Digital Security Guidelines

The world is changing. We recommend these guidelines for every worker—not just those in restricted fields.

➔ 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.

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.

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.

Poor digital security habits can lead to being arrested or expelled.

Updated: March, 2023

2023-CM-860PZ3735

Table of Contents

Use Common Sense Digital Discernment

DO...

- ✔ Use strong passwords, and NEVER reuse passwords for different sites.
- ✔ Consider using a password manager.
- ✔ Use your ABWE email for all company communications.
- ✔ Keep your Operating Systems up to date with all software patches.
- ✔ Keep your laptop and phone locked when not in use. Configure the device to encrypt data stored locally.
- ✔ If in doubt, ask your leadership team for guidance and assistance.
- ✔ Maintain an antivirus subscription with a reputable company (like Malwarebytes).

DON'T...

- ✘ Don't open or interact with suspicious emails and never click links from unknown sources.
- ✘ Don't allow others to access devices that connect to ABWE or your email. Make a separate user profile if sharing hardware.
- ✘ 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 connect to ABWE systems or check your "work" email in public without a VPN, especially in sensitive countries.

1 Protect Passwords and Always Use 2FA

Creating and using unique, strong passwords is incredibly important. A strong password is the first line of defense against attackers but often it takes more than just a strong password. Combining a strong password with two-factor authentication (2FA) helps bolster your defenses against attackers.

Use strong, unique passwords

- The foundation to a good defense starts with a strong, unique password.
- Passwords should be long with a combination of lots of characters, numbers, and symbols. An easy recommendation is to turn a sentence into a password and make sure to add a few numbers and symbols in the sentence or at the end.
- Choose passwords that would be nearly impossible for someone to guess, even someone who knows everything about you (birthdate, kids names, etc.) because all of that information can be obtained with research.
- Never reuse passwords across sites. If one website is breached by hackers and your password is uncovered, the hacker will attempt to access other sites using the same password.

Strong Passwords

Consider using a password manager

Because remembering every password for every site feels overwhelming, we recommend you use a password manager. Password managers recommend strong passwords and remember them for you.

ABWE has negotiated a discount rate with 1Password - for $1.99/month (a 50% discount). To sign up for this, just email **itsupport@abwe.org**.

Password Manager

Always use two-factor authentication (2FA)

2FA prevents an attacker from gaining access to your accounts. 2FA is one of the best ways to protect your accounts from unauthorized access and is very simple to setup.

It uses a text message, secure key, or a code to verify your identity before completing the login.

Even if your password is stolen or compromised, the bad actor will not be able to access your account if 2FA is properly configured.

You should enable 2FA on all of your accounts, not just email. 2FA is an option with most banks, social media accounts, and most other apps that store profiles.

We recommend configuring multiple 2FA methods, especially if you travel to places without cellular service. Remember, texts are easy to intercept, so if you are in a secure area, never use the texting option.

Two-factor Authentication

2 Use a Virtual Private Network (VPN)

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 Wifi or access the 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 our team members with NordVPN and can have the funds come directly from your ministry account. The cost is only $37 annually.

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

Each VPN license can be used on up to 6 devices at a time. This way you can use one account on multiple laptops and phones.

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

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.

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

You should always use a VPN for anything done online, including email. You should configure your device so it cannot access the internet if your VPN is not connected.

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

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

3 Protect Digital Files

When you hand a physical file to someone, you have no control over what that person does with it or whom they share it. The same is true with digital files (pictures, video, audio, word docs, etc)—only more so as sharing is much easier with digital files.

Be especially careful sharing photos or stories of others as they can put team members, partners, or locals at risk.

Anything you send has the risk of being forwarded, posted, or used in a manner you did not intend.

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

Email is only as secure as the person receiving your email, which means bulk emails magnify the risk. Make sure not to include people who live in hostile countries on your update list.

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

IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

Minimize the data you store on your phone and laptop. Use device encryption and strong passwords.

Always use a VPN when doing anything on the internet.

Use caution when emailing files you don't want shared.

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.

4 Avoid Phishing Attempts

Nearly 33% of people will fall victim to at least one scam in their lifetime. In 2021 alone, 59 million people lost nearly $30 billion dollars to a combination of online, phone, and text scams. But, money isn't the only thing lost by falling victim to these scams.

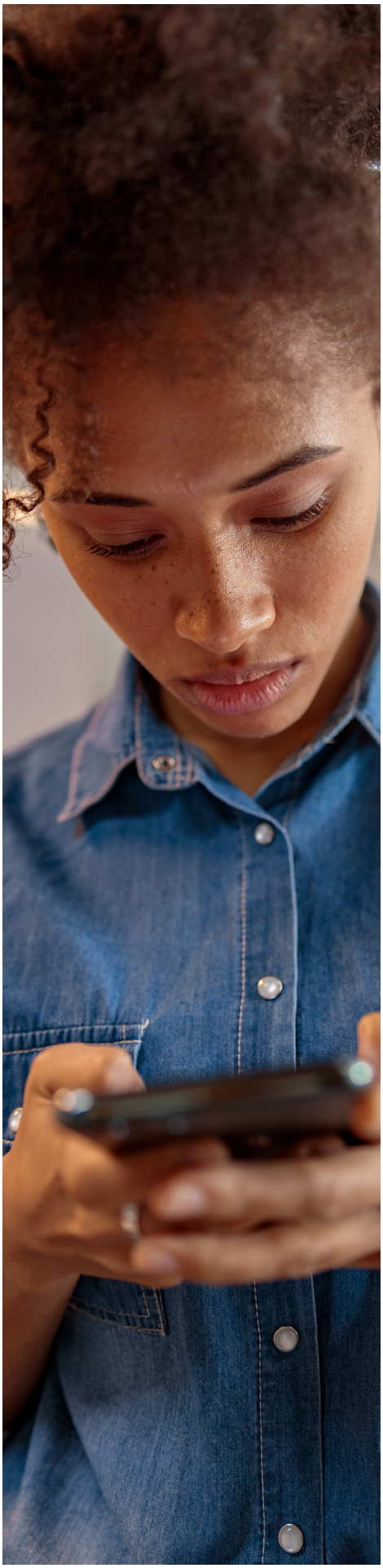
Your identity can be stolen, your passwords could be compromised, or you could unknowingly expose the personal data of every ABWE missionary, staff, and donor. The number one way attackers gain access to your information is by tricking you into clicking malicious links or downloading corrupted files. The stakes are high, and you play an important role in our defense.

➔ Before you click any link, download any attachment, or respond to any email with personal information, ask these questions:

1. **Was I expecting this message, and does it address me by name?**
   - An unexpected message, especially one that doesn't address you by name, is a sign that the message could have been spam sent to a very large group with little effort.
2. **Are there attachments or links in the message?**
   - Attachments and links are commonly part of the message. The links or attachments can force malicious programs to run on your device and should never be blindly trusted unless you know the sender.
   - Links can take you to fake sites that look real but will steal the information you enter.
   - Never share your login credentials with anyone. Always contact **itsupport@abwe.org** if you have questions.
3. **Do I recognize the email address it came from?**
   - The sender may use an email address that doesn't match the company they claim to represent. Note: It may be a close misspelling (like **finance@awbe.org**), so look carefully.
4. **Does the message mention a problem or a potential prize?**
   - Messages meant to deceive you usually come with a threat, problem, or promised prize that requires information or action on your part.
5. **Does the message require me to act immediately/quickly?**
   - Scams work by inducing a sense of urgency or fear. Reputable companies will give you time to react to their communications.
6. **Are there spelling or grammatical errors in the message?**
   - Many scam messages contain grammatical errors and misspellings.

These are all indicators that warrant extra scrutiny by you. If you are not sure about the legitimacy of a message, contact the company* the message claims to come from to verify the message.

*Don't use the contact info included in the email message, as it could belong to the scammer. Research the contact information directly from the company website.



5 Use Secure Communication

Part 1: Use Secure Apps

Governments and 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's 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, who you're communicating with, your country, and other factors.

Normal texting is not secure. Use MS Teams or the Signal app for messaging team members. Also, do not message using social media platforms.

Email is only as secure as the other person receiving it. In general, assume emails sent or received outside of ABWE are not secure.

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

Using encrypted or secure communication may not be as big a concern for you, but it could be for the recipient. Therefore, always practice smart communication processes.

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.

Part 2: Be wise in your vocabulary

Since government actors can access messages, be careful with the language used to minimize the possibility of raising alarms. It's possible to stay in touch and have fruitful communications without causing unnecessary risks to you and others.

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 ministry-related words (i.e., baptism, missionary, etc.) when it comes to your communication.

Here are a few principles to keep in mind as you communicate:

- You don't want to be linked (or link others) to conversion work.
- Do not talk negatively about your host country or foreign countries.
- Be sensitive when talking about our national partners.
- Don't give excessive details (i.e., names, location) that identify people or ministries.

6 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's often far more information about you on social media than you 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.

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.

Facebook

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."

Twitter

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

Instagram

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

You Tube

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

LinkedIn

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

➔ We recommend not downloading or using the TikTok app at all due to the security concerns associated with it.

Be Wise with Social Media

Part 2: Understanding Data Points

There are many ways social media platforms gather and display data about you that can jeopardize you or your team members and partners.

Here are some things to watch out for:

Friends/Connections

Your friends list should always be private. Much like in real life, your friends reveal a lot about you.

We know people who were denied tourist visas into India because their friend list was public, and they were Facebook friends with too many people in India.

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.

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.

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?

Off-App Data Collection

Many social media apps can even collect data about you even when you aren't using their app or website, especially if you click ads or links from their apps. Check app settings and turn off background refresh for the apps.

Posts

What you posts matters! 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 help protect your ministry.

7 Have a Clean Online Presence

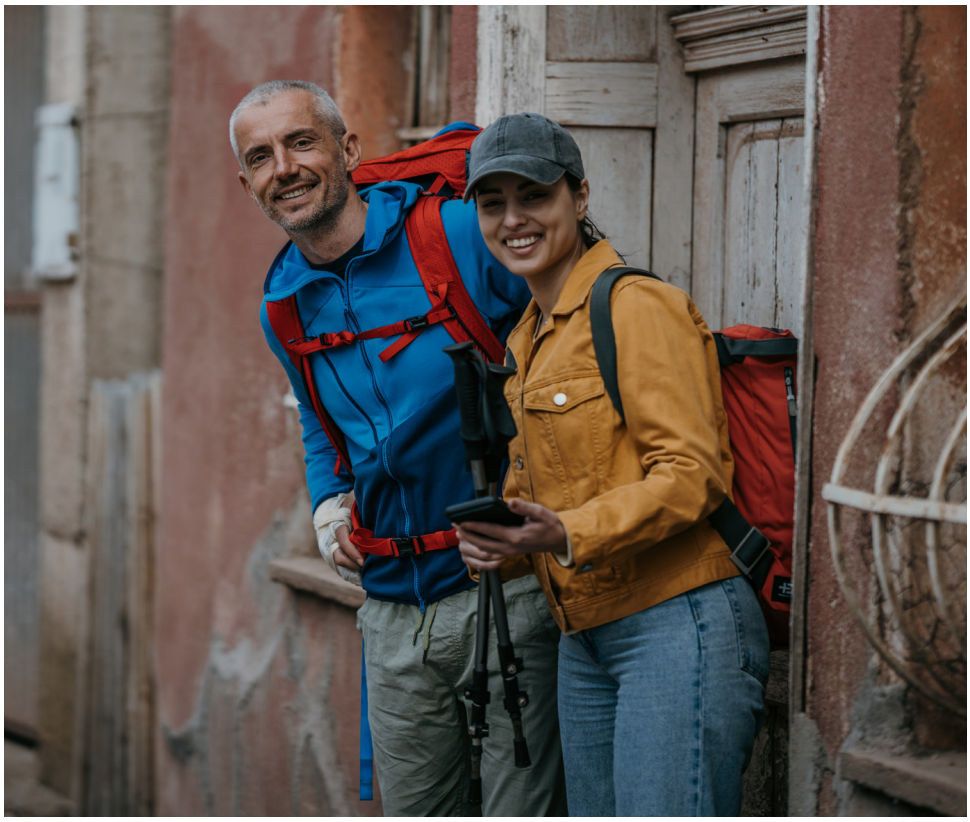
When applying for a visa to other countries, they often use the internet to see if you're linked to any sort of mission work. Furthermore, your connection to partners and other team members can jeopardize their ministry by your openness.

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.

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.



IF YOU LIVE OR PRIMARILY WORK IN A RESTRICTED ACCESS COUNTRY

You should not have your ministry listed anywhere online, especially on churches' websites. Make sure churches know not to post anything about you or your ministry online.

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 using 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 the webmaster set the page to "noindex." Find instructions at

It's OK to be identified online as a Christian or someone who travels to other countries but try to avoid being identified as someone involved with foreign mission (conversion) work.