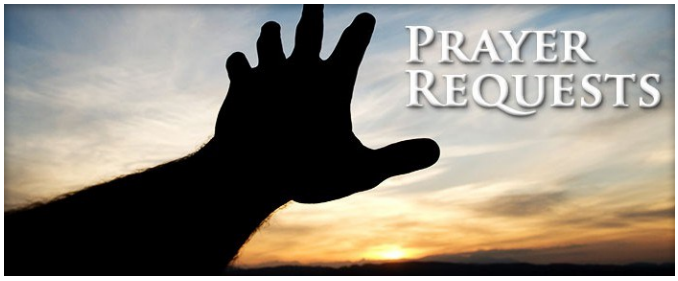
How to Communicate Safely and Securely with Deployed Ministry Teams

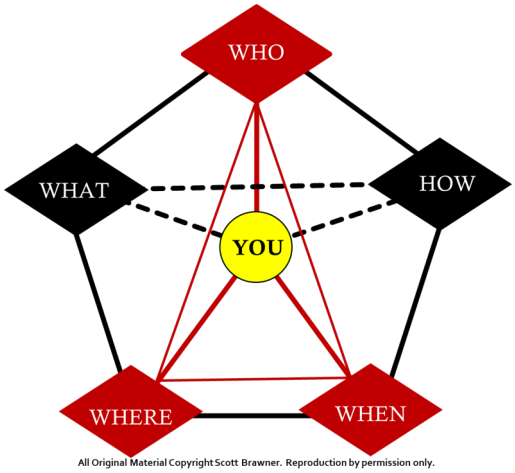
Many missionaries and gospel workers have been forced to return home because either they, or their families and supporters revealed too much information about their work in a security-sensitive location. The unfortunate release of sensitive information can have a catastrophic impact on the field, including team members and local partners. So how should someone communicate safely to and from the field? Here are a few ideas:

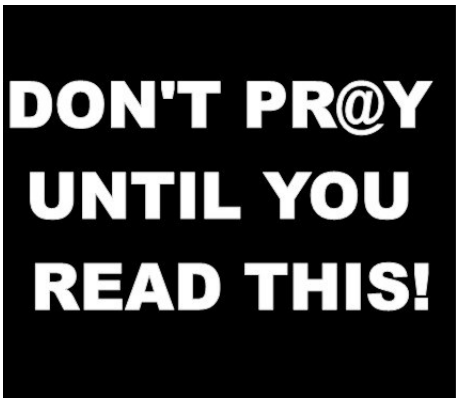
1. You are your own gatekeeper—remember that. When it comes to information security, protection begins with YOU! You are responsible for what you put into your correspondence. Don't depend on a firewall, VPN or email encryption to protect you. Be smart about what you put into your communications. You can never say enough how you love someone, or be in trouble for encouraging someone to grow in love. Focus on that. The specifics of who, where, when, why, and how can wait until you speak in person.



2. Keep prayer requests and updates personal enough to connect, yet general enough to protect. We cannot say it enough how important prayer is for gospel workers! That said, be very careful placing too much information into those prayer requests and updates. Ask yourself: Is the info that I'm communicating necessary? If you wouldn't say it quietly a crowded room, don't publish it either!

3. Avoid "connecting the dots of the *Vulnerability Pentagon* on social media. The Vulnerability Pentagon consists first of a *Vulnerability Triangle* of "who," "where" and "when." Also, be careful how you communicate about "what" you are doing and "how" you are doing it. These two areas can get gospel workers into hot water faster than the *Vulnerability Triangle*. The dots are connected by both physical and electronic means, especially in social media. From email prayer requests that get forwarded, to text messages and other messenger apps that are monitored, to paper trails such as itineraries and ministry materials that get left laying around, it is very important to protect critical information from those who would use it against your kids.





4. Don't even think that Christian "monikers" protect you. If you are involved at all with international missions or missionaries, you have probably seen at least once well intended missionary use a moniker or other "code words" to and try and obscure what they are saying in email. Guess what: it doesn't work. When communicating via email, texts, or other messenger apps out there, monikers and code words like pr@y, ch*rch, "Talk to Father," etc. don't protect anyone. Moreover, many governments have filters that are looking for these very words! Remember, if someone is sophisticated enough to monitor your communications, they are smart enough to know that "yarp" is just pray spelled backward….

CONCILIUM