Security Briefs – AI Security Challenges Series

Security Briefs 039 – AI Security Challenges Part 1

Introduction to AI Security Risks

Welcome to the beginning of our second series on Artificial Intelligence, or AI.

Artificial intelligence is becoming part of everyday life. For many, it feels exciting — even liberating. But AI is a tool, and like any tool, it can be used for both good and harm.

Think about the printing press. When it was invented, it made the Bible more widely available — a tremendous gift. But it also spread heresies and propaganda. The same tool carried both blessing and danger. AI works in much the same way: it amplifies whatever we put into it.

For global workers, this means we cannot treat AI as neutral. What happens if sensitive prayer requests are entered into a chatbot? What if travel or ministry strategies end up in a system you don't control? And beyond the technical issues, what happens if we begin to lean on AI in place of prayer, discernment, or community?

In this series, we'll talk about three areas of risk: Information Security, Operational Security, and Spiritual Security. Information security deals with protecting data from exposure. Operational security asks how adversaries might misuse AI. And spiritual security asks how reliance on AI shapes our hearts.

As we begin, remember: every tool shapes the user. The question is, are we being shaped toward wisdom and worship, or toward exposure and dependency?

Now you know.

In our next episode, we'll look more closely at the first challenge: information security.

Episode Summary

This episode introduces the series on AI security challenges with the illustration of the printing press, showing how new tools can be used for both good and harm. We highlight three areas of concern — information, operational, and spiritual security — and ask whether AI is shaping us toward wisdom or dependency.

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.

Security Briefs 041 – AI Security Challenges Part 3

Operational Security and Manipulation

Welcome back. In this episode of our series on AI Security Challenges, we will talk about Operational Security.

AI doesn't just threaten information we put into it. It also creates new risks when adversaries use it against us.

One of the fastest-growing threats is phishing. AI can generate emails that are free of spelling mistakes, formatted professionally, and tailored to look like they came from someone you know. A team member receives an urgent message from "you," asking them to forward sensitive files. It looks convincing — but it's a trap.

Another danger is deepfakes — videos or audio clips that look and sound real but are entirely fabricated. These tools are already being used in scams. Imagine a video surfacing online of a pastor saying something inflammatory. The video is fake, but by the time the truth comes out, the damage is done.

In conflict zones, false news created by AI has already sparked fear and division. In one example, images of an explosion were generated by AI and circulated as real events, triggering panic before authorities could clarify.

The problem isn't just what AI can create — it's our tendency to trust it. If we lean on AI for crisis updates or quick decisions, we may be deceived. Operational security requires layered verification: check sources, confirm through trusted human channels, and resist the temptation to take AI-generated information at face value.

AI can multiply our reach — but it can also multiply our vulnerability.

Now you know.

In our next episode, we'll explore another angle: privacy and identity risks when personal information is misused by AI.

Episode Summary

This episode highlights operational risks of AI, focusing on phishing, deepfakes, and disinformation. Real-world examples show how AI-generated content spreads faster than corrections. We emphasize layered verification and resisting the temptation to outsource decisions to machines.

Security Briefs 042 – AI Security Challenges Part 4

Privacy, Identity, and Misuse of Personal Information

Welcome back to our series on AI Security Challenges. Today we'll discuss AI and privacy issues.

AI systems are trained on massive amounts of online data — much of it scraped without permission. That means your photos, sermons, or social media posts could already be fueling someone else's model.

This creates serious risks of impersonation. We're now seeing AI-generated phone calls that mimic the voice of family members. In one case, a scammer used a cloned voice of a CEO to trick a company into wiring millions of dollars. For global workers, it could be the voice of a spouse, teammate, or supervisor.

Deepfake videos are another risk. Pastors and leaders have had their likenesses faked to spread false messages. These videos can circulate quickly, sowing doubt and suspicion. Even if they're eventually disproven, reputations may never fully recover.

For ministry teams, the question is urgent: could your voice, your image, or your words be twisted and used against you? Sadly, the answer is yes. That's why protecting privacy isn't optional anymore — it's a frontline of security.

Here are some practical steps:

- Enable multi-factor authentication on accounts.
- Be cautious with photos and posts.
- Work as a team to establish verification protocols, such as safe words or secondary channels, so you know when a message is real.

The fewer open doors you leave, the harder it is for adversaries to exploit your identity.

Now you know.

In our next episode, we'll widen the lens to look at spiritual and ethical risks of relying on AI.

Episode Summary

This episode explores privacy and identity dangers in the AI age, from cloned voices to deepfake impersonations. We highlight the need for multi-factor authentication, cautious sharing, and agreed team verification protocols to protect against exploitation.

Security Briefs 043 – AI Security Challenges Part 5

Spiritual and Ethical Risks

Welcome back. By now you know that AI isn't just a technical issue. It shapes how we think, trust, and even pray.

One danger is dependency — leaning on AI for comfort, guidance, or even companionship. In recent months, people have described AI chatbots as "friends" or "partners." Some have even held mock weddings with their bots. But these simulations cannot love, covenant, or sacrifice. They offer a counterfeit intimacy that can quietly replace real community.

Another danger is idolatry of efficiency. When speed and productivity become our highest values, we risk trusting the tool instead of the Spirit. AI can draft a sermon outline in seconds, but if it replaces prayerful reflection and study, then we've lost something essential.

AI also shapes discipleship by default. What we normalize in our personal lives will ripple outward. If our teams see us leaning on AI for wisdom or comfort, they may follow our example — for better or worse.

The call is simple: stay rooted in God's Word, in prayer, and in the fellowship of His people. Let AI be a tool, not a teacher. Let Christ remain the center of our trust.

Now you know.

In our next episode, we'll wrap up this series with a framework for wise use.

Episode Summary

This episode focuses on spiritual and ethical risks, such as dependency on chatbots and idolizing efficiency. It highlights how AI can quietly reshape discipleship if unchecked. We emphasize staying rooted in prayer, Scripture, and community while resisting counterfeit intimacy.

Security Briefs 044 – AI Security Challenges Part 6

A Framework for Wise Use

We've explored the risks of AI: information security, operational manipulation, privacy threats, and spiritual dangers. Now let's tie it all together.

Here are five guiding principles for wise AI use in ministry:

1. Protect sensitive data — never feed names, strategies, or donor info into AI tools.
2. Verify, don't assume — always confirm AI outputs with trusted human sources.
3. Guard identity and privacy — strengthen authentication and limit oversharing.
4. Stay rooted in community — let accountability and fellowship guide your decisions.
5. Keep worship at the center — if AI doesn't lead you toward Christ, it may be leading you away.

Here's an illustration. A ministry team decided to use AI to help draft communication. But before long, they found themselves relying on it for every message — even prayer updates. The words looked polished, but they no longer reflected their hearts. Once they recognized the drift, they scaled back and returned to writing together in prayer, allowing AI only to help with formatting. That shift restored both authenticity and integrity.

The lesson is simple: AI can serve us, but it must never master us. Used with vigilance and faith, it can amplify our mission. Used carelessly, it can compromise it.

Now you know.

In our next series, we'll turn to another pressing challenge facing global workers.

Episode Summary

This episode concludes the series with five guiding principles for wise AI use and an illustration of a team that drifted into over-reliance. It reinforces the message: AI is a tool, powerful but not ultimate, and must be kept under the lordship of Christ.