



## **Wireless Data Security: Best Practices for Researchers**

The downside of a wireless network is that, unless researchers take certain precautions, anyone with a wireless-ready computer can use their network. That means neighbors, competitors, passers-by, or even hackers lurking nearby, could “piggyback” on researchers' networks or access the information on their computers. Even if no data is stolen, unauthorized use of a researcher's network to commit a crime or send spam can be traced back to the researcher's account – and the researcher could be held liable. Also, these guidelines will be among the minimal standards expected by state and federal regulators.

1. **Use encryption.** The most effective way to secure a wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If a wireless router doesn't have an encryption feature, be sure to purchase one that does. And be sure to enable the encryption functions at the highest level.
2. **Use anti-virus and anti-spyware software, and a firewall.** Computers on a wireless network need the same protections as any computer connected to the Internet. Be sure to install anti-virus and anti-spyware software and a firewall, activate them, and ensure they are up-to-date.
3. **Turn off identifier broadcasting.** Most wireless routers have a mechanism called “identifier broadcasting,” which should be turned off. It sends out a signal to any device in the vicinity announcing its presence -- if a researcher/employee using the network already knows it is there, this broadcasting is unnecessary. Hackers can use identifier broadcasting to home in on vulnerable wireless networks.
4. **Change the identifier on a router from the default.** The identifier for a router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Hackers know the default IDs and can use them to try to access the network. Change the identifier to something only the owner knows, and remember to configure the same unique ID into a wireless router and a computer so they can communicate. Use a password that's at least 10 characters long: longer passwords are harder to break.
5. **Change a router's pre-set password for administration.** Hackers know the standard default passwords that allow someone to set up and operate routers. Change them to long passwords only the owner knows.
6. **Allow only specific computers to access researchers' wireless networks.** Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network.
7. **Turn off a wireless network when not in use.** Hackers cannot access a wireless router when it is off.
8. **Don't assume that public “hot spots” are secure.** Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use. Unless researchers can verify that such a “hot spot” has effective security measures in place, sending or receiving personally identifiable data over that network should be avoided.

### **More Information**

For more information on laws and best practices impacting research, contact MRA, and consider becoming a [member](#) to get free access to the [MRA Compliance Guide](#).