Wi-Fi Best Practices

One major interference source is unauthorized wireless devices, most commonly wireless routers. These devices can disrupt the service for neighboring wireless access points. They also pose a security risk and are in violation of acceptable use policy. The UPIKE ITS will detect and disable unauthorized wireless routers.

Since drivers can change, keep the drivers for your wireless card up to date. Having the latest driver ensures the best performance and user experience.

Keep Windows updated and run regular updates.

Make sure you are using antivirus software and run regular updates.

Make sure your firewall is on.

Make sure your computer is using the current date and time.

Cordless phones operate on many different frequencies. You can typically find out which frequency your phone uses by simply reading the labels. They include the following: 900MHz, 2.4GHz and 5.8GHz. A computer using Wi-Fi may have connection problems if anyone is using a 2.4GHz phone in the area.

Microwave ovens can also cause interference with Wi-Fi devices. If a computer within 10 feet of an operating microwave is experiencing slow connection, consider relocating one of the devices.

FAQ

Q: I have low signal strength, is this an issue.

A: Computer network cards can have problems filtering out interference and interpret the extra interference as low signal strength. Since our wireless system communicates with each other to avoid interfering with themselves, there is very little actual interference from the UPIKE wireless infrastructure. As long as internet speeds remain acceptable, the low signal strength should not be a problem. If you are getting low internet speed, check for the following common causes of interference:

- Personal wireless routers (prohibited)
- Wireless printers (disable the wireless)
- Microwaves
• Cordless phones (2.4 GHz)
• Personal wireless cameras
• MiFi and other signal boosters, or cell phone personal hot spots
• Bad electrical connections

Q: Who can get a wireless connection on campus?

A: All students, faculty and staff with a UPIKE account can access the campus wireless network.

Q: Why is a secure connection important?

A: The campus strongly recommends using an encrypted connection whenever possible. However, an unencrypted connection is available for residence hall devices that do not support Wi-Fi Protected Access 2 (WPA2) encryption and for gaming devices. Data transmitted “in the air” (i.e., to and from your computer and the access point) without encryption can be easily snooped and captured.

Q: What is WPA2?

A: Wi-Fi Protected Access 2 (WPA2) is a wireless standard of data encryption that allows for authentication and is more powerful than the Wired Equivalent Privacy (WEP) security standard.

Q: Will the UPIKE Wireless be available 24/7?

A: Yes. The wireless will be available 24/7 excluding scheduled maintenance.

Q: Do wireless frequencies pose health concerns?

A: The campus is not aware of any scientific consensus that low-power devices such as cell phones or laptops using wireless frequencies pose health risks to users. However, users should research this topic and make their own determination about the safety of using wireless devices.

Q: How fast will my wireless connection be?

A: Connection speeds of up to 300 mb/s are possible throughout most of the campus if the client is 802.11n compatible; although internet based traffic will not reach this speed. Connection rates will vary with type (802.11b/g/n), signal strength, and amount of usage on a particular access point.

Q: Is my computer protected from malicious software while using the Campus Wireless network?

A: The Campus Wireless network does not protect your machine from malicious software such as viruses, spyware, and cross-site scripting attacks. UPIKE’s network access control will scan to verify an antivirus is installed before allowing student connections. We strongly recommend that users maintain updated anti-virus software and safe computing practices.

Q: How is the campus dealing with rogue access points or ad hoc networks?

A: The campus wireless system monitors unauthorized wireless devices with sensors and systems to detect and classify them. The campus reserves the right to disable and remove unauthorized access points (rogue access points).