# Security Briefs: Secure Connections – Episode 049

## Bonus Episode: Social Media and the Illusion of Security

### Introduction

Today on Security Briefs, we are continuing our conversation about social media — but this time, we're going a little deeper. There is a lot to say about social media and so I decided to do a special bonus episode on using social media as a secure connection platform.

In our last episode, we talked about location tags, timelines, and unintended exposure. Today, we need to talk about something more subtle. And that is the **illusion of security.**

Many of us assume that because something feels private… it is private. Because something says "secure"… it is secure. Because we changed a few letters in a word… it is hidden.

But technology has evolved. And in some parts of the world, the entities monitoring communication are not amateurs. So today, we're going to talk about technical misconceptions — and why wisdom must grow with technology.

### The Missionary Side

**First,** to our missionary friends. Let's talk about **"private" Facebook groups** and other similar social media platforms. Understand that "Private" does not mean invisible. It means limited membership. But screenshots can be taken. Members can copy content. Accounts can be compromised. Platforms can change privacy policies.

Nothing posted on a major platform should be assumed confidential.

**Second,** encrypted does not mean invincible. Some communication apps offer end-to-end encryption, and that is helpful. But security is never just about the platform. It includes device security, account security, password strength, phishing awareness, and who is on the other end of the conversation.

**Third,** let's address something many of us have done – or perhaps still do. Replacing letters. In earlier days of communication, we wrote things in our updates like:

- Pr@y
- G0d
- Mi55ionary

At one time, this may have bypassed simple keyword filters. Today, automated systems — including and especially those used by nation states — can easily recognize contextual spelling variations. Pattern recognition has far surpassed basic word filters. Changing vowels is not a security strategy.

If you are operating in a restricted environment, assume that sophisticated monitoring may exist. Security today requires layered thinking — not clever spelling.

And remember: the most secure information is information that was never transmitted in the first place.

## The Supporter Side

Now, to our supporters and churches. You may assume that a "private prayer group" online is secure. It may feel that way. But if it is hosted on a public platform, it is not fully private. Members may unknowingly share content outside the group. Accounts can be hacked. Screenshots travel quickly. So here are a few guardrails:

- Avoid posting specific locations, names, or travel plans in online prayer groups.
- If something is marked confidential, treat it as if it could eventually become public.
- And resist the temptation to use creative spelling to "hide" sensitive words. That practice may give a false sense of security.

Instead, if something is sensitive, communicate it through the appropriate channel — or not at all. Wisdom is not about being paranoid. It is about being realistic.

I helped one Ministry Network create a directory for all the missionaries (global and local) that are sent out by that Network. They adopted a policy that would only send digital copies of this directory to people who specifically requested it and with a password specific to them. In that way, even if it was inadvertently forwarded – it was less likely to end up "out there" in the wild.

## The Shared Principle

Psalm 20 says, "Some trust in chariots and some in horses…" Today, we might say, "Some trust in platforms and privacy settings." But ultimate security is not found in technology. Technology is a tool. And tools must be used wisely.

Secure connection requires maturity — not fear. It requires recognizing that the digital world is not neutral and adjusting accordingly. As technology advances, so must our discernment.

## Practical Takeaways

**Missionaries:** Review your communication assumptions. Ask yourself: Am I relying on platform privacy rather than layered security? And where possible, reduce digital exposure rather than trying to disguise it.

**Supporters:** Treat every online space as semi-public. If something is sensitive, ask whether it should be posted at all. Security is rarely about clever tricks. It is about wise habits. And wise habits protect people.

Now you know.

We'll see you next time as we continue to talk about Secure Connections.