

Uber was hacked, so change your password right now. Here's what else you need to know

November 24 2017, by Rohan Miller, David Oliver



Uber has admitted that a 2016 [data breach](#) put at risk the personal information of 57 million Uber users worldwide and at least 600,000 drivers in the United States.

The ride-share firm's CEO [said](#) that:

two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use.

Now it has [been reported](#) that Australian riders and [drivers](#) are part of the data [breach](#).

It would be prudent for Australian Uber users and drivers to change their passwords as soon as possible. Here's what else you need to know:

If you use Uber, your name, email address and mobile phone number may have been leaked

Uber [says](#):

Rider information [put at risk in this data breach] included the names, email addresses and mobile phone numbers related to accounts globally. Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded.

Breaches of this kind can mean an increase in people receiving spam email. Some experts have [said](#) that any personal information could be worth something to criminals.

What evidence is there that the hack included data from Australian users of Uber?

The public disclosures Uber has made so far make it very difficult to identify Australians caught up in the data breach. That's because the firm was not very transparent about it.

Media reports that Uber worked hard to [conceal the data breach](#) suggest

Uber's corporate governance needs improvement.

In its recent [statement](#) on the data breach, Uber CEO Dara Khosrowshahi acknowledged the firm's "failure to notify affected individuals or regulators last year" and promised to do better.

I'm an Uber driver. What do I need to know?

Uber has [said](#):

Driver information included the names, email addresses and mobile phone numbers related to accounts globally. In addition, the driver's license numbers of around 600,000 drivers in the United States were downloaded.

As with the message to riders, Uber says it has seen no indication that trip location history, [credit card numbers](#), bank account numbers, Social Security numbers, or dates of birth were downloaded.

The firm says that it is directly notifying affected drivers by mail or email, and is offering them free credit monitoring and identity theft protection – but, in any case, it's a good idea for any Uber driver to change their password.

The longer-term issue is that news of the hack might conceivably dissuade some people from using Uber at all, which would be bad news for drivers.

So a fundamental part of Uber's crisis management strategy should be educating drivers on how to respond to consumer questions about data privacy. This will not only assure the drivers but also help rebuild the trust of customers.

That said, it is pre-Christmas party time in cities throughout the world,

and that means boom time for the Uber, taxi and personal transport industries.

So it's easy to imagine there would be only a small impact on Uber drivers over this period.

What's the cost of online convenience?

Uber is not the first and won't be the last to be involved in a data breach. As transactions are increasingly made over the internet, it is highly likely Australians will fall victim to more and more data hacks.

Consumers who may be left out-of-pocket, receiving increased spam email and risking other privacy breaches such as identity theft may be less than loyal to firms that don't look after their data.

Moreover, as there is [money and influence to be gained](#) through online data crime, it is highly likely that criminals will become better organised to reap the incentives in a very strategic manner.

It's worth remembering that, in many cases, the cost of convenience for using a service over the internet is your private information.

Many [people](#) do [not read the terms and conditions](#) they agreed to for internet transactions, and they may be shocked by the level of exposure they face.

Consumers accept financial and privacy risk by trading over the internet, all for the sake of cheap tickets, discount car rides and other conveniences.

As these breaches happen more often, it may be impossible to totally avoid one's exposure to internet-based transactions and online data

storage. So there will likely be increasing pressure on politicians and regulators to add some real teeth to prosecutions (although many seem to be based in difficult-to-prosecute jurisdictions).

The Australian government's [notifiable data breach scheme](#) will start on February 22, 2018. It only applies to eligible data breaches that occur on, or after, that date.

How can Uber prevent this from happening again?

In the short term, Uber says it has "implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts".

The longer-term problem is changing the attitudes that led to the [data breach](#) being concealed for so long.

When Dara Khosrowshahi took over as Uber's CEO last August, hopes were high that he would soften some aspects of the extreme-performance culture that led to earlier ethical lapses in Uber.

There may be a perception among consumers that the firm's desire to keep secret its intellectual property relating to algorithms has spread to its broader operations.

A good start for Uber would be to increase its public reporting on its operations. A widely publicised code of ethics, whistleblowing protections and ethics training for all staff would certainly not go amiss.

Rohan Miller, Senior Lecturer, Marketing and Digital Business,
University of Sydney and David Oliver, Senior Lecturer in Management,
University of Sydney

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation

Citation: Uber was hacked, so change your password right now. Here's what else you need to know (2017, November 24) retrieved 10 April 2024 from <https://phys.org/news/2017-11-uber-hacked-password.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--