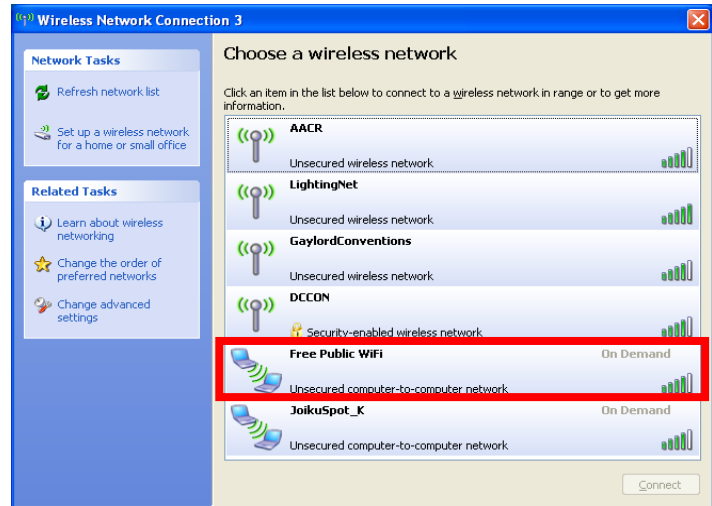




## Endpoint Wireless Security Best Practices

1. Connect only to trusted networks known to you.

Alluring WiFi networks, such as the one marked in the figure, can be harmful. Connecting to such networks can make your laptop vulnerable to WiFi hack attacks.



2. Configure your laptop to connect only to “Access point (Infrastructure)” networks and make sure the “Automatically connect to non-preferred networks” option is NOT selected.

These settings will ensure that your laptop will not connect to any WiFi network without your knowledge and not connect to other laptops to form an ad-hoc network.

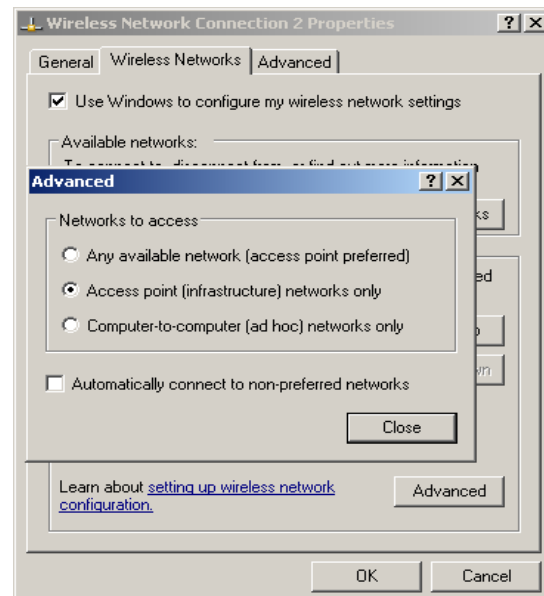


icon represents an ad-hoc WiFi network.



icon represents an infrastructure WiFi network.

Other laptops directly connecting to your laptop can expose security holes in your laptop and could even gain access to your hard disk.



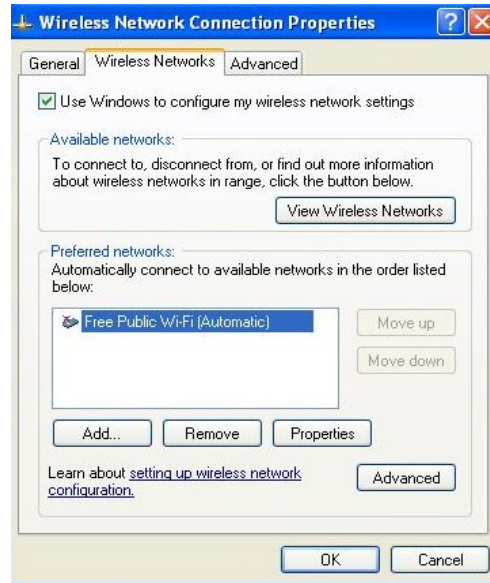
3. Avoid accessing confidential or sensitive information over Open (unsecured) connections. Prefer SSL-secured websites (that use https).

4. Use a VPN client when connecting over unsecured public WiFi hotspots. VPN clients are available for free download on the Internet.

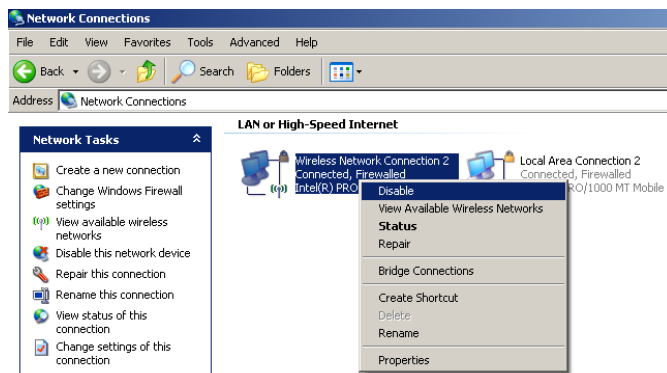
5. Remove undesirable wireless networks from your wireless network connection profile.

Your laptop keeps searching for WiFi networks in your “Preferred networks” list by broadcasting probe requests. This increases the likelihood of your laptop automatically connecting to an untrusted WiFi network.

Regularly clean up your “Preferred networks” list and remove networks that you don’t use.



6. Turn off your wireless card when you do not need to be connected over wireless.



7. Keep your laptop’s WiFi driver software up to date by applying appropriate patches when they are available.

8. Avoid connecting to a wired network (e.g., your corporate network) with your WiFi turned ON.

9. Use a **wireless security endpoint agent** that automates and implements most of these best practices for you and keeps your laptop secure even when you are travelling. Windows firewall and anti-virus software do not protect you from WiFi vulnerabilities and attacks.

For more information, please visit: [www.airtightnetworks.com](http://www.airtightnetworks.com)