The Inherent Risk of Guest Wi-Fi Access at Your Church

By Lisa Traina, Partner

With the myriad of wireless devices in constant use, many churches provide Wi-Fi for the convenience of employees and guests. However, this complimentary benefit can come with a heavy price if security is taken for granted.

Unprotected guest networks can become a serious liability for churches if illegal or suspicious content is viewed or downloaded. After all, the church's name is on the Internet service provider bill that comes every month. **Policy enforcement is necessary.** Churches must ensure compliance with a lengthy list of laws and regulations, including new U.S. privacy laws, the EU's General Data Protection Regulation (GDPR), health and financial information confidentiality regulations, and the Child Internet Protection Act.

In addition, the right cybersecurity controls are extremely important when providing complimentary Wi-Fi service to employees or guests. Otherwise, that one networking asset can become a backdoor into your network for others. With the Internet of Things (IoT) in every workplace, and 24/7 online, enterprise, and small- and medium-sized business cloud data applications, Wi-Fi security needs to be one of the most essential network tasks, with continual monitoring.

Safeguards for a Church Guest Wi-Fi Network

There are two essential aspects to consider with guest Wi-Fi: **content management** and **controlled access.** We recommend these best practices:

1. Invest in an enterprise wireless router to protect your data. Many features in these routers are crucial to maintaining adequate security.

2. Use a separate router for guest Wi-Fi access. Keep guest access separate from your church's main network at all times.

3. Isolate IoT devices, such as thermostats, security cameras, and smart TVs, from your main network.

4. Configure the guest Wi-Fi to be on a completely different subnet (segregated) and use WPA2, a security protocol that uses encryption to secure networks.

5. Create users that have a basic timer schedule. If a guest needs Wi-Fi, give them access as a user with an appropriate time allowance. Configure guests using pre-configured provisioning templates that come with the router.

6. Specify bandwidth limitations and policies by individual user or group. Give as little bandwidth as possible per user account. Just enough for email is typically adequate.

7. If you have a large number of guests who need wireless access, create a user login portal. Most routers offer this along with pre-defined templates. Before they can access the Internet, users will need to login on this web page using a one-time password you provide.

   This will give your church more control over who is on the network and the activity taking place. You also can configure your portal template to automatically generate logs for each session, which provides a much-needed audit trail for each user. These logs can be essential in incident response if a data breach is discovered.

8. If you have a smaller number of guest Wi-Fi users, consider a guest access option that you can turn off when not in use. Some consumer routers include this option to make it easy to create guest networks. If you

Keep guest access separate from your church's main network at all times.

use this, be aware that some router models will automatically make a separate guest network with an open Wi-Fi.

9. If you use Windows 10, turn off Wi-Fi Sense. This feature makes it all too easy to accidentally share a Wi-Fi password.

In addition, every church should filter all Internet traffic (wireless or not) to block file sharing and access to pornographic and suspicious websites.

If your church offers guest Wi-Fi, take the steps above to tighten your security. And if your church doesn't need a guest network, do not create one. **No one can hack into a network that doesn't exist**, and it will give you one less thing to worry about.

This article first appeared on XPastor.org.

If you have a smaller number of guest Wi-Fi users, consider a guest access option that you can turn off when not in use.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA