FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Best Practices for Securing Your Router / Wi-Fi

Setting up your router / Wi-Fi router to optimize privacy and cybersecurity is a good practice. This product will provide you with the minimum fundamental steps that can be taken to protect from network from unnecessary cybersecurity risks.

Did You know?

If you don't secure your Wi-Fi network, cyber threat actors can perform a number of operations that are detrimental to your privacy and security.

Here are some basic tips on securing the Router/Wi-Fi at your congregation (and at home):

1. **Always Change your default router login credentials**: When you set up a new router (or if you never changed the default on your current router) make sure to change the default username and password to something strong and unique.
2. **Enable WPA2 or WPA3 encryption**: WPA2 (Wi-Fi Protected Access 2) and WPA3 are the most secure encryption protocols currently available for wireless networks. By enabling these protocols on your router, you can further secure your Wi-Fi traffic.
3. **Use a strong, unique Wi-Fi password**: Create a strong, unique password for your Wi-Fi network that includes a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using common words or phrases that can be easily guessed and try to have a password length of at least 8-12 characters.
4. **Disable remote administration**: Many routers have a remote administration feature that allows you to access the router's settings from outside your network. Unless you truly need the ability to access your Router remotely, it's best to disable it to prevent potential unauthorized access.
5. **Keep your router firmware updated**: Router manufacturers regularly release firmware updates to address security vulnerabilities and improve performance. Many people overlook this but hackers search for vulnerable routers to gain access to your network. Check for updates regularly and install them as soon as they become available.
6. **Use a guest network for your parishioners**: If your router supports it, enable the guest network feature and provide the guest network credentials to your parishioners and visitors instead of your main Wi-Fi password. This way, your main network remains more secure.
7. **Enable firewall protection**: Most modern routers have built-in firewall protection. Enable this feature to help block unauthorized access to your network from the internet. If you have an older router, think about upgrading to a newer model with a built-in firewall.
8. **Disable WPS** (Wi-Fi Protected Setup): WPS is a feature that allows devices to connect to your network with a simple button push or PIN code. However, it can be exploited by attackers, so it's generally safer to disable it unless you need it. A new vulnerability was just released which allows hackers easy access to your network via WPS.
9. **Consider using a VPN**: If your House of Worship needs an extra layer of security, consider using a virtual private network (VPN) for your internet connection. A VPN encrypts your internet traffic, making it more difficult for others to intercept or monitor your online activities.

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Parting Thoughts and Ideas.

- Store your router / Wi-Fi in a secure physical location.
- If your router / Wi-Fi has a “Guest” Wi-Fi option, consider enabling it.
- Avoid using personal information in your Wi-Fi name.
- If you need assistance, you can:
  - Ask your local tech guru.
  - Post a question in the FB-ISAO Slack general or ask-me-anything channels.

This product was developed by the FB-ISAO Cyber Threat Intelligence Working Group.
Get involved! Write to membership@faithbased-isao.org.