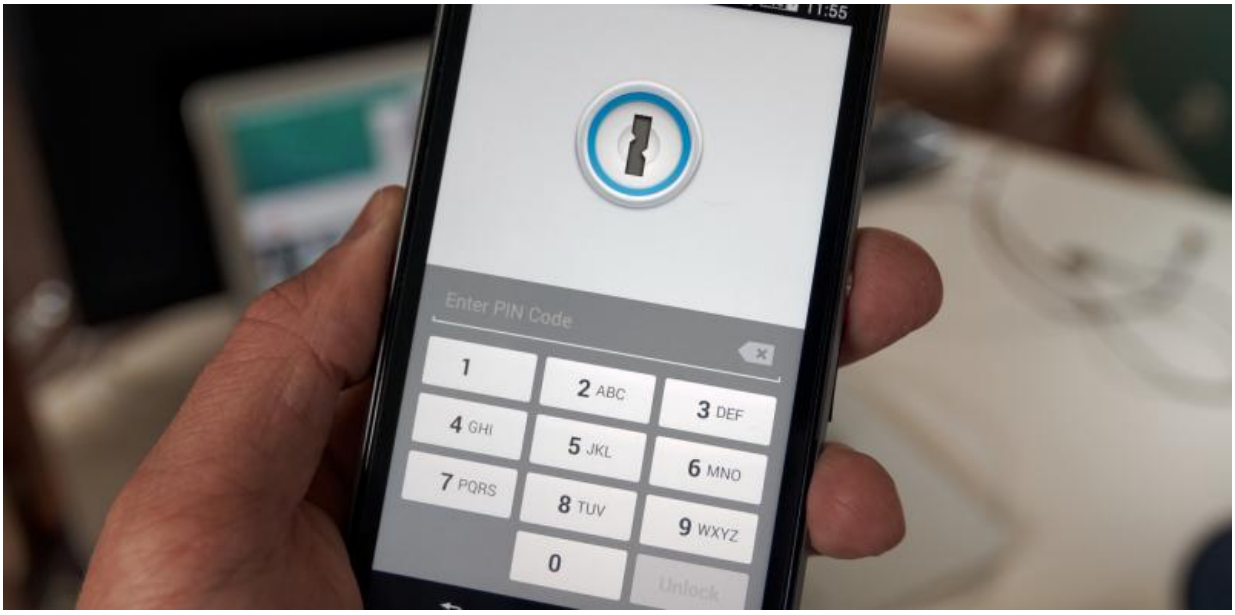
# How secure is your smartphone's lock screen?

April 6 2016, by Clinton Carpene, Edith Cowan University




There’s a big difference between a 4-digit PIN and a 6-digit PIN. Credit: Ervins Strauhmanis/Flickr, CC BY

One consequence of the Apple vs FBI drama has been to shine a spotlight on the security of smartphone lockscreens.

The fact that the FBI managed to hack the iPhone of the San Bernardino shooter without Apple's help raises questions about whether PIN codes and swipe patterns are as secure as we think.

In fact, they're probably not as secure as we'd hope. No device as complex as a smartphone or tablet is ever completely secure, but device manufactures and developers are still doing their best to keep your data safe.

The first line of defence is your lockscreen, typically protected by a PIN code or password.

When it comes to smartphones, the humble four-digit PIN code is the most popular choice. Unfortunately, even ignoring terrible PIN combinations such as "1234", "1111" or "7777", four-digit PIN codes are still incredibly weak, since there are only 10,000 unique possible PINs.

If you lose your device, and there are no other protections, it would only take a couple of days for someone to find the correct PIN through brute force (i.e. attempting every combination of four-digit PIN).

A random six-digit PIN will afford you better security, given that there are a million possible combinations. However, with a weak PIN and a bit of time and luck, it's still possible for someone to bypass this using something like Rubber Ducky, a tool designed to try every PIN combination without triggering other security mechanisms.

**Checks and balances**

Fortunately, there other safeguards in place. On iPhones and iPads, for instance, there is a forced delay of 80 milliseconds between PIN or password attempts.

And after 10 incorrect attempts, the device will either time-out for increasing periods of time, lock out completely, or potentially delete all data permanently, depending on your settings.

Similarly, Android devices enforce time delays after a number of passcode or password entries. However, stock Android devices will not delete their contents after any number of incorrect entries.

Swipe patterns are also a good security mechanism, as there are more possible combinations than a four-digit PIN. Additionally, you can't set your swipe pattern to be the same as your banking PIN or password, so if one is compromised, then the others remain secure.

However, all of these security controls can potentially be thwarted. By simply observing the fingerprints on a device's display on an unclean screen, it is possible to discern a swipe pattern or passcode. When it comes to touch screen devices: cleanliness is next to secure-ness.

## Bypasses

Speaking of fingers, biometrics have increased in popularity recently. Biometric security controls simply means that traits of a human body can be used to identify someone and therefore unlock something.

In the case of smartphones, there are competing systems that offer various levels of security. Android has facial, voice and fingerprint unlocking, while iOS has fingerprint unlocking only.

Generally, biometrics on their own are not inherently secure. When used as the only protection mechanism, they're often very unreliable, either allowing too many unauthorised users to access a device (false positives), or by creating a frustrating user experience by locking out legitimate users (false negatives).

Some methods of bypassing these biometric protections have been widely publicised, such as using a gummi bear or PVA glue to bypass Apple's TouchID, or using a picture to fool facial recognition on

Android.

To combat this, Apple disables the TouchID after five incorrect fingerprint attempts, requiring a passcode or password entry to re-enable the sensor. Likewise, current versions of Android enforce increasing time-outs on after a number of incorrect entries.

These methods help strike a balance between security and usability, which is crucial for making sure smartphones don't end up hurled at a wall.

Although these lockscreen protections are in place, your device may still contain bugs in its software that can allow attackers to bypass them. A quick search for "smartphone lockscreen bypasses" on your favourite search engine will yield more results than you'd probably care to read.

Lockscreen bypasses are particularly problematic for older devices that are no longer receiving security updates, but new devices are not immune. For example, the latest major iOS release (iOS 9.0) contained a flaw that allowed users to access the device without entering a valid passcode via the Clock app, which is accessible on the lockscreen. Similar bugs have been discovered for Android devices as well.

All of these efforts could be thrown out the window if you install an app that includes malware.

So lockscreens, PIN codes, passwords and swipe patters should only be considered your first line of defence rather than a foolproof means of securing your device.

Source: The Conversation