

Cybersecurity & AI: What Every Church Should Know in Today's Digital World

How to protect your ministry as technology and threats evolve. Featuring Insurance Board's Technology Team

In today's digital age, churches are more connected than ever. Sunday sermons are streamed online. Tithes are given through apps. Events are organized via email and social media.

It's an incredible way to reach people where they are — but it also opens the door to new risks. As more of church life moves online, two big topics are becoming increasingly important: cybersecurity and artificial intelligence (AI).

Don't worry — you don't need to be a tech expert. This article is designed to explain what these terms mean, why they matter to churches, and what simple steps you can take to stay safe.

What Is Cybersecurity?

Cybersecurity is just a fancy word for protecting your church's digital information. Think of it like locking the church building — but for your emails, online donations, livestreams, and digital records. It helps prevent things like:

- ◇ Identity theft
- ◇ Email scams
- ◇ Website hacks
- ◇ Unauthorized access to member data

Why Are Churches Targeted?

You might not think of your church as a target — but unfortunately, many cybercriminals do.

Here's why:

- ◇ Churches store personal data, like names, emails, and donation history.
- ◇ Many churches have limited tech support, which makes them easier to exploit.
- ◇ Their open, trusting nature can make it easier for scammers to manipulate staff or volunteers.

Did You Know?

- ◇ In 2024, nonprofits experienced a 30% increase in cyberattacks, with over 1,600 attacks each week.
- ◇ 68% of data breaches involved human error — like clicking a phishing email.
- ◇ 32% of attacks happened because software wasn't kept up to date.

(Source: BDO & CyberPeace Institute Reports, 2025)

What About AI? Is It Helping or Hurting?

Artificial Intelligence (AI) is everywhere — even in church life. AI can be a blessing, but it can also be misused.

How Churches Use AI for Good:

- ◇ Spam filters: Automatically detect and block scam emails.
- ◇ Fraud alerts: Some donation platforms use AI to catch unusual transactions.
- ◇ Chatbots: Help answer basic questions on your website, even outside office hours.

But There Are Risks:

- ◇ AI-generated scams: Attackers now use AI to write convincing phishing emails.
- ◇ Deepfakes: Fake videos or audio that sound like someone you know.
- ◇ Targeted attacks: AI tools can scan your website and social media to learn how to trick your team.

Simple Steps to Protect Your Church

You don't need a tech team to be smart about cybersecurity. Here are easy, practical steps you can start today:

- ◇ Use strong, unique passwords
- ◇ Avoid short, common passwords. Consider using a password manager.
- ◇ Turn on two-factor authentication (2FA)

Cybersecurity & AI: What Every Church Should Know in Today's Digital World

How to protect your ministry as technology and threats evolve. Featuring Insurance Board's Technology Team

- ◇ Add an extra layer of security to logins with a text or app code.
- ◇ Train your staff and volunteers
- ◇ Teach them how to recognize suspicious emails and websites.
- ◇ Keep everything updated
- ◇ Updates often include important security patches. Don't skip them.
- ◇ Back up your data regularly
- ◇ Save copies of critical files in a secure cloud or offline location.

Final Thoughts

Your church already protects what matters — its people, its message, its resources. Cybersecurity is simply an extension of that in the digital world.

You don't have to fear technology. With a little awareness and some thoughtful planning, your church can use digital tools confidently and responsibly.

Whether you're the pastor, administrator, or the person who updates the church's Facebook page, your role in cybersecurity matters. And the good news is, you're not alone. There are simple, affordable ways to stay safe and keep your ministry moving forward.

This communication, along with any attachment, does not amend, extend or alter the coverage terms, exclusions, and conditions of insurance policies referenced herein. Policy language is controlling and supersedes. Guidance provided by the Insurance Board does not constitute legal advice; please seek the advice of an attorney if you wish to obtain legal advice.

Agent Corner



Michael Campbell, MinistrySure Agency

AI in Ministry: Opportunities, Risks, and the Need for a Cyber Strategy

In recent conversations with churches, I'm hearing more about Artificial Intelligence (AI)—not as a distant trend, but as a tool pastors, administrators, and volunteers are already using. From drafting newsletters and creating sermon visuals to organizing membership records, AI can help ministries accomplish more with limited time and resources.

The benefits are real—but so are the risks. Concerns about accuracy, bias, and the privacy of sensitive member or donor data are growing. Even more concerning is the rise of AI-enabled scams: emails or text messages that mimic a trusted leader's tone perfectly, deepfake videos that look real, and automated phishing campaigns that are harder than ever to detect.

That's why I encourage every ministry to go beyond simply "using" AI and instead develop a cyber/data strategy. This includes:

- **Setting clear policies** for what information AI tools are allowed to access.
- **Training staff and volunteers** to verify unusual or urgent requests before responding.
- **Keeping systems updated** and limiting access to sensitive data.
- **Pairing strong practices with cyber liability insurance** to help your ministry recover if a breach occurs.

As an agent, I've seen AI make my own work faster and more efficient—but I never skip the human review step. With the right safeguards and insurance coverage, churches can embrace AI's potential while protecting their people, their data, and their mission.