BIZCOMMUNITY

57 million riders, drivers affected by Uber breach

By Simon Campbell-Young

13 Dec 2017

Global transportation technology company Uber Technologies has admitted it suffered a breach that saw hackers stealing the personal information of approximately 57 million customers and drivers.

So how did it happen?

It was reported that two hackers gained access to a private area of the online resource for developers dubbed “Github”. From that point, the threat actors found the transport giant’s login credentials for Amazon Web Services (AWS) - a cloud computing platform used by myriad companies to store all sorts of data, including apps.

As if that isn’t bad enough, the company is now in hot water, as it failed to disclose the breach for nearly a year. It has also been claimed it paid off hackers to destroy the data. Uber is now facing a multimillion-dollar consumer protection lawsuit.

Database of 30 million+ South Africans leaked online, property group is culprit

Ilse van den Berg 19 Oct 2017

The breach exposed the names and driver’s license numbers of about 600,000 drivers in the US, and other personal information of all 57 million Uber users and drivers around the world, including names, email addresses and mobile phone numbers. The company insisted its forensics experts saw no evidence that trip location history, credit card numbers, bank account numbers, social security numbers or dates of birth were compromised, and said it is monitoring the affected accounts and has flagged them for extra fraud protection.

It says it had notified affected drivers whose driver's license numbers were compromised, and is giving them free credit monitoring as well as identity theft protection.

Although Uber believes no action is needed, we still need to be aware of other factors when breaches of this scale take place. When well-known entities attract attention in the news, threat actors could try to use the conversation around these incidents to their advantage.

Safeguarding your customers against the threat of identity theft

Wynand Smit 17 Nov 2017

One way they could do this is through phishing attacks, or emails that appear to come from Uber, in an effort to fool unwitting users into disclosing sensitive data, including account credentials or payment card information. In any event of this nature, it is advisable to go directly to the source, and get updates only from the organisation's official Web site. Be suspicious of mails claiming to be from Uber, and under no circumstances click on any links or attachments in the mails.

"No company's data is safe"

The bottom line is that Uber was not prepared, and didn't handle the incident well. Even with the latest and most advanced threat protection technologies, no company's data is safe. There's no silver bullet when it comes to cyber security. Businesses have to ensure they are covered in the event of a data breach.

Cyber insurance

Had Uber had cyber insurance in place, it could have saved itself a whole world of pain.

> *"Cyber insurance is highly specialised, and designed specifically to help protect organisations, as well as help them recover in the event of a security incident. Cyber events come in all shapes and sizes, and can be catastrophic for businesses."*

Similarly, cyber insurance protects individuals. Should any Uber customers have money stolen out of their credit cards, the insurance would cover this.
Cyber insurance offers cover for hardware damage, data loss or corruption, cyber liability and crime, expenses covering recovery and loss of income. Moreover, it covers bringing in specialists to minimise damage to reputation and loss of confidence - something I bet Uber wishes it has now.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Adding threat intelligence to the security mix - 26 Nov 2018
- Digital forensics is crucial to the security chain - 6 Nov 2018
- App permissions can be used to exploit your data - 26 Oct 2018
- 57 million riders, drivers affected by Uber breach - 13 Dec 2017
- Prevention through awareness - 12 May 2014