Security Best Practices - Part 2d: Fingerprints & Mobile Devices

Travis - 2021-03-16 - Best Security Practices

Part 2D: Fingerprints & Mobile Devices



TL/DR: Don't use your fingerprints as passwords.

Fingerprints are not secure. Fingerprints as passwords are not legally protected. You can't change your Fingerprints but a password should always be changeable.

More and more technology is being released with the addition of a fingerprint scanner; Apple's iPhone, Samsung's Galaxy, Dell's Laptops.... all feature biometric scanners for easy unlocking of the device to prove ownership.

However, fingerprints are insecure. Yes, they confirm who you are. Yes, they're always attached to you. Yes, you don't need to remember anything. No, they're not legally protected... at least not in the US or the UK.

In the United States, defendants have the right not to testify against themselves under the Fifth Amendment and providing a pass code or password can be considered testimonial. However biometrics (DNA, fingerprints etc) are not protected.

In the United Kingdom, you can be mandated by court warrant to divulge your password under the The Regulation of Investigatory Powers Act (RIPA), Part III. Failure to comply can result in imprisonment. However, a court order is not needed to force a person to unlock a device by fingerprint.

Until there are significant changes in legislation and security, fingerprints as passwords will continue to be insecure.

Tags

Security