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.