Security Briefs 29 – Practical Digital Habits for Cross-Cultural Workers

Introduction

In our last two episodes, we introduced the concept of Digital SIR—how the principles of Legitimacy, Awareness, and Respect apply to your online life.

Today, we'll go one step further and get practical.

We'll walk through some digital habits that can help you live securely, serve wisely, and protect both yourself and others in our connected world.

Whether you're in a high-risk environment or a low-risk one, these habits matter.

If you download the transcript of today's episode, we have also provided a checklist of all the habits we have covered today along with some links to some good online resources that can help you better understand these digital habits.

Habit 1: Audit Your Digital Footprint

Start by reviewing what's already online.

- What do your social media bios say?
- What photos are publicly visible?
- Are you tagged in posts that might raise questions?

If your online identity doesn't match your real-world role, fix it now—before someone else raises the question.

Make sure your online presence supports your Short Truthful Statement, not undermines it.

Habit 2: Use Secure Communication Tools

Not all apps are equal when it comes to privacy.

We recommend using end-to-end encrypted messaging apps like Signal or WhatsApp for sensitive conversations.

Avoid discussing ministry details over email or unencrypted messaging apps unless absolutely necessary. And don't assume that "private" social media messages are actually private.

Habit 3: Control Your Sharing Settings

Set your default mindset to “private first.”

- Turn off geolocation for photos and posts.
- Don’t share where you are in real time.
- Avoid tagging others—especially national believers or local workers—unless you’ve asked their permission. One careless photo or comment can do real harm.

Habit 4: Think Before You Post

This is about more than safety—it’s about your witness.

Ask yourself:

- Does this post build bridges or create barriers?
- Is this encouraging, honorable, and culturally appropriate?
- Would I say this publicly in my host country?

Also, delay posting about events, trips, or ministry until after they’ve happened—or don’t post at all.

Habit 5: Train Your Team and Family

You may be careful—but is your team?

Make sure everyone you serve with understands your digital security standards, including interns, visiting teams, and family members. This includes:

- What’s safe to share
- What language to use
- What platforms are appropriate

One careless post from a teammate can undo years of careful relationship-building.

Conclusion

Now you know: Good digital habits aren’t about paranoia—they’re about intentionality.

When you align your digital life with your values, your mission, and your security needs, you’re not just protecting yourself—you’re honoring the people around you. So take a few minutes this week to do a digital checkup. It might be one of the most important things you do for your witness and your work.

We’ll see you next time.

Checklist: Practical Digital Habits for Cross-Cultural Workers

☑ Habit 1: Audit Your Digital Footprint

- Search for your name, email addresses, and usernames in incognito mode to see what's publicly available.
- Review your social media profiles for outdated or sensitive information.
- Remove or update content that doesn't align with your current role or values.
- Set up Google Alerts for your name to monitor new mentions.

Resources:

How to Audit Your Digital Footprint: https://career-advice.jobs.ac.uk/jobseeking-and-interview-tips/how-to-audit-your-digital-footprint/

3 Ways to Audit Your Digital Footprint: https://www.linkedin.com/pulse/how-audit-your-digital-footprint-3-easy-steps-gail-hopkins

Habit 2: Use Secure Communication Tools

- Use messaging apps with end-to-end encryption like Signal or WhatsApp for sensitive communications.
- Avoid discussing confidential information over unencrypted channels.
- Regularly update your communication apps to the latest versions.

Resources:

How to Communicate Securely on Your Mobile Device – CISA: https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device

Secure Messaging Apps Comparison: https://www.securemessagingapps.com/

Habit 3: Control Your Sharing Settings

- Review and adjust privacy settings on all social media platforms.
- Turn off location sharing for posts and photos.
- Be cautious about tagging others, especially in sensitive contexts.

Resources:

Manage Your Privacy Settings – National Cybersecurity Alliance: https://www.staysafeonline.org/articles/manage-your-privacy-settings

How to Manage Your Privacy Settings on Social Media (Experian): https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/

🤔 Habit 4: Think Before You Post

- Consider the cultural and political context of your audience before sharing content.
- Avoid posting in real-time about your location or activities.
- Reflect on whether your post could be misunderstood or cause harm.

Resources:

Think Before You Post – Eastern Michigan University: https://www.emich.edu/it/security/cyber-security-awareness/think-before-you-post.php

Think Before You Post – Total Defense: https://www.totaldefense.com/security-blog/think-before-you-post-protecting-your-digital-footprint/

👥 Habit 5: Train Your Team and Family

- Educate team members and family about digital security best practices.
- Establish clear guidelines for online communication and content sharing.
- Regularly review and update your digital security policies together.