# Top 10 Security Tips for Churches

Our Director of Security (think physical security) ask me if I could put together 10 points for information security for an upcoming conference he is presenting at. These points are mainly for small churches without IT staff. I wasn't going to post them here as they're pretty basic, but as I wrote them I couldn't help but think how much improvement we could still make in some of these areas… I won't say which ones

Anyways… for what it's worth, here they are.

1. **Train employees not to give out personal information on attendees**
   Speaking Notes: Most breaches come through "Social Hacking". Someone calls the organization with a "good story" and the employee hands out proprietary information.
2. **Check what leaves the building through the trash**
   Speaking Note: All of the information security in the world is a waste when information can be printed, put in the office trash and then placed at the curb of the street.
3. **Limit access to servers and network equipment**
   Speaker Notes: The first layer of IT security starts at physical access. Servers and switches should be behind locked doors / cabinets.
4. **Implement password changes / sharing**
   Speaker Notes: Passwords should be required to change every 45 days and should not be shared with volunteers or other staff. Each person should have their own.
5. **Protect computers from viruses and spyware**
   Speaker Notes: Every server and computer on the network should have anti-virus / spyware software installed and up to date. This doesn't have to be expensive. Small churches can use AVG and Malware Bytes.
6. **WiFi networks should be protected**
   Speaker Notes: WiFi access points should be configured by someone familiar with the various types of encryption available. WiFi networks for use by attendees should not be on the same network as the office.
7. **Access to backups should be secured**
   Speaker Notes: Access to backup hard drives / tapes should be secured. A good off-site option is to use a safety deposit box at a bank.
8. **Laptops with attendee private information on the local drive should be encrypted**
   Speaker Notes: Computers with attendee information on them should have their hard drives encrypted. This is built into Windows 7 Ultimate, but other free tools exist like TrueCrypt.
9. **Educate volunteers on your information security practices**
   Speaker Notes: Anyone with access to attendee information should be instructed on the proper use of it. Never assume that they know right from wrong. There have been several cases where a volunteer has used the church's attendee information for their network marketing business and never thought twice about if it was right or wrong. It would be best to have them sign a documenting that they understand and agree to the policies and procedures. We call this the "Ministry Partner Form".
10. **Never feel like you're finished**
    Speaker Notes: These are the very basic of tips. Always realize that it takes work to keep up with these 9 items and there is always more that could be done.