Will the hack of 500 million Yahoo accounts get everyone to protect their passwords?

September 26 2016, by David Glance

How to Hack Yahoo. Credit: The Hacker News

Yahoo has confirmed that account information of around 500 million users was stolen by hackers in 2014. This hack, which Yahoo blamed on a foreign "state-sponsored actor", could have been part of, or following on from, an earlier breach in 2012 in which 450,000 accounts were compromised.

Other than the immediate concern of a password being compromised,

there is additional information that was stolen such as the answer to security challenge questions, phone numbers, linked email addresses and dates of birth.

The latest hack is the latest in a regular succession of incidents with large organisations in which account information has been stolen and compromised. And this is only the times when specific organisations have lost large scale numbers of user account information. The everyday compromise of accounts and passwords through malware and phishing attacks is ongoing and persistent.

Given how hard it has been to keep passwords secure, companies have been looking at alternative approaches. Ironically enough, given the poor security that lead to the loss of 500 million accounts, Yahoo is one of the companies that has introduced technology that has tried to do just that.

In 2015, Yahoo introduced a service called Account Key. Account Key works by using push notifications to a Yahoo app on your mobile phone that will pop up a screen asking whether you are trying to sign in to another Yahoo app anywhere else. It will then provide an key consisting of letters that you type into the login window of the other app.

Other than the initial setting up of Account Key, you don't need to use a password again. Google has been experimenting with a similar system and right now, the Google app can be used as the second factor in 2 factor authentication.

This type of password-less login is different from 2 factor authentication which is another approach to add protection to the use of a password. In 2 factor authentication, which you can use on Apple iCloud, Google, Facebook and other accounts (including Yahoo), users still use a password but also use an app on their phone to provide an access key that is available for a limited time when a user logs in. 2 factor

authentication works on the principle of using "something you know", i.e. your password, and "something you own", i.e. your phone.

Apple and others have been introducing biometrics to act in the place of passwords and pins on apps on iPhone and Android phones. The fingerprint sensor on iPhones and phones like the Samsung Galaxy range of phones can be used to access many apps. Whilst this is convenient, it doesn't replace passwords or pins entirely because these are still needed periodically and so theoretically passwords could still be compromised if the system, or its data, was accessed.

Likewise Apple's new feature on MacOS Sierra whereby an Apple Mac can be unlocked automatically using an owner's Apple Watch. Again, a password is still needed for the system, the Apple Watch just becomes a convenience feature to access the system quickly when in regular use.

2 factor authentication is still by far the safest way to protect against hackers getting access to a system even if they have managed to get a password. If accounts from Google and Facebook are being used to authorise access to other apps, it becomes even more important that these accounts in particular are protected. Even though Google's and Facebook's security is considered to be very good, the security of the system doesn't protect an individual's account details from being compromised through a targeted attack like phishing.

Yahoo has managed to dispense with passwords but the system does rely on the user having access to their phone, having a working network and that phone itself having security applied to it. Also, because the Yahoo mail app for example is always logged in, in order to provide Access Keys, anyone getting access to the unlocked phone can get access to a user's Yahoo Access Keys. Even with 2 factor authentication, keeping the phone protected becomes critical because if it is lost, it could provide the person who has it with the means to reset passwords and get access to

all accounts it is protecting.

The advice to anyone still using Yahoo (which by now must be a rapidly diminishing number) has been to switch to 2 factor authentication, or use Google instead.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation