Security Briefs 040 – AI Security Challenges Part 2

Information Security and Data Exposure

We are continuing our series on AI and security challenges. Today we will talk about information security.

When you type something into an AI chatbot, it may feel private. But in many cases, it isn't. Conversations may be logged, stored, or even used to train future models.

Earlier this year, a medical transcriptionist entered patient details into a chatbot to "help" summarize notes. The tool polished the language, but in the process, highly sensitive health information was exposed outside the hospital system. That single action created legal risks, privacy violations, and a loss of trust.

For ministry workers, the risk is just as real. Imagine entering names of local believers to improve a newsletter draft. Or pasting donor records to make a thank-you letter sound smoother. If that information is stored by the AI platform, it's no longer yours to control.

The rule of thumb is simple: if you wouldn't put it on a postcard, don't put it into AI. Postcards can be read by anyone along the way — and once the message leaves your hands, you can't take it back.

So be disciplined. Avoid sharing real names, locations, or strategies. If you must use AI, strip out identifiers and keep it generic. Assume everything you type may one day be visible to others.

AI can be helpful. But careless inputs can expose the very people you are called to protect.

Now you know.

In our next episode, we'll look at operational security — how adversaries can misuse AI to deceive and manipulate.

Episode Summary

This episode focuses on information security, with an example from the medical field where AI use exposed sensitive data. It explains why typing private details into chatbots is like writing on a postcard and offers practical guidelines to anonymize or avoid risky inputs.