We cannot imagine a world without wireless access today. The connectivity it offers is priceless — allowing employees to work from just about anywhere, increasing productivity, mobility and convenience. With these advantages, however, come a security risk, though they can be easily managed by taking the following precautions:

1. **Change passwords** – Default passwords must be changed for all equipment. Create a strong password with 8 or more characters using numbers, upper and lower case letters, as well non-alphanumeric characters. All hardware comes with preset passwords, but many people don't take the time to change them. This makes it easy for hackers to get into corporate devices as default passwords can be easily found on the internet.
2. **Choose business class equipment –** Equipment made specifically for business use offers better security. Stick to a well-known brand and use WPA2 for wireless security.
3. **Separate corporate data from personal devices -** Many wifi routers allow multiple wireless networks. Creating separate networks for corporate data, personal devices, and guests makes it difficult for non-corporate users to access or corrupt your business's equipment and data.
4. **Keep all software up to date** – Hardware vendors periodically release firmware updates that provide security fixes for their devices when a flaw or security hole is found. Ignoring software updates gives intruders an easy way to access your equipment.
5. **Secure devices** – Keep corporate equipment out of reach or locked away. This helps prevent the power switch or reset button from being hit by mistake. Placing access points at a height not only keeps the equipment out of reach but also helps distribute better signal.
6. **Create a wireless policy** – Lay down ground rules for the use of your corporate wireless network. It's never too early to create and implement a wireless access policy to promote best practices.

Wireless security is vital and only one tool for keeping your corporate environment safe. Let us know what you would like to learn more about when it comes to using technology to help your business succeed. If you have any questions or comments, please reach out to us at info@misits.com or find me on twitter @jmlucien.