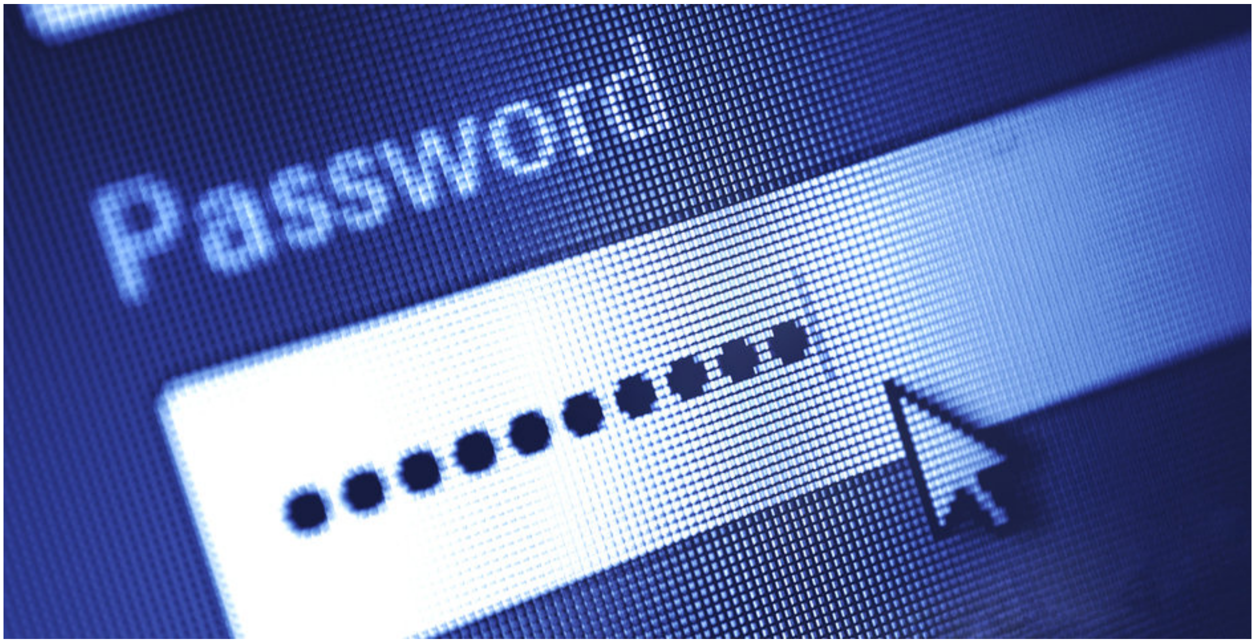
Why We Should Not Know Our Own Passwords

March 10, 2017



Since 2009, U.S. Customs and Border Protection agents have been allowed to search electronic devices carried by citizens or noncitizens as they cross the border into the United States from other countries. More recently, Homeland Security Secretary John Kelly suggested this digital vetting should also include harvesting social media passwords. Kelly's proposal prompted legal and technology experts to respond with an open letter expressing deep concern about any policy that demands that individuals violate the "first rule of online security": Do not share your passwords.

Travelers themselves responded, too, looking for ways to avoid surrendering their device passwords to federal agents. One approach – what we might call the "Nothing To See Here" method – tries to make a device unsearchable by erasing the hard drive before travel, uninstalling social media apps, letting the device's battery charge run out or even wiping the device if an emergency or "duress" password was entered.

The "I'd Love To Comply, But I Can't" approach involves exotic solutions like installing two-factor authentication on the device or social media account, and then making the second factor (such as a passcode or digital key) available only in a remote location. Retrieving the second factor would require a warrant and travel outside the border crossing.

These methods are dangerous because they put an already stressed traveler in the position of defying law enforcement at the border, a legal environment that is designed to support the government and not the traveler. Following this advice properly also requires careful execution of technical skills that most travelers don't have. And the degree of advance planning and preparation required might itself be considered a sign of suspicious activity requiring deeper scrutiny by border officials.

But it's tempting to wonder: Could computer scientists and software designers like me create a better password system? Can we make "I'd Love To Comply, But I Can't" the only possible answer for every traveler? In short, can we create passwords even their owners don't know?

The search for the unknowable password

Developing unknowable passwords is an active area of security research. In 2012, a team from Stanford University, Northwestern University and the SRI research center developed a scheme for using a computer game similar to "Guitar Hero" to train the subconscious brain to learn a series of keystrokes. When a musician memorizes how to play a piece of music, she doesn't need to think about each note or sequence. It becomes an ingrained, trained reaction usable as a password but nearly impossible even for the musician to spell out note by note, or for the user to disclose letter by letter.

In addition, the system is designed so that even if the password is discovered, the attacker is unable to enter the keystrokes with the same fluidity as the trained user. The combination of keystrokes and ease of performance uniquely ties the password to the user, while freeing the user from having to remember anything consciously.

Unfortunately, in our border travel scenario, the agent could demand that the traveler unlock the device or application using the subconscious password.

Could this be the new way to log in online? Listening to headphones via shutterstock.com

A team at California State Polytechnic University, Pomona, proposed a different solution in 2016. Their solution, called Chill-Pass, measures an individual's unique brain chemistry response while listening to her choice of relaxing music. This biometric reaction becomes part of the user's log-in process. If a user is under duress, she will be unable to relax enough to match her previously measured "chill" state, and the log-in will fail.

It is unclear whether CBP agents would be able to defeat a system like Chill-Pass by providing travelers with, say, massage chairs and spa treatments. Even so, the stresses of daily life would make it impractical to use this kind of password regularly. A relaxation-based system would be most useful for people undertaking high-stakes missions where they fear coercion.

And just like with other plans to make CBP scrutiny impossible, this might end up attracting more attention to a traveler, rather than encouraging officers to give up and move on to the next person.

Can you score security?

In 2015, Google announced Project Abacus, another solution to the "I'd Love To Comply, But I Can't " problem. It replaces the traditional password with a "Trust Score," a proprietary cocktail of characteristics that Google has determined can identify you. The score includes biometric factors like your typing patterns, walking speed, voice patterns and facial expressions. And it can include your location and other unspecified elements.

The Trust Score calculator constantly runs in the background of a smartphone or other device, updating itself with new information and recalculating the score throughout the day. If the Trust Score falls below a certain threshold, say by observing a strange typing pattern or an unfamiliar location, the system will require the user to enter additional authentication credentials.

It's unclear how a Trust Score authentication might affect a border search. A CBP agent could still demand that a traveler unlock the device and its apps. But if the agency couldn't disable the Trust Score system, the phone's owner would have to be allowed to hold the device and use it throughout the agent's inspection. If someone else tried to use it, the constantly recalculated Trust Score could fall, locking out an investigator.

That process would at least ensure a phone's owner knew what information federal agents were collecting from the phone. That hasn't been possible for some arriving travelers, including U.S. citizens and even government employees.

But the Trust Score system puts a lot of control in the hands of Google, a for-profit corporation that could decide – or could be compelled – to provide government with a way around it.

So now what?

None of these technological solutions to the password problem is perfect, and none of them is commercially available today. Until research, industry and innovation come up with better ones, what's a digital age traveler to do?

First, do not lie to a federal agent. That’s a felony and will definitely attract more unwanted attention from investigators.

Next, determine how much inconvenience you are willing to tolerate in order to remain silent or to refuse to comply. Noncompliance will have a cost: Your devices could be seized and your travel could be seriously disrupted.

Either way, if and when you are asked for your social media handles or passwords, or to unlock your devices, pay attention and remember as many details as you can. Then, if you wish, alert a digital civil liberties group that this happened. The Electronic Frontier Foundation has a web page with instructions for how to report a device search at the border.

If you think that sensitive materials might have been compromised in the search, notify family, friends and colleagues who might be affected. And – until we figure out a better way – change your passwords.

Megan Squire , Professor of Computing Sciences, Elon University . This article was originally published on The Conversation . Read the original article .