abwe

Digital Security Guidelines

THE WORLD IS CHANGING. WE RECOMMEND THESE GUIDELINES FOR **EVERY** WORKER—NOT JUST THOSE IN RESTRICTED FIELDS.

WHY? You may travel to a restricted access country, or talk with partners in sensitive areas

» God may lead you to work in a restricted access country in the future

» You are part of a team, and your actions impact other team members and partners

more on p 2

Use Secure Communication *p 3-4*

- We recommend the Signal app for text messages and phone calls for ministry.
- If in a closed country, use "code words" instead of religious words.
- Do not criticize foreign governments or your host country.

Have a Clean Online Presence *p 5*

- Your ministry should never be linked to your name in a Google search.
- If you're not currently in a closed country, there are ways you can maintain a web presence that doesn't appear in Google.

Be Wise with Social Media *p 6-7*

- Nothing about your ministry should be **publicly** visible (to those who are not your friends).
- Approve friends carefully.

These guidelines may apply differently to you. Talk to your Executive Director.

Use a VPN *p 8*

- We recommend NordVPN, and have discounted rates for all team members.
- You should use a VPN anytime you're in another country, or anytime you're on a Wi-Fi network that is not your home or work.

Protect Digital Files *p 9*

- Sharing pictures or documents can put partners or team members at risk.
- When traveling or living in restricted countries, do not have unencrypted data stored locally on your phone or laptop.

NEVER Reuse a Password

- Weak and reused passwords are the number one way that digital accounts are compromised.

ALWAYS Use 2FA

Two Factor Authentication adds additional security to any login you have, from banking, email, and even social media

Ultimate security is found in Jesus, not in a list of best practices.

DIGITAL SECURITY GUIDELINES

Why These Guidelines

The world is rapidly changing, and those hostile to the gospel use technology as their primary tool to identify believers. From hacking, cyber tracking, or even Googling, technology is an easy tool to target unsuspecting people who are careless with their digital activity.

The goal is to give you principles to protect yourself, your team, and your partners—while still allowing you to build your support team and share how God is working through you.

▶ **One of the greatest risks to missionaries is having poor digital habits, which can lead to being arrested or expelled.**

The guidelines in the following pages are not meant to be all-inclusive, but are meant to be a framework and starting point for you to assess your own digital security.

Use Common Sense Digital Discernment

☑ *DO...*

- Use strong passwords, and don't reuse passwords for different sites.
- Keep your Operating Systems up to date with any software patches that are released.
- Keep your laptop and phone locked when not with you.
- If in doubt, ask the leadership team for guidance.

✕ *DON'T...*

- Don't open or interact with suspicious emails.
- Don't plug thumb drives into your laptop if you don't know and trust the source.
- Don't use public phone charging stations.
- Don't share team or partner details to unsolicited strangers.
- Don't check your "work" email in sensitive countries without a VPN.

If you are ever unsure or uneasy about something related to digital security, ask your Executive Director. Your team members and leadership would love to help.

1 Use Secure Communication

Part 1: Use Secure Apps

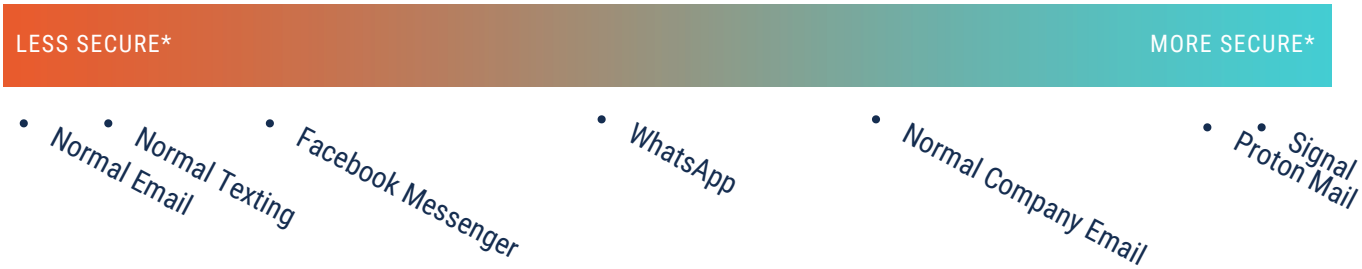
Governments or even just other apps can easily intercept some forms of communication (like text messaging). When you're messaging with other people, the goal is that the messages are only read by you and those you intend.

When approaching communication, it is not as simple as "secure" or "not secure." Rather, it is varying shades and degrees of security and safety. These levels are impacted by the app you're using, your country, and other factors.

Normal texting is one of the least secure ways of communicating. We recommend using the Signal app for messaging with other team members.

Email is only as secure as the other person receiving it. In general, assume that email is not secure.

> **"Email is the easiest to spy on."**
> -Micah Lee, Director of Information Security for the Intercept



**Many factors impact whether something is secure or not secure. This is not meant to be a definitive guide to the security or quality of apps, but rather it highlights that while it may be equally easy to send messages to others using any of these methods, it's not equally secure.*

IF YOU LIVE OR PRIMARILY WORK IN A "SAFE" COUNTRY

- Using encrypted or secure communication may not be a huge concern for you, but it could be for the recipient.
- Even if you aren't messaging WITH someone in a restricted access country, messaging ABOUT someone in a restricted access country could still put that person at risk.

1 Use Secure Communication

Part 2: Change your vocabulary

Since government actors have the ability to access our messages, it's wise to use language that does not raise alarms.

Much like there are certain words that raise alarms when said in an airport context, there are certain religious words that raise alarm to other governments. Building a practice of avoiding these will help you fly under the radar when it comes to your communication.

Here are a few principles to keep in mind as you communicate:
1. You don't want to be linked (or link others) to conversion work
2. Do not talk negatively about your host country or foreign countries
3. Be sensitive when talking about our national partners

▶ It's possible to stay in touch and have fruitful conversations without using alarming keywords.

Here are examples of how changing your vocabulary can protect your conversations:

INSTEAD OF SAYING:	SAY:
Missionary	Worker or Team Member
ABWE	The Company
Gospel	Good News
Witnessed/Evangelized	Shared
Baptized	Dunked
Bible/Scripture	Word
God/Jesus	Father/Son

This list is not meant to be all-inclusive or definitive. It is to show you how you can omit religious words from your conversations with others and still communicate about your life without it sounding like a religious conversation.

2 Have a Clean Online Presence

When applying for a visa to other countries, they often use the internet to see if you're linked to any sort of mission work. Furthermore, your connection to partners can jeopardize their ministry by your openness.

▶ **Even if you aren't living in a restricted access country, you may travel to one or have communication with team members and partners living in one.**

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

- You should not have your ministry listed anywhere on the internet, especially on supporting churches' websites.
- Your picture, name, and location are all sensitive pieces of information that should never be linked to you or your ministry.

IF YOU LIVE OR PRIMARILY WORK IN A "SAFE" COUNTRY

You and your leadership may decide to avoid appearing in Google searches by using these tips:

- If possible, avoid use your last name on any sites that directly talk about your ministry.
- If there are sites who want to list your work or missions bio, request that the webmaster set the page to "noindex." Find instructions at abwe.org/noindex
- It's OK if you can be identified as a Christian online, or someone who travels to other countries. But try not to be identified digitally as someone involved with foreign mission (conversion) work.

Periodically search your name in Google to see if you appear on any unexpected websites or pages. If so, reach out to them and ask them to remove that content.

A stranger should not be able to use the internet to identify you as being in full-time ministry, or involved in conversion work, regardless of where you live.

▶ **These guidelines are important to share with your supporters and supporting churches. Verify your supporting churches are not accidentally posting about you or your ministry.**

3 Be Wise with Social Media

Part 1: Platform Introductions

One of the most common ways that people and ministries are jeopardized is through social media. It's great for staying in touch with family, friends, and supporters, but there is often far more information on it about us than we realize.

For many team members, the benefits of using social media far outweigh the risks—if done with wisdom, and the right settings.

▶ **The primary concern with social media is *not* that you'll be identified as a Christian, but that you'll be linked to conversion work, or that you would shame your host country, government, or religious leaders.**

Don't let any posts about your ministry be seen by those who are not your friends. Don't let your friend list be public.

If you use a Facebook group to keep your supporters informed, make sure it is set to secret, not just private.

To see what your account looks like to those you haven't approved as friends, go to your profile -> Click on the three dots under your header picture -> Click "View As."

Ministry videos should be carefully reviewed so they don't unnecessarily link to people who fall under these guidelines.

If you use Twitter to publish ministry updates, make your account private, and ensure that there isn't sensitive information in your profile.

If you use Instagram to publish ministry updates, make your account private, and ensure that there isn't sensitive information in your profile.

If you list ministry jobs in your LinkedIn profile, ensure that only your connections can see them.

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

It's best to assume that any information you publish, even if limited to just your friends, will be read by your host government.

3 Be Wise with Social Media

Part 2: Understanding Data Points

There are many ways that social media platforms gather and display data about you that can jeopardize you or your team members and partners. Here are some of the big ones to watch out for:

Friends/Connections
Your friends list should always be private. Much like in real life, who you are friends with reveals a lot about you.

We've known of people who have been denied tourist visas into India because their friend list was public, and they were friends with too many Indians on facebook.

Location Services & Checkins
Many social media apps track your location, even when you aren't using it. Turn off location services for every app that doesn't need it. If you can do so via your OS, that's even better.

Off-App data collection
Many social media apps can collect data about you even when you aren't on their app or website.

Photos
If someone else posts a photo of you and tags you in it, it could be visible to the world, betraying your friends, location, or other sensitive data. Change privacy settings so you have to approve it first.

Likes
What you "like" reveals your heart and priorities. If that is public (to everyone or unbelieving friends), it could jeopardize your ministry.

What are things you liked 5 or 10 years ago that are still on your profile?

Posts
What you posts matters too! Posts that link you to conversion work are more sensitive than posts that identify you as a believer. Use wisdom depending on your home country and who you're posting about.

▶ **Watch our online tutorial of how to change your settings. Visit abwe.org/social-media-checkup**

Take these into consideration as you use social media; they will go a long way in protecting your ministry.

4 Use a VPN (Virtual Private Network)

It's easy for others to intercept your web traffic and even see what websites you are going to (and other sensitive information) when you use public internet, or internet in other countries. A VPN adds security that keeps your browsing safe.

There are many VPNs that you can choose from, but an industry leader that we recommend is NordVPN (nordvpn.com).

This VPN can work on Windows, macOS, Linux, iOS, Android, and Android TV. There are also proxy extensions for Chrome and Firefox.

We have negotiated special rates (60% off their lowest rate) for all of our team members with NordVPN, and can have the funds come directly from your ministry account. The cost is $37 annually.

To request a VPN, just send an email to itsupport@abwe.org.

Each family will be given 6 different VPN licenses, so your family can use one account on multiple laptops and phones.

▶ **Learn how to set up your VPN at nordvpn.com/tutorials**

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

Use a VPN for any work conversations, browsing, or when you don't want someone else to have access to your entire current internet activity.

IF YOU LIVE OR PRIMARILY WORK IN A "SAFE" COUNTRY

Use a VPN anytime you're not at your home or office.

Using a VPN will add a layer of security to all of your digital communication. If you are video chatting from overseas, we recommend you only do so with a VPN turned on.

***Please note that those in East Asia have different VPN guidelines.**

5 Protect Digital Files

Much like when you hand a physical file to someone, it is out of your control what that person does with it, or who they share it with.

The same is true with digital files (pictures, video, audio, word docs, etc)—only more so. Careless uploading of files could put others and their ministries in danger.

- **Anything you send to all of your supporters has the risk of being forwarded, posted, or used in a way you did not intend.**

- **Always request that supporters not post or forward your support emails, but do not assume that will always be honored.**

Remember that email is not very secure to begin with, and it's even more true with bulk emails. Do not include people who live in hostile countries on your update list.

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

- Minimize the data you store on your phone and laptop.
- Use laptop encryption, and strong passwords.
- Only upload files to cloud storage (ie, Google Drive) while using a VPN
- Use caution when emailing files

IF YOU LIVE OR PRIMARILY WORK IN A "SAFE" COUNTRY

- When traveling to restricted access countries, do not have sensitive files, pictures, or contacts on your phone or laptop

- **Digital security is not just about protecting yourself and your ministry, but about protecting your team members, partners, and other believers around the world.**

6 NEVER Reuse a Password

Simply put, never ever under any circumstances reuse a password across a site.

The #1 way hackers gain access to sensitive things digitally in your life is exploiting reused passwords, or using weak passwords.

Q: What do you consider the most common internet security mistake that people make to be?

A: "Weak and Reused Passwords."

- Aubrey Cottle a.k.a. Kirtaner, the founder of the hacker collective "Anonymous"

Two Factor Authentication uses a text message, secure key, or even a backup code to make sure it's really you logging in. This is one of the best ways to protect your accounts from unauthorized access, and is very simple to set up.

We recommend using more than just the text option, especially if you may travel in a place where you don't have access to cell data.