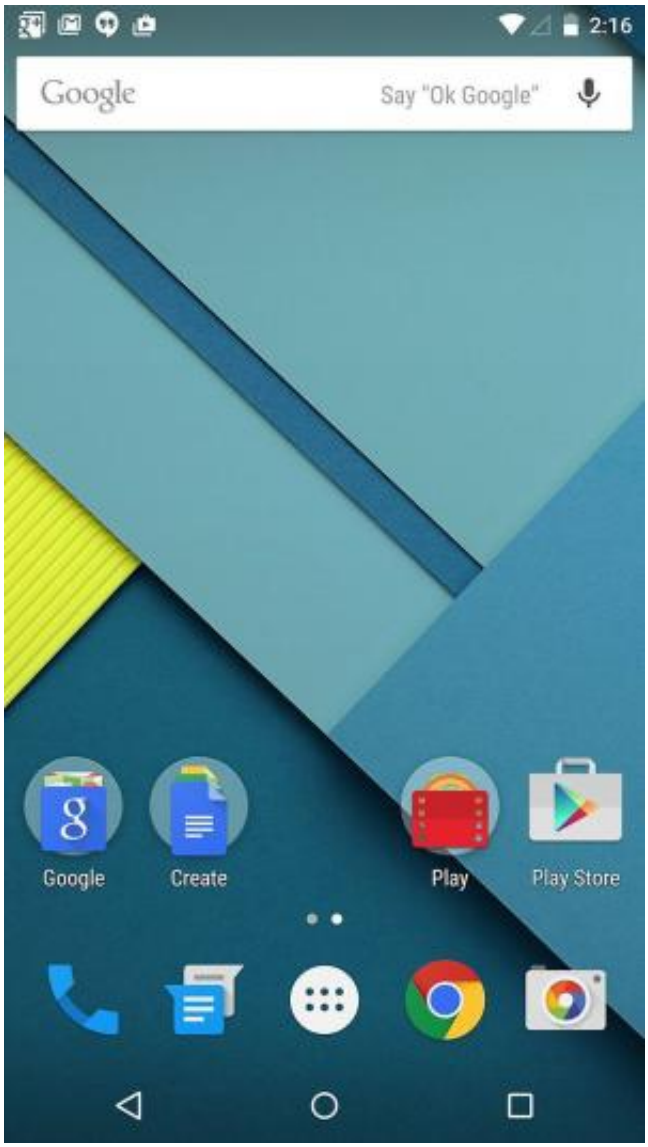
Google eyes shift from passwords sooner than you may think

29 May 2016, by Nancy Owano



Is this a dream or an answer to yours? Is Google really set to kill the password on Android—in 2016? Wait, that is this year. The headlines are not a dream. Google is to ditch passwords in favor of a biometrics means for authentication.

Google could replace passwords with a Trust Score on devices running Android. Madhumita Murgia, *The Telegraph*, said the system would use biometrics, "unique signatures like your typing pattern, your face and your location - to figure out whether it's really you, rather than relying on a password."

The news is according to plans that emerged from the recent Google I/O developers conference, said *FindBiometrics*.

Daniel Kaufman, head of Google's Advanced Technology and Projects (ATAP) team, said the company was aiming to replace passwords on Android devices with passive authentication by the end of 2016.

Google's Project Abacus, with a goal of killing the password, was initially launched to find password replacements but it evolved into "an investigation focusing on passive authentication factors such as facial recognition, behavioral biometrics, and metadata like geolocation information," said *FindBiometrics*.

Geolocation information? *The Telegraph* said "The search giant has already been experimenting with nascent biometric unlocking systems. For instance, the 'Smart Lock' feature means you can unlock your Android phone in a preset trusted location, without a password."

A company team was working on a system that would leverage data collected through a mobile device's camera and sensors for a Trust Score, which in turn would determine if a user can be accurately authenticated.

Kaufman, as reported in *The Telegraph*, explained how this would work: Google will provide app designers with a Trust Score API that can integrated into any app. "Banks will be testing the API starting next month, he said." Ashley Carman

in *The Verge* said that the API is rolling out to "several very large" financial institutions in the coming weeks.

"Assuming it goes well, this should become available to every Android developer around the world by the end of the year," said Kaufman.

What exactly is this Trust Score about?

The scores incorporate various data points about users to determine whether or not they're legitimate, said *The Verge*. Murgia in *The Telegraph*: "Your Android phone is constantly collecting background data on your typing habits and locations so it forms a signature of who you are over time. Using this data, it gives you a score of whether it trusts you or not."

Long and short of all this is that "The way Project Abacus works is that instead of relying on passwords or two-factor authentication to open your Android phone, your device will instead authenticate you based on how you used your device," wrote Tom Spring in *Threatpost*.

That Truth Score could make use of information such as "keystroke speed, pattern of speech, location, rhythm of your walk, facial features, the way you swipe open your phone," said Spring.

Meanwhile, Google is not the only tech giant making footprints in the sand. A team from Microsoft has moved to nix the use of common or simple passwords that may be easy to guess or have already appeared in breach lists. action has been taken regarding the Microsoft Account and Azure AD system by dynamically banning commonly used passwords.

In a May 24 blog, the news was that "This service is already live in the Microsoft Account Service and in private preview in Azure AD. Over the next few months we will roll it out across all 10m+ Azure AD tenants."

CBC News reported this on Friday. "In a blog post, Microsoft said it has rejigged its password policies in an attempt to stem the flow of password breaches."

Interestingly, users who think they are smart in composing complex passwords are also potential sitting ducks. As it turns out, many users think up similar patterns—put a capital letter in the first position, a symbol in the last, and a number in the last two, said CBC News.

Carrying reactions to Microsoft's password news, *Information Security Buzz* quoted Jonathan Sander, VP of Product Strategy at Lieberman Software: "The point isn't to make the passwords impossible for you, but rather to ensure you don't use something so well known that it's on every bad guy's short list of passwords to guess."

He also said, "Microsoft analyzing passwords to keep a dynamic list of password values too weak to use safely is excellent for everyone."

Brian Spector, CEO of MIRACL, said, "Microsoft's move doesn't fix the underlying problem that passwords just aren't secure enough to protect the personal information that we all store and access online today. The IT industry needs to get over passwords all together. They don't scale for users, they don't protect the service itself and they are vulnerable to a myriad of attacks.

Spector also pointed out that "The most attractive attack vector for cyber-criminals is not the individual user's vault that store passwords, but the database on the provider side that stores all user passwords."