How to protect your private data when you travel to the United States

March 7 2017, by Paul Ralph

What do you do if a border official asks for your phone PIN? Credit: Ervins Strauhmanis/Flickr, CC BY-SA

On January 30 – three days after US President Donald Trump signed an executive order restricting immigration from several predominantly Muslim countries – an American scientist employed by NASA was detained at the US border until he relinquished his phone and PIN to border agents. Travellers are also reporting border agents reviewing their Facebook feeds, while the Department of Homeland Security considers

requiring social media passwords as a condition of entry.

Intimidating travellers into revealing passwords is a much greater invasion of privacy than inspecting their belongings for contraband.

Technology pundits have already recommended steps to prevent privacy intrusion at the US border, including leaving your phone at home, encrypting your hard drive and enabling two-factor authentication. However, these steps only apply to US citizens. Visitors need a totally different strategy to protect their private information.

The problem

Giving border agents access to your devices and accounts is problematic for three reasons:

1) It violates the privacy of not only you but also your friends, family, colleagues and anyone else who has shared private messages, pictures, videos or data with you.

2) Doctors, lawyers, scientists, government officials and many business people's devices contain sensitive data. For example, your lawyer might be carrying documents subject to attorney-client privilege. Providing such privileged information to border agents may be illegal.

3) In the wake of revelations from Chelsea Manning and Edward Snowden, we have good reason to distrust the US government's intentions for our data.

This problem cannot be solved through normal cybersecurity countermeasures.

Encryption, passwords and two-factor authentication are useless if

someone intimidates you into revealing your passwords. Leaving your devices at home or securely wiping them before travelling is ineffective if all of your data is in the cloud and accessible from any device. What do you do if border agents simply ask for your Facebook password?

And leaving your phone at home, wiping your devices and deactivating your social media will only increase suspicion.

What you can do

First, recognise that lying to a border agent (including giving them fake accounts) or obstructing their investigation will land you in serious trouble, and that agents have sweeping power to deny entry to the US. So you need a strategy where you can fully cooperate without disclosing private data or acting suspicious.

Second, recognise that there are two distinct threats:

1) Border agents extracting private or sensitive data from devices (phone, tablet, laptop, camera, USB drive, SIM card, etc.) that you are carrying.

Entering the US can be a hectic environment. Best to be prepared before you get off the plane. Credit: EPA/SHAWN THEW

2) Border agents compelling you to disclose your passwords, or extracting your passwords from your devices.

Protecting your devices

To protect your privacy when travelling, here's what you can do.

First, use a cloud-based service such as Dropbox, Google Drive, OneDrive or Box.com to backup all of your data. Use another service like Boxcryptor, Cryptomator or Sookasa to protect your data such that neither the storage provider nor government agencies can read it. While

these services are not foolproof, they significantly increase the difficulty of accessing your data.

Next, cross the border with no or clean devices. Legally-purchased entertainment should be fine, but do not sync your contacts, calendar, email, social media apps, or anything that requires a password.

If a border agent asks you to unlock your device, simply do so and hand it over. There should be nothing for them to find. You can access your data from the cloud at your destination.

Protecting your cloud data

However, border agents do not need your device to access your online accounts. What happens if they simply demand your login credentials? Protecting your cloud data requires a more sophisticated strategy.

First, add all of your passwords to a password manager such as LastPass, KeePass or Dashlane. While you're at it, change any passwords that are easy to guess, easy to remember or are duplicates.

Before leaving home, generate a new master password for your password manager that is difficult to guess *and* difficult to remember. Give the password to a trusted third party such as your spouse or IT manager. Instruct him or her not to provide the password until you call from your destination. (Don't forget to memorise their phone number!)

If asked, you can now honestly say that you don't know or have access to any of your passwords. If pressed, you can explain that your passwords are stored in a password vault precisely so that you cannot be compelled to divulge them, if, for example, you were abducted while travelling.

This may sound pretty suspicious, but we're not done.

Raise the issue at your workplace. Emphasise the risks of leaking trade secrets or sensitive, protected or legally privileged data about customers, employees, strategy or research while travelling.

Encourage your organisation to develop a policy of holding passwords for travelling employees and lending out secure travel-only devices. Make the policy official, print it and bring it with you when you travel.

Now if border agents demand passwords, you don't know them, and if they demand you explain how you can not know your own passwords, you can show them your organisation's policy.

This may all seem like an instruction manual for criminals, but actual criminals will likely just create fake accounts. Rather, I believe it's important to provide this advice to those who have done nothing illegal but who value their privacy in the face of intrusive government security measures.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How to protect your private data when you travel to the United States (2017, March 7) retrieved 20 July 2024 from https://phys.org/news/2017-03-private-states.html