The potential dangers of Wi-Fi

Most in today's business world, especially those who regularly travel, are sure that laptops and Wi-Fi connections are indispensable. Most laptops today support Wi-Fi as a default configuration.

Most in today's business world, especially those who regularly travel, are sure that laptops and Wi-Fi connections are indispensable. Most laptops today support Wi-Fi as a default configuration.

Wireless network offers great advantages, but contains hidden dangers, especially security issues.As a mobile user, entrepreneurs, end users always need to use a laptop to connect to a corporate network or access public Wi-Fi networks . However, they are still not aware of risk of wireless network security.

Most Wi-Fi security connections depend on wireless data encryption, wireless access management or intrusion prevention.The potential risks in wireless networking are always a huge challenge in network security.Two of the most significant Wi-Fi network security risks are *ad hoc* (*ad hoc mode*) and *dual homing.*

Ad hoc mode

Wireless network cards (NICs) operate in two modes: *infrastructure* (infrastructure) and *ad hoc* (in particular). *Infrastructure* mode is used when a laptop connects to an *access point* such as an office, at home or a public hotspot.

Ad hoc mode allows your laptop to act as an access point, and other users can connect to this laptop as a peer-to-peer wireless connection. Wireless laptops in *ad hoc* mode are always hackers' targets. Because connecting to

these laptops and stealing information is simple, quick and almost undetectable. The normally configured *Ad hoc* mode works in the default mode from the time it is manufactured, and many users often retain this default configuration.

Even this becomes even more frightening.When a hacker sets up his laptop with the same name as the access point (as configured in your laptop) - this is perfectly valid.Consequently, other users are unaware that they are connecting to a hacker computer, not your laptop.Next, important information such as passwords and credit card numbers can easily be stolen by hackers.

Dual homing

Most laptops today use 2 network cards.One for wired connections like Ethernet, dial-up . and one for Wi-Fi wireless connections.This means that this computer can access both wireless and wired networks simultaneously.

If the laptop's Wi-Fi network card has *Ad hoc* mode installed and the user connects to the wired network, the hacker can easily connect to this laptop via ad hoc mode.Next, you can access the wired network using that laptop as a bridge.Consequently, hackers can sabotage and steal important business information .

Here are a few simple steps to help laptop users avoid the risks of using Wi-Fi wireless connections:

1. Please turn off *ad hoc* mode and do not connect to other *ad hoc* networks unless you have good reasons such as exchanging information between users who really believe in the meeting room. However, it is best not to use *ad hoc* mode.
2. Before connecting to wired networks in businesses, turn off the wireless network card or check that the wireless network is off *ad hoc* mode and not connect to any wireless network.
3. Ask the company's IT staff about policies to use wireless networks and follow these rules.These policies protect the information in the company and everyone who uses wireless or wired connections must follow.

   IT staff in companies need to ensure security in the network and manage wireless connections well:

4. Don't assume wireless technology is a completely different network system in the enterprise network.Wireless networking is really an important part of the corporate network.
5. Network management in the enterprise needs to include network security and good management of wireless devices.
6. Use a network management solution for businesses that provides secure binding policies between wired and wireless connections.

   Currently, network connectivity will continue to be the hybrid network generation between wired and wireless networks.Be careful, and use the same precautions as the best way to protect your network.

   Minh Phuc