spyware

Spyware

The term spyware refers to any software that hijacks a computer's normal operation in order to invade the user's privacy. Spyware can interfere with normal network use in any number of ways, and a spyware problem can show up as just about any kind of network problem. To date, spyware only affects Windows systems.

Most spyware installs itself into Internet Explorer and intercepts Web browsing – popping up ads or redirecting the user's searches to advertisements. Other browsers are (so far) not usually affected by spyware.

Spyware replaces Windows' network drivers (Winsock), sending all network traffic through the spyware operator's site. This will cause all sorts of networking problems, and can usually only be fixed by reinstalling the network drivers.

Some spyware can be removed with ordinary anti-virus software. However, specialized anti-spyware software such as Microsoft AntiSpyware, Ad-Aware, or Spybot Search & Destroy is usually more effective.

Understanding IP addresses

10.202.x.y is an address on the Atlantic wireless network. This is what you want.

169.x.y.z is a "link local" address. It shows up if you don't have a working network connection or can't reach a DHCP server. This may be caused by spyware.

10.128.x.y and 128.128.x.y are wired IP addresses. Make sure you are looking at the wireless interface. You may need to disable the wired interface.

Other IP addresses may show up if a host has been configured for another Internet site's network. Make sure it is set to use DHCP, then release and renew the DHCP lease.

DHCP

DHCP is a "link local" address. It shows up if your computer is not on a wired network and you have an 802.11b or 802.11a/g wireless card and its associated drivers installed.

Access points

Wireless network connectivity emanates from access points, special network devices also known as base stations, wireless hubs, or wireless routers. In order to use the wireless network, you need to be physically near an access point. For a list of access point locations, see:

http://www.whoi.edu/CIS/networking/wireless/access_points.html

If wireless coverage is poor in your area (you get low signal or get disconnected) please contact the Help Desk.

NetReg Wireless

All computers on WHOInet need to be registered with NetReg for wireless access: https://netreg.whoi.edu/bin/wireless.pl

VPN

VPN allows you to access the WHOI intranet from any Internet site. You can access the WHOI Web site, the WHOI Internal Web site, and connect to the VPN.

VPN client software, and learn more about VPN access, see:

http://www.whoi.edu/CIS/networking/remote_access/vpn/vpn.html

The WHOInet VPN

For security reasons, all network traffic from the Atlantic wireless network must go over the WHOInet VPN.

To register for a RAS/VPN account, download and configure VPN client software, and learn more about VPN access, see:

http://www.whoi.edu/CIS/networking/remote_access/vpn/vpn.html

Additional questions

1. Were you ever able to use the Atlantic network? With the same computer? In the same location? Do any computers currently work in your location?
2. What is the MAC address of the access point you are trying to use? Do other people nearby use Atlantic?
3. Does your wireless card support 802.11b/g or just 802.11b?
4. Do you have a personal firewall enabled?
5. Have you checked for spyware?