How secure is fingerprint recognition?

From: https://blog.kaspersky.com/fingerprints-sensors-security/10951/

* So if your hands are sweaty in summer or during workouts, your smartphone may dig its heels in and not recognize you
* New technologies are always vulnerable — because they are new.
* [Security experts discovered](http://www.zdnet.com/article/hackers-can-remotely-steal-fingerprints-from-android-phones/) that HTC One Max and Samsung Galaxy S5 smartphones stored fingerprint images in an unencrypted, readable-by-any-app .bmp file — just as a common bitmap picture. Any software, which has access to user’s pictures and Internet, could steal them.
* [ARM TrustZone](https://en.wikipedia.org/wiki/ARM_architecture#Security_extensions_.28TrustZone.29) technology to protect data on their devices. It works with fingerprints images in a [dedicated virtual “world”](http://www.arm.com/products/processors/technologies/trustzone/tee-smc.php), which is not accessible for the main OS. As a result, crucial data (such as fingerprints) cannot leak and be used by the third-party apps. Unfortunately, depending on implementation model, this [technology can also be flawed](https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf).
* Apple smartphones turned to be quite secure, as they encrypt fingerprint data from the scanner.
* An SLR camera with a good zooming lens or even a magazine photo printed in high resolution are enough. By the way, the same [method can be used to fake an iris](https://blog.kaspersky.com/stealing-digital-identity/10386/).
* In general, fingerprint scanner is a great innovation, which is more useful, than harmful. But don’t rely only on it too much — use the new technology wisely and don’t neglect passwords, [two-factor authentication](https://blog.kaspersky.com/what_is_two_factor_authentication/5036/) and other security measures.