Cybercrime is a reality for everyone who uses the internet and who stores vital data online. Hackers are continually looking for secret information they can leverage for money or other gain from data owners. You may have thought your church does not have data to attract cybercriminals; however, it does! The cybersecurity of your church is paramount and deserves your attention.

Hackers eagerly wait to sink their cyber claws into churches because they're a goldmine of data — information such as donors' personal contact information and offering records. Some hackers want to hijack your website and post obscene content, while others want to siphon finances from your online giving platform.

When your website or data center has a weakness, hackers know how to exploit it for easy access. They use different ways to access your data, for example, installing malware on your computers, decoding passwords for your online accounts, impersonating pastors in emails sent to the accounts department, fake credit card fraud alerts via email, and the list is endless.

Your church network may be secure, but it only takes one person to compromise the system and cause a cyber-breach. Churches often rely on outside financing to run and generally do not have large budgets to get sophisticated equipment as corporations do. Therefore, it is essential to know how to protect your network without breaking the bank.

The following are measures you can take to secure your church network against cybercrime:

1. Train your staff and volunteers. Your team must take personal responsibility for ensuring they protect the church's network from their point of access. Inform them of the dangers of visiting unsafe websites, responding to fake emails requiring personal details, or sharing passwords. Your staff's password should be THEIR password. Tell them not to share their password with any other staff member.

2. Use authentication controls. The use of strong or complex passwords is encouraged. For access to your "cloud" applications, a two-factor authentication process adds a layer of security. Some services require two methods to login, such as a password and text message with a unique one-time number to key in the required field.

3. Place restrictions on WiFi. If your church offers WiFi to members and visitors, you can segregate its access according to different groups. The Guest WiFi provided by the church should only provide internet access. Anyone using the Guest WiFi should NOT have access to technology for the staff, such as computers, files, and copiers.

4. Monitor your system. Have a knowledgeable IT person analyze the computer network for any potential security risks.

5. Update your software. I am sure you have seen a pop-up message on your computer asking you to update your software. Many times, people ignore this message or opt for “remind me later.” Depending on the configuration of your computers, these messages may be prompts to update the applications on your computer for added security. Confirm with your IT department that they are intentional about keeping your computers updated with the necessary security updates.

6. Backup your data. Always have a backup of your data to ensure you can access it in case of any unfortunate loss of data. If hackers get into your network and delete your records, you should still be able to get your data back if you have it backed up. We recommend both a local back to external hard drives as well as cloud-based backups. That way, you are protected both ways. With modern technology and faster internet speeds, cloud backups are an easy and affordable backup solution.

While this list is not all-inclusive, it is an excellent start toward protecting your church. If you are concerned about your cybersecurity, please reach out to us at https://www.MinistryCraft.com. It is possible to stay online and safe.