

Wi-Fi is a high security risk if not secured.

Today, Wi-Fi has become a valuable part of the mobile computing arsenal for working professionals. Usage of Wi-Fi has enabled easier connectivity over the air, enabling larger mobility for professionals. Wi-Fi has enabled employees to remain in continual communication with their offices through the use of hotspots to gain internet connections. Unfortunately, the mobility, technology and information access that make Wi-Fi so useful to employees and organizations have also increased risk for enterprises.

This Better Security Practices Note, aims to help users of wireless communication media realize the risks associated with wireless media usage and advice on implementing security measures to mitigate the same.

Wireless Access a backdoor to your corporate network

Most enterprises setting up wireless networks have implemented Wi-Fi with the sole objective to enable mobility and internet connectivity to the end user. Laptops preloaded with wireless access cards and auto connectivity settings have also facilitated large scale deployment.

Most users connecting to these wireless devices are unaware that they are actually transmitting information over the air which can be easily viewed by others. Remote wireless accessibility has also enabled hackers to connect to the corporate networks from outside the corporate premises.

Doing these basic steps will go a long way

Like most issues, this problem needs to be addressed at the individual and corporate level. While the latter is out of the purview of this note, here is what you can do at an individual level to mitigate many of the risks.

What can go wrong?

- Accidental association where user latches on to a wireless access point from neighboring company's overlapping wireless network thereby endangering corporate information.
- Malicious associations where wireless devices can be actively made by hackers to connect to company network through their dummy access points instead of company's access points thereby sniffing wireless traffic to get valuable information.
- Ad Hoc networks where connectivity is established between wireless computers without the need for a wireless access point.
- Remote access to your corporate data and wired communication infrastructure from a remote location due to the coverage area offered by your wireless access point.

What you should be doing right away to fix this?

- Change the default wireless device administrator password. Do it now!
- Turn on WPA/WEP encryption to be used by your wireless device.

- Unplug or disable Wi-Fi media if not in use.

Comprehensive Mitigation Checklist (what you need a additional resource to do)

- Enable MAC Address filtering so as to allow connection only to the authorized devices.
- Change default SSID to prevent attacks.
- Disable SSID broadcasts if not required.
- Disable setting to auto connect to open Wi-Fi networks.
- Enable firewalls on all your wireless routers.
- Place wireless access point at the centre of your premises rather than near the edges or walls to contain leakage.