Aardsma Archives *prepare well. protect well.*

Protect Computer Networks When Offering Free Wi-Fi

IT'S NOT FREE IF YOU GET RIPPED OFF

Free Wi-Fi has become commonplace in many venues, from coffee shops and bookstores to auto repair shops and laundromats. Now churches are providing the same service.

In order to safely provide free Wi-Fi, churches should protect their administrative computers, put passwords in place, and prevent

A few of the ways churches have begun to use wireless Internet include:

- Encouraging congregants to look up scripture on their smart phones, or even to tweet quotes from the sermon.
- Enabling guest speakers to use their iPads for sample photos and video clips.
- Enhancing church cafés. Offering free Wi-Fi can make church coffee shops more attractive to people in the community.

While free Wi-Fi provides many benefits, it also carries risk. For example:

- Unauthorized church members could access important financial or personal files.
- Users might illegally download music and videos.
- People from the community could park outside the church and use its free Wi-Fi to access immoral or illegal content.

In each of these situations, the church could be held accountable for what has happened on its network.

In order to safely provide free Wi-Fi, churches should protect their administrative computers, put passwords in place, and prevent illegal Internet usage on their network.

(Continued page 2)

Protect Admin Computers

Administrative computers often contain confidential information, like bank account numbers or information from counseling sessions. In the wrong hands, personally identifiable information can be used to steal the identities of the people who participate in your ministry.

To help protect the church's administrative computers and data, create a Wi-Fi network for guests that is separate from the network used by staff members. The guest network should only have access to the Internet.

Use Password Protection

A strong password makes for a safer network. Changing the password for administrative computers every six months decreases the likelihood of someone breaking into church files. Consider creating a password for the Wi-Fi network that you offer to church goers. Having a password also can help prevent people from accessing your Wi-Fi while they loiter nearby.

One way to keep the free wireless connection particularly secure is to change the password weekly. Some churches do this by announcing the new password each Sunday morning, and making it correlate with the sermon.

Develop an Internet Usage Policy

You or your church could be punished for what others do while utilizing your free wireless Internet connection. It's important to prevent members of the church and community from using the church's Internet connection illegally.

One way to help prevent illegal Internet usage is to require all visitors to agree to an Internet Usage Policy before using church Wi-Fi. Key terms in the policy could include:

- Prohibiting activities such as online bullying and harassment, accessing obscene or offensive content, online gambling, illegally downloading copyrighted content, and other actions that are not consistent with the Biblically-based beliefs of the ministry.
- Requiring an age minimum and parental supervision of minors. A contract or agreement that is signed by someone under the age of 18 is generally not enforceable.

(Continued page 3)

- Requiring visitors to use updated anti-virus software.
- Advising visitors to avoid sharing personal and sensitive information, such as credit card numbers, over the network.
- A “hold-harmless” clause that notifies the visitor that the church is not responsible for damage to the user’s electronic devices or software, or the loss or theft of personal information. Use of the wireless network is at the visitor’s own risk.

To put your Internet Usage Policy into effect, ask users to agree to follow the policy before allowing them to use church Wi-Fi. You could obtain agreements by:

1. Asking users to sign a paper agreement before giving them the Wi-Fi password.
2. Setting up a “login” page that automatically appears when users connect to the Wi-Fi network. The landing page can display your Internet Usage Policy and ask the user to accept by checking a box before allowing them to access other websites. Or, the page could clearly state that by using church Wi-Fi, users verify that they have read, understood, and agreed to follow the Internet Usage Policy. Instructions for setting up and personalizing landing pages can be found online, or you may want to ask a trusted, qualified information technology vendor to set up the page.

Use a Content Filter

A content filter is another measure that can help prevent illegal Internet use. OpenDNS, or similar software, can protect you and your ministry from liability by blocking websites that you don’t want people visiting while on the church’s Wi-Fi.

If you want to set up free Wi-Fi in a safe and secure way, and don’t know where to turn for help, Church IT Network has a live chat section on their website where churches can go to ask tech questions.

With preventative measures put in place, the growing trend of offering free Wi-Fi at church can continue to energize ministries. There’s no limit to the number of ways churches can use wireless Internet and handheld devices to spread the gospel message through their city, their country, and the world.