

A Closer Look: Secure your phone without passcodes

August 4 2014, by Anick Jesdanun

Passcodes are outdated. They're a pain to use, and they aren't secure when they are based on easy-to-guess digits, such as a birth date or street address. Many people don't bother using them on phones, even though that means any thief can get instant access to email, banking apps and more. Fortunately, phone makers have started to come up with alternatives to passcodes.

I take a deeper look at those options as I debut an occasional series, A Closer Look. Over the weeks, we'll explore features in various gadgets and services. Rarely does one feature make or break a buying decision, but these elements collectively might push you in one direction or another. And for those who already own these gadgets, it's a way to discover features you might not know about.

—

— FINGERPRINTS:

Apple included a [fingerprint sensor](#) in the iPhone 5s last year. Later, HTC included one on its HTC One Max, while Samsung added it to its latest flagship [phone](#), the Galaxy S5. Samsung's Galaxy Tab S tablets also have fingerprint sensors. With all of these, you can unlock the device with your fingerprint and avoid typing in numbers on the screen.

The iPhone's sensor still works well after nearly a year of use. I begin by training the phone to recognize up to five fingers. To unlock the phone, I

simply touch the home button for about a second. It works when my finger is upside down or sideways, but the sensor has trouble when it's wet or greasy. In such cases, I can go back to using the passcode.

Samsung's approach is similar, except it recognizes only three fingerprints, and it requires you to swipe down on the home button rather than simply touch it. The fingerprint can be used to authenticate purchases using the PayPal app or to unlock the device's private mode, which lets you hide photos and other documents you designate as sensitive.

The HTC One Max's sensor is on the back rather than on the home button. Unfortunately, it often fails to recognize my print. I like that I can instruct the phone to open a particular app automatically depending on the finger I use. The sensor isn't available with the HTC One M8, which came out in March.

Many security experts have expressed concerns that once a finger's compromised, you can't replace it the way you can a passcode.

No one's saying these measures are foolproof. But they are better than no security, which is what happens when people turn off the passcode feature because it's too much of a hassle. Since the passcode can be used as a backup, don't make it easy to guess.

— ANDROID ALTERNATIVES:

Most Android phones have passcode alternatives under "Security" or "Lock screen" in the settings.

Instead of a numeric passcode, you can opt for a regular password. You

improve security by choosing a combination of numbers and letters, some capitalized. You can throw in some punctuation marks, too. Though security improves, convenience drops.

Another option, called Pattern, lets you draw a pattern on the screen. You are presented nine dots, and you must connect at least four of them by swiping on the screen using a pattern you can remember. Your passcode is your fallback.

Though it's easier to swipe than to type, it's actually less secure. Someone with the phone can guess your pattern based on smudge marks on the screen.

—

— KNOCK, KNOCK:

LG's new G3 phone gives Pattern a twist.

Picture a square divided into four quadrants. You create a code by tapping on the various quadrants in an order you'll remember, such as upper left/upper right/lower left/upper right. You need at least three taps, but you can go as long as eight, for more than 80,000 possible combinations.

This approach, known as Knock Code, doesn't leave smudge marks the way Pattern does.

Plus, you have flexibility in the way you define your quadrants. You can divide the entire phone's screen into four quadrants, or you can pick a small corner and divide that into quadrants. That way, you're not being obvious with your taps when you're in a public place. You don't have to choose ahead of time. The phone figures it out.

After six failed attempts, you're required to use your [passcode](#) or sign in with your Google account.

All of these [security](#) measures do make it less convenient to use your phone, as it means an extra step to send a quick text message or view a photo. These alternatives aim to reduce the inconvenience enough that you'll have something in place if your phone falls into the wrong hands.

In a future column, I'll discuss options for finding your phone or wiping out its data remotely, should your phone get lost or stolen. For now, be sure to check out what your phone offers—and use it.

© 2014 The Associated Press. All rights reserved.

Citation: A Closer Look: Secure your phone without passcodes (2014, August 4) retrieved 23 June 2024 from <https://phys.org/news/2014-08-closer-passcodes.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--