News Brief

Over 70 Million AT&T Customers' Data Exposed in Data Breach

On Saturday, March 30, 2024, telecommunications giant AT&T released a statement saying current and former customer data was exposed on the dark web.

AT&T account numbers, Social Security numbers, email addresses, names, phone numbers and birth dates may all have been among the compromised data.

"Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders," the company said in its statement.

> **"AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago."**
>
> **- AT&T press release**

Was I Affected?

Affected AT&T customers should be notified by the company. This may come in the form of an email or letter. AT&T began notifying customers on Saturday.

AT&T said it reset customer passwords, and individuals will be prompted to change them.

Will This Happen Again?

AT&T is currently investigating the situation. Specifically, the company is trying to determine if the compromised data originated from AT&T or one of its vendors.

Regarding future potential data exposure, some risks will always be present; AT&T, T-Mobile and other companies experienced data breaches just last year. In today's connected world, there is always some possibility that data provided online could be compromised. That's why it's critical to avoid reusing passwords and other login details across accounts.

Can I Better Protect My Data?

Unfortunately, there's nothing people can do to prevent organizations from having data exposed. However, there are some steps individuals can take that may better protect their information, such as the following:

- Utilize credit-monitoring services. AT&T said it would cover such costs for applicable parties affected by this latest data breach.
- Use unique, strong passwords across accounts.
- Enable multifactor authentication to make it harder for unauthorized logins.
- Check bank and account activity regularly for suspicious transactions. Consider a credit freeze as necessary.
- If notified about a data breach from a company, follow all recommended guidance, especially regarding password resets.

Following a breach notice, be especially vigilant for phishing scams or similar tricks, which may be tailored using your personal information.