Duo Travel Guide

Version 2.0 Published November 29, 2018

Overview

As a member of an organization **protected by Duo**, you already have secure access to applications and assets. This guide is designed to **help you maintain that trusted access** while you're on the go.

Whether it's local travel and you need to plan for a drained phone battery, or international travel during which you may lose access to phone callback or the Internet entirely, we want to make sure you **feel equipped to continue securely** reaching the services you need.

Additionally, we leaned on the security expertise of our Duo Labs research team to provide more general guidelines for **traveling safely**. Wondering if you should connect to that public Wi-Fi hotspot? Concerned about pickpockets? Should you really back everything up? We have the answers—and more—below.

Table of Contents

Using Duo During Travel

Duo offers a variety of options to allow you to **maintain trusted access while traveling.** In many cases you will be able to continue using your existing authentication methods, but some travel plans may require you to have additional options in place.

Preparing to Travel

If your organization uses Duo's self-service feature, be sure you have **enrolled a mobile device with the Duo Mobile app or access to cellular networks while traveling**. If possible, we recommend having a **second device** configured before traveling as well.

Before you go, speak with your help desk administrator and see if they recommend configuring two-factor authentication for additional applications while you're traveling. Depending on where you're going and what applications you'll need to access, they may have additional security concerns or need to adjust location-based policies.

Authenticating on the Road

It's important to remember that the **Duo Mobile application can be used to generate passcodes** on airplanes or in remote regions where Duo Push, SMS-delivered passcodes, or phone callback may be unavailable of difficult to use.

Please note that **Duo Push can use a Wi-Fi connection** to function. If you can access the Internet from your mobile device, you can receive push notifications.

Lost or Stolen Devices

Contact your help desk immediately if you lose your phone or suspect that it's been stolen. If your organization has enabled **Duo's self-service feature** and you had previously enrolled an additional authentication device, you can use **My Settings & Devices** to delete your lost or stolen phone.

If you aren't able to log in to Duo at all, then your Duo administrator can disable the missing phone for authentication and help you log in using another method.

Traveling Safe

Beyond making sure you're prepared to continue using Duo when on the road, here are some general security recommendations from our Senior Security Researcher, Mark Loveless, for keeping your devices and data safe.

Thwarting Pickpockets and Thieves

If you're used to putting your phone in your back pocket, don't. **Put it in your front pocket**. Consider doing the same for your wallet as well, if you carry one of those. Using a zipped or snapped pocket if possible is even better. Always make sure your device is screenlocked. If it is lost or stolen, make sure to contact your organization's security team as soon as possible.

If you carry a purse, satchel, or backpack, I'd recommend one with **minimal outside pockets** that are not easy to get into, and keep those outside pockets empty or filled with non-essentials. I'd also recommend a bag that is resistant to a quick knife slice to gain access to the insides. **Keep it with you at all times**, unless you are leaving it in a safe place.

Not looking like a tourist helps prevent you from standing out to would-be pickpockets who frequently target those who look out of place or like they are in an unfamiliar location. Blend in, and remember this is more than simply not wearing a tuxedo to the beach. Avoid flashy colors and clothing with memorable logos or slogans. Do a bit of research on your destination and figure out what "normal" looks like, and adjust your wardrobe accordingly. Everything you can do to not stand out helps prevent you from becoming a pickpocket victim.

Reduce Your Load

Most devices do not need to make the trip. Typically a smartphone and some earbuds are enough, and you only need to take one charger. The point is to **try and take that huge list of tech and reduce it down to the basics**. A modern phone is your boarding pass, credit card, camera, GPS, and general concierge.

Only take your laptop if you think you're going to need to dump photos because you're out of space on your cloud account or cannot add extra memory to the phone. If it is a working trip, you may not be able to leave the laptop home. **But if at all possible, reduce it to one item if you can.**

The strategy is simple: **have less to lose** (think about all those cables). If your phone is stolen, it is a lot easier to replace this single item than all of your tech at once.

Reduce Your Attack Surface

Make sure any tech you travel with has a **password, code, or screenlock and ensure that disk encryption is enabled**. This will help keep your **data safe and unseen by prying eyes**, in the event of a lost or stolen device. Watch what network you connect to when using Wi-Fi. Free doesn't always mean free, it could be someone doing something bad to present you with a myriad of fake websites to get you to give up credentials.

If you are using your phone, **I'd recommend turning off Wi-Fi and using your data plan—it's much safer**. This may not be an option for international travel as your data plan may not work when out of your home country. If in doubt, contact your carrier and ask what they offer for out-of -country data plan solutions. If your device is carrier unlocked, consider purchasing a local SIM upon arrival to maintain access to network data.

Turning off Bluetooth and everything else is also a good idea. If you bring your laptop, turn off all of the extra communication. If you need Bluetooth for one task (say, a data transfer between devices), then turn it on for that one task and turn it back off immediately after you're done.

Update Everything and Make Sure Everything Works

Make sure you update your device so that it is **running the latest and greatest**, and that all associated apps are also up to date on all devices. In your rush to reduce your load, don't simply download some app to your phone so you can leave your laptop at home. Use that app and make sure it works. The last thing you want to do is try to reset your forgotten bank account password from Uncle Bob's computer that's running Windows 95, all because you realize too late that your app doesn't have password autofill like your browser at home does.

There are multiple services that allow **cloud sharing of data between devices**, if you've never done this before, testing it at the airport on your way out of town is not the best method. Make sure you know how things work and what those limits are. Don't do a manual backup of your phone in the car on the way to the airport—**do the backup before you leav**e. Oh yeah, **back up everything before you leave**.

Vigilance Online

Whenever you're out and about on Wi-Fi from a hotel, Grandma's house, or coffee shop at the airport, stick to the known good sites. If you see those odd browser warnings that the site you are visiting is unsafe, pay attention—especially if you're using public Wi-Fi. **Use two-factor authentication**. Make sure your connection is encrypted, and seriously avoid any online shopping—it's much safer to do shopping from home vs. a public network.

In Conclusion

Patch. Update. Reduce attack surface. Do backups. Test stuff before travel. Do wicked cool stuff like putting your phone in the front pocket instead of the back. Don't dress like a tourist, even if you are one. **Use two-factor authentication**. Avoid suspicious networks, use your data plan on your phone, don't shop online while traveling, and stay away from any stranger's computer.