How to protect your personal info after AT&T's data breach

July 15 2024, by Irving Mejia-Hilario, The Dallas Morning News

Credit: Unsplash/CC0 Public Domain

Dallas-based telecommunications company AT&T revealed its second data breach of the year on Friday morning, a leak that affects more than 100 million U.S. customers.

The cause of the breach was not a breakdown of company servers, the company said, but a malicious actor who illegally broke into an AT&T workspace from a remote platform. The data compromised contains communication records from May 1 to Oct. 31, 2022, as well as on Jan. 2, 2023. The concerned data was not taken on those dates, but from those dates after the fact.

The company's first data breach of the year occurred roughly a month before the larger breach was uncovered. Nearly 73 million current and former AT&T companies had social security numbers and names leaked onto the dark web, opening them up to potential identity fraud and other dangers.

The data breaches could pose serious risks to those affected and open up users to becoming victims of identity fraud. However, there are some steps AT&T account holders can take right now and in the future to prevent the impact from becoming worse.

"In today's day and age, third parties have your data. It's just a fact of life that we all have to live with," said Mitch Thornton, executive director of the Darwin Deason Institute for Cybersecurity at Southern Methodist University. "All you can do is protect yourself, your systems and your access to third-party accounts."

AT&T said it will notify users who have been affected through mail or email. The company has also said it has begun an investigation to determine what the cause of the data breach was and is offering affected customers complimentary identity theft and credit monitoring services.

But, in the meantime, here are some steps you can take to protect yourself and your private information.

The basics

Criminals who steal private data often sneak small purchases in between larger bills in the hopes users won't notice it, Thornton said. Checking credit should be the first step most people will need to take, he said.

"Monitor your credit for suspicious activity. Don't just pay your credit card bills and whatnot without going through your transactions," Thornton said. "Oftentimes, these criminals will make a small purchase just to test if you're monitoring your accounts. You'd be surprised at the kinds of stuff you might find."

Resetting passwords and applying two-factor authentication, a security system that requires two different forms of identification, should always be in place to be the most well protected. But if users haven't already, doing both is crucial at a time like this.

Resetting a password every six months, while time-consuming, could save individuals a headache down the road, Thornton said.

"A lot of people choose not to do either of them, because it's an inconvenience. Every time you log in, you have to do more work and people could forget passwords," he said. "But in cases like this, it could help you because the adversaries have your password, but they may not have your cellphone so they might not be able authenticate you fully."

Though it might be a pain, applying credit freezes and locks could also be helpful. Though they both block individuals who have not been authorized to have access to credit reports, their main differences are in cost and how quickly it goes into effect.

Credit locks are typically services that cost users between $10 to $25 and can be applied instantly, while credit freezes are usually free but can take longer to go into effect—sometimes up to five business days.

For users who are especially concerned, purchasing and using security software, while too late in the case of protecting data that AT&T stored, could prove to be helpful in the future, Thornton said.

"No matter what security software you have on your end systems at home, it wouldn't have helped here because they didn't attack you, they attacked your data that's held by a third party," he said. "However, I would always tell people for their home systems that they should use security software."

What might come next?

AT&T account holders will need to watch their email inboxes and their mailboxes.

However, there's still a chance that cybercriminals will take advantage of that too, Thornton said.

"If someone calls you up, or sends you an email that says, 'Hey, we think you're one of the people who have been affected. You need to authenticate information so send us your password,' don't do that," he said. "You can always say you can provide it, but contact AT&T separately and ask them to verify that they're actually the ones contacting you."

With private information out on the dark web, the stakes are raised for affected individuals and they need to take precautionary steps, Thornton said.

"Your data is already out and available on the dark web. Usually, that is sold from one criminal to another and the threat of identity fraud is much higher," he said. "I know it's time-consuming, but I highly suggest taking steps to protect yourself."

2024 The Dallas Morning News. Distributed by Tribune Content Agency, LLC.

Citation: How to protect your personal info after AT&T's data breach (2024, July 15) retrieved 17 July 2024 from https://techxplore.com/news/2024-07-personal-info-att-breach.html

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.