Bunnings' drive and collect customer data caught up in FlexBooker security breach on Amazon cloud

Canberra Times, January 12

https://www.canberratimes.com.au/story/7578921/bunnings-customers-data-exposed-in-cyber-security-breach/

Bunnings has emailed its customers about a data-security breach involving a third party.

Bunnings' customers using the company's COVID-triggered drive and collect service may have had some of their personal data exposed after the software firm behind the service experienced a major security breach that affected 3.7 million people worldwide.

Online booking platform FlexBooker said that on December 23, its account on Amazon's cloud platform was compromised after its data storage was accessed and downloaded.

In an "incident alert", FlexBooker said they worked to restore a backup within 12 hours.

"After working further with Amazon to understand what happened, we learned a certain set of data, including personal information of some customers was accessed and downloaded," it said.

This included first and last names, email addresses and phone numbers."The data accessed did not include credit card or other payment card numbers," it said.

In an email to customers on Wednesday afternoon, Bunnings said it was recently made aware of the breach, which may have "included the name and email address you provided when selecting a timeslot for a previous Bunnings drive and collect order".

"We take the privacy and the protection of customer information very seriously and we sincerely regret that this has happened," the email reads.

Organisations need to be proactive in protecting personal information and preventing these breaches. ***Office of the Australian Information Commissioner spokesperson***

Bunnings assured customers that "passwords, credit card information and mobile numbers are not collected when using Flexbooker to make a booking with us. We are confident that none of these categories of customer data have been compromised."

The email goes on to say that Bunnings is "currently working with FlexBooker to further understand how the breach occurred in their systems and the extent of the impact".

"We're reaching out directly to any customers whose name or email address may have been accessed," the company said.

Bunnings said that while customers were not required to take action, they were encouraged as a precaution to "be cautious of any unusual activity in their email accounts and to regularly change passwords to enhance online safety".

"At Bunnings, keeping your personal information safe and secure is our priority," it said.

The company's chief information officer, Leah Balter, said they "will carry out a thorough investigation into this incident".

Bunnings, which introduced the drive and collect service in April 2020 at 250 stores across Australia in response to COVID, said it had notified the Office of the Australian Information Commissioner (OAIC). An OAIC spokesperson said they could not speak about specific cases, but they expected "any organisation responding to a data breach involving personal information to act quickly to contain the incident and assess the potential impact on those affected".

"If it's likely to result in serious harm and the organisation is covered by the *Privacy Act*, they must notify the people who are affected and the OAIC as quickly as possible," the spokesperson said. The OAIC received 446 data breach notifications under the mandatory Notifiable Data Breaches scheme from January to June 2021.

Forty three per cent of those breaches resulted from cyber-security incidents. "Organisations need to be proactive in protecting personal information and preventing these breaches," the spokesperson said.

"We advise individuals to respond quickly when they're notified and take the appropriate action, such as changing passwords, checking accounts and credit reports, and watching out for scams."

Australian security expert Troy Hunt, who runs the Have I Been Pwned website, tweeted 3.7 million accounts were breached and that partial credit card data were also taken.

A FlexBooker spokesperson confirmed that report to *ZDNet*, sayingthe last three digits of card numbers were included in the breach but not other data. FlexBooker, which also serves other industries including health and the arts, has been contacted for further details about the breach.

In its incident alert, it also said customer passwords included in the data were encrypted and the encryption key was not accessed or downloaded.

It has since restored the security of its account and "will continue to work with Amazon to maintain security".