Keep Your Devices and Data Safe During International Travel

University Communications
May 2018

For general tips about staying safe while traveling, please see this related article.

There's a lot to think about when planning a trip abroad: getting to your destination country, figuring out where you'll stay and how you'll get around while you're there, and how to stay safe during travel and after you arrive.

One aspect you might not have considered: keeping your electronic devices and data safe.

The Information Security Office and Office of Global Initiatives share their expert advice for protecting your electronic data before, during and after your time abroad.

Before you go

Traveling safely with your gadgets means planning ahead, says Teresa Banks, program manager in the Information Security Office. Before the trip, she says, ask yourself what devices you really need, and leave behind ones that aren't absolutely necessary.

"If you absolutely don't need a device, don't take it with you because it's just one more thing you can lose or have stolen or be compromised," Banks says. "In some countries, the minute you hit the ground, you can expect someone is trolling through your data."

If you're traveling on UA business, Banks says, ask if your department has a clean loaner laptop that you can take. This allows you to leave your own work computer behind – along with all the data stored on it – and still do your work abroad.

Similarly, Banks suggests using a "burner" phone, or a no-contract prepaid cellphone, if you can manage without your own.

If you do need to travel with your own UA-issued or personal devices, Banks says, make sure your laptop is loaded with antivirus software and encrypted. But keep in mind that some countries prohibit encrypted devices, so research is required prior to your trip. Cellphones should be set to automatically update their apps, she says.

The other thing to consider before the trip, Banks adds, is how you'll use NetID+ two-factor authentication. If you typically use your cellphone to complete the second phase of the login, that may not work while abroad. Banks recommends considering using a hardware token or bypass codes. More information about NetID+ is available here.

During the trip

When you've arrived, keep devices out of sight, but also keep in mind that thieves can usually
tell if a bag has a laptop inside, says Laura Provencher, associate director of global resiliency in Global Initiatives. She suggests keeping handheld devices in front jacket pockets and keeping a close eye on shoulder bags, which can be easily snatched away.

"Don't travel with the newest gadgets, especially if you are going somewhere with high rates of crime," Provencher said. "If you take them, removing unnecessary apps, data or info is a good idea, especially anything that could be a problem if other people could access them, like banking apps."

If you're online while abroad, Banks suggests connecting to the UA's virtual private network, which allows you to use the internet via an encrypted connection. A similar option is a service called Eduroam [7], which is used by universities all over the world, including the UA. Eduroam can be accessed with NetID credentials.

After returning

When you return from your trip, Banks says it's a good idea to have a security scan run on your device to check for any malware that may have been used on it. Departmental IT staff, or staff with the 24/7 IT Support Center [8], can help with that. Passwords for any accounts used during the trip, she adds, should be changed.

Source URL: https://uaatwork.arizona.edu/lqp/keep-your-devices-and-data-safe-during-international-travel

Links
[1] https://uaatwork.arizona.edu/lqp/traveling-abroad-summer-stay-safe-these-tips
[2] https://security.arizona.edu
[3] https://global.arizona.edu/
[4] https://security.arizona.edu/security-guidelines-international-travel
[5] https://netid-plus.arizona.edu
[6] https://it.arizona.edu/service/netid-plus
[8] https://it.arizona.edu/service/247-it-support