Uber hacked by teenager demanding higher pay for drivers

C
ybersecurity policies at Uber were called into question today after the ride-hailing app was forced to shut down its staff messaging service following a security breach on its computer network.

The hacker who claimed responsibility for the breach said he was 18 years old, according to the New York Times, and called for Uber drivers to receive higher pay. He claimed to have been able to access to the company's email and cloud storage systems, and said the firm had weak security standards.

He was able to gain access to an Uber worker's Slack account posing as an IT assistant and sent messages to Uber employees which read: "I announce that I am a hacker and Uber has suffered a data breach."

Uber's Slack system was taken offline as a result of the hack, with staff told the firm's security workers "don't have an estimate right now as to when full access to tools will be restored" in an internal email seen by the New York Times.

San Francisco-based Uber has faced criticism in the past for its handling of cybersecurity incidents. In 2016, the firm paid a $100,000 ransom to hackers to delete records of millions of driver and rider accounts stolen from the company. Uber's security chief, Joe Sullivan, was fired by the company for his role in the debacle, and was charged with obstructing justice for keeping the security breach a secret for more than a year.

Read More

- Frasers Group rejected by Australian fashion platform MySale on takeover bid
- FTSE 100 Live: Retail sales slide, FedEx warning hits US market
- Customers tightened belts in August as they bought fewer items and spent less
-  BRANDPOST | PAID CONTENTHow Uber is helping the rollout of charging points across London

In a tweet, Uber said: “We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available.”

In a statement to the Reuters news agency, Slack said it was investigating the incident and that there was no evidence of vulnerability on its network.