PHYS.ORG

Encrypted smartphones secure your identity, not just your data

February 28 2018, by Susan Landau

IOWA
USA IA
DRIVER LICENSE
TROMBINO
PAUL , III
[redacted]
JOHNSTON, IA 501314751
DL No [redacted]
ISS 01/17/2013 EXP 06/24/2016
Class C End NONE
Restrictions B
DOB [redacted]
DD 600000006TP1757M240616D
Sex M
Hgt 6'-00"
Eyes BRO
DONOR Y

A smartphone is a digital form of ID for many apps and services. Credit: Iowa Department of Transportation

Smartphones store your email, your photos and your calendar. They provide access to online social media sites like Facebook and Twitter, and even your bank and credit card accounts. And they're keys to something even more private and precious – your digital identity.

Through their role in two-factor authentication systems, the most commonly used secure digital identity protection method, smartphones have become essential to identifying people both online and off. If data and apps on smartphones are not secure, that is a threat to people's identities, potentially allowing intruders to pose as their targets on social networks, email, workplace communications and other online accounts.

As recently as 2012, the FBI recommended the public protect their smartphones' data by encrypting it. More recently, though, the agency has asked phone makers to provide a way to get into encrypted devices, what police call "exceptional access." The debate so far has focused on data privacy, but that leaves out a vital aspect of smartphone encryption: its ability to secure people's personal online identities.

As I wrote in my recent book, "Listening In: Cybersecurity in an Insecure Age," doing what the FBI wants – making phones easier to unlock – necessarily decreases users' security. A recent National Academies of Sciences, Engineering and Medicine study, in which I participated, also warns that making phones easier to unlock potentially weakens this key element of securing people's online identities.

Gathering evidence or weakening security?

In recent years, police have sought access to suspects' smartphones as part of criminal investigations, and technology companies have resisted. The most prominent of these situations arose in the wake of the 2015 San Bernardino mass shooting. Before the attackers themselves were killed in a shootout, they were able to destroy their computers and phones – except one, a locked iPhone. The FBI wanted the phone decrypted, but worried that failed attempts to crack Apple's security mechanisms could cause the phone to delete all its data.

The agency took Apple to court, seeking to force the company to write special software to avoid the phone's built-in protections. Apple resisted, arguing that the FBI's effort was government overreach that, if successful, would decrease all iPhone users' safety – and, by extension, that of all smartphone users.

The conflict was resolved when the FBI paid a cybersecurity firm to break into the phone – and found nothing of relevance to the investigation. But the bureau remained steadfast that investigators should have what they called "exceptional access," and what others called a "back door": built-in software allowing police to decrypt locked phones.

The importance of two-factor authentication

The situation is not as simple as the FBI suggests. Secure phones do provide barriers to police investigations, but they are also an excellent component of strong cybersecurity. And given the frequency of cyberattacks and the diversity of their targets, that's extremely important.

In July 2015, U.S. officials announced that cyberthieves had stolen the Social Security numbers, health and financial information and other private data of 21.5 million people who had applied for federal security clearances from the U.S. Office of Personnel Management. In December 2015, a cyberattack at three electricity companies in Ukraine left a quarter of a million people without power for six hours. In March 2016, countless emails were stolen from the personal Gmail account of John Podesta, chairman of Hillary Clinton's presidential campaign.

In each of these cases, and many more around the world since, a poor security practice – securing accounts solely through passwords – let bad guys do serious damage. When login credentials are easy to crack, intruders get in quickly – and can go unnoticed for months.

The technology to secure online accounts lies in people's pockets. Using a smartphone to run a piece of software called two-factor (or second-factor) authentication makes logging into online accounts far harder for the bad guys. Software on the smartphone generates an additional piece of information that a user must supply, beyond a username and password, before being allowed to login.

At present, many smartphone owners use text messages as a second factor, but that's not good enough. The U.S. National Institute of Standards and Technology warns that texting is far less secure than authentication apps: Attackers can intercept texts or even convince a mobile company to forward the SMS message to another phone. (It's happened to Russian activists, Black Lives Matter activist DeRay Mckesson, and others.)

A safer version is a specialized app, like Google Authenticator or Authy, which generates what are called time-based one-time passwords. When a user wants to login to a service, she provides a username and password, and then gets a prompt for the app's code. Opening the app reveals a six-digit code that changes every 30 seconds. Only upon typing that in is the user actually logged in. A Michigan startup called Duo makes this even easier: After a user types in a username and password, the system pings the Duo app on her phone, allowing her to tap the screen to confirm the login.

However, these apps are only as secure as the phone itself is. If a smartphone has weak security, someone who has possession of it can gain access to a person's digital accounts, even locking the owner out. Indeed, not long after the iPhone debuted in 2007, hackers developed techniques for hacking into lost and stolen phones. Apple responded by building better security for the data on its phones; these are the same set of protections that law enforcement is now seeking to undo.

Avoiding disaster

Using a phone as a second factor in authentication is convenient: Most people carry their phones all the time, and the apps are easy to use. And it's secure: Users notice if their phone is missing, which they don't if a password is lifted. Phones as second-factor authenticators offer a vast increase in security beyond just usernames and passwords.

Had the Office of Personnel Management been using second-factor authentication, those personnel records wouldn't have been so easy to lift. Had the Ukrainian power companies been using second-factor authentication for access to the internal networks controlling power distribution, the hackers would have found it much harder to disrupt the power grid itself. And had John Podesta been using second-factor authentication, Russian hackers would not have been able to get into his Gmail account, even with his password.

The FBI contradicts itself on this important issue. The agency has suggested the public use two-factor authentication and requires it when police officers want to connect to federal criminal justice database systems from an insecure location such as a coffee shop or even a police car. But then the bureau wants to make smartphones easier to unlock, weakening its own system's protections.

Yes, phones that are difficult to unlock impede investigations. But that misses a larger story. Online crime is sharply increasing, and attacks are growing more sophisticated. Making phones easy for investigators to unlock will undermine the best way there is for ordinary people to secure their online accounts. It's a mistake for the FBI to be pursuing this policy.

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

Provided by The Conversation

Citation: Encrypted smartphones secure your identity, not just your data (2018, February 28) retrieved 26 April 2024 from
https://phys.org/news/2018-02-encrypted-smartphones-identity.html