

Forum:[Hack Forums](#)

Thread: [protect my privacy on open wifi networks](#)

nicodemo - June 2, 2015, 11:28 am

I have access to a wifi network without password then a public network. a curious person can see the sites I'm visiting? in what way? (wireshark?). I can prevent him to see the sites I'm visiting?

pomwtin - June 2, 2015, 11:57 am

Sure, without encryption everything is plain-text.

Easiest fix would be VPN with "end to end" encryption.

You can use tor for example.

|Foundry - June 2, 2015, 1:41 pm

Yes, a curious person can easily monitor most communications which take place over a public WiFi network, both by intercepting plaintext HTTP traffic and in cases where the attacker has more experience or dedication, stripping SSL from HTTPS connections. Either way, using public WiFi networks can turn out very poorly without taking steps to protect yourself.

This person could see the sites you are visiting through several tools, but yes, Wireshark is one of them. Anything that can sniff the packets which are passed around a network can be used to monitor the traffic of a user of that network.

To protect yourself, the only catch-all solution that you can use is to use a VPN or a SSH proxy. A VPN or SSH tunnel will act as the middleman between your computer and the dubiously secure servers on the internet so that everything sent between your computer and your VPN or SSH server will be encrypted — in effect securing all traffic that someone on your current network might want to try sniffing.

I'd personally recommend [Cryptostorm](#) for anyone looking to get a VPN for security purposes since there aren't any better solutions than what they provide, period. If you're looking for a VPN with a larger feature list for an excellent price and you aren't a security fanatic, I'd recommend using [143VPN](#) which offers quality service as well as several neat features such as allowing you to open your own ports on their VPN.

D3xH3x - June 2, 2015, 1:53 pm

(Jun 2, 2015 01:41 PM)|Foundry Wrote: [\[CITE\]](#) Yes, a curious person can easily monitor most communications which take place over a public WiFi network, both by intercepting plaintext HTTP traffic and in cases where the attacker has more experience or dedication, stripping SSL from HTTPS connections. Either way, using public WiFi networks can turn out very poorly without taking steps to protect yourself.

This person could see the sites you are visiting through several tools, but yes, Wireshark is one of them. Anything that can sniff the packets which are passed around a network can be used to monitor the traffic of a user of that network.

To protect yourself, the only catch-all solution that you can use is to use a VPN or a SSH proxy. A VPN or SSH tunnel will act as the middleman between your computer and the dubiously secure servers on the internet so that everything sent between your computer and your VPN or SSH server will be encrypted — in effect securing all traffic that someone on your current network might want to try sniffing.

I'd personally recommend [Cryptostorm](#) for anyone looking to get a VPN for security purposes since there aren't any better solutions than what they provide, period. If you're looking for a VPN with a

larger feature list for an excellent price and you aren't a security fanatic, I'd recommend using [143VPN](#) which offers quality service as well as several neat features such as allowing you to open your own ports on their VPN.

Agree with Foundry.

'Putty' is a great little tool for SSH tunneling.

If you don't want to pay for a VPN service then I recommend running a SSH server at home (if you are not worried about anonymity), which is suitably locked down so it can be exposed to the internet. You can then SSH to it from your PC on a public wi-fi and tunnel all your traffic through it.

Alternatively you can use openvpn as your own vpn between your pc and home.

D3x

webdev77 - June 2, 2015, 1:55 pm

Using an encrypted VPN is a standard method of protecting yourself on public networks. Many businesses that allow employees to use laptops require that VPN clients be used when not in the office.

Supreme??????? - June 2, 2015, 1:56 pm

VPNs are the way to go in this case. You can find free and fairly cheap ones around HF.

Frosteh - June 3, 2015, 8:42 am

On an OPN network with no encryption, or even with WEP where only 1 encryption key is used, all traffic can be sniffed, even traffic that goes over SSL connections to encrypt the data still reveal who you're talking to since the packets contain the header IP of the host.

The best solution is a VPN provider, you create a VPN tunnel from your PC to an external provider which encrypts all traffic inside it and to an outsider all they see is encrypted bytes being shuffled between you and the VPN provider, with no data leakage.