of paper waste.

Data protection on public networks

Since most Wi-Fi hotspots do not use any secure encryption method and do not provide traffic protection, stealing information seems to be a concern over public networks. Obviously, there are a lot of tools that can be easily used by ordinary users to steal information from others. Not even more than a smartphone to steal your password or block your account.

The best solution to keep your network traffic safe when using Wi-Fi hotspots is to use a VPN for connecting to a corporate intranet or server. Or use a master service designed specifically for hotspot protection such as Private Wi-Fi or Hotspot Shield. When connecting to a VPN, all Internet traffic sent from the computer or user device will pass through a secure encrypted tunnel to the VPN provider network. So the traffic is completely safe from Wi-Fi spies at the internal hotspot.

If you can't or don't like using a VPN, users should at least make sure that any service or website will use it while connecting a hotspot is safe with SSL encryption. When SSL is applied, the web browser will have an https address instead of http and will display a pad lock with some other directives. For mail application programs such as Outlook or Thunderbird, users need to make sure SSL is being used for POP3 or IMAP connections and SMTP servers. However, many email providers do not support this encryption feature. You can find other solutions such as Neomailbox, Hushmail or 4Secure-mail.

For access on public hotspots, you must always ensure that any website you sign in for sensitive information or any service you use (such as email and FTP) is protected by SSL. This will ensure that the information between the computer and the site or service is always safe.

Data protection on private networks

Although stealing information is a major concern on untrusted Wi-Fi networks, it still causes some anxiety on private networks. An enterprise network, for example, can still be threatened by bad employees or intruders. While using WPA2's PSK data encryption mode (also called Personal mode) for wireless networks and requiring private network users to enter a connection password, it still allows one person Internal users catch traffic of other users. Fortunately, WPA2 has a mode called enterprise mode (Enterprise mode or 802.1X or EAP) to prevent this user from reading traffic of other users. This is because each user will be given authentication information such as username, password . to connect to the network instead of using the most common password such as personal mode. When a person logs in through enterprise mode, an automatic encryption key is issued and changed periodically.

However, the Enterprise mode of WPA2 requires an authentication server, often called RADIUS (Remote Authentication Dial In User Service). But if you are using Windows Server, you can use the IAS (Internet Authentication Service) program in previous versions of Windows Server 2003 R2 or Network Policy Server (NPS) in Windows Server 2008 and later versions next.

If the user's current servers do not have RADIUS functionality, there are still many free or cheap servers such as FreeRADIUS, TekRADIUS, ClearBox and Elektron. Some access points (such as HP ProCurve 530 or ZyXEL NWA 3500, NWA 3166 or NWA 3160-N) even embed a RADIUS server, great for small networks. And if you don't want to run your own server, there are many master services like AuthenticateMyWifi for users to choose from.

summary

Thus, Wi-Fi spying can be a real problem with public Wi-Fi networks. The best way to protect yourself is to use a VPN connection or at least make sure that at the site or service you are using SSL encryption. And with personal network, you must always pay attention to internal safety and ensure this user cannot catch other user traffic.