May 2024

In the Loop

CDC Drops 5-day Isolation Guidance for COVID-19

On March 1, 2024, the Centers for Disease Control and Prevention (CDC) released new guidance for individuals who test positive for coronavirus (COVID-19).

For the first time since 2021, the agency loosened its COVID-19 isolation guidance to better reflect the virus's evolving risk as hospitalizations and deaths from COVID-19 dropped.

Individuals who test positive for COVID-19 no longer need to stay home from work and school for five days. Isolation is no longer necessary if the individual has been fever-free for at least 24 hours without the aid of medication and overall symptoms are improving. Once people resume normal activities, they are encouraged to take preventive measures—such as washing their hands often and cleaning frequently touched surfaces—for the next five days to curb the spread of disease.

The CDC further noted that this change streamlines its guidance for respiratory viruses. That means Americans can manage COVID-19 like they do for influenza and respiratory syncytial virus (RSV). While every respiratory virus is different, a common approach to limiting the spread of disease makes the CDC's recommendations easier to follow and more likely to be adopted. Other countries, including Britain, Australia, France and Canada, have implemented similar guidance and found no significant change in the spread of COVID-19.

Staying Healthy

The latest CDC guidance changes reflect the progress made in protecting Americans against severe illness from COVID-19. Regardless, the CDC offers the following tips for reducing the spread of COVID-19:

- Get vaccinated with the latest version of the COVID-19 vaccine.
- Cover coughs and sneezes.
- Wash hands frequently.
- Clean frequently touched surfaces.
- Increase ventilation by opening windows and using air purifiers.

People at higher risk for severe complications from COVID-19, such as those who are pregnant or have a weakened immune system, may need to take additional precautions. The CDC recommends that adults 65 and older get a COVID-19 booster shot this spring in anticipation of an uptick in the virus later this summer. Talk to your primary care physician if you have any vaccination questions or concerns.

fifs Franconia Insurance & Financial Services
KEYSTONE

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

On March 30, 2024, telecommunications giant AT&T released a statement saying current and former customer data was exposed on the dark web. Based on a preliminary analysis, the data set appears to be from 2019 and earlier, impacting roughly 7.6 million current AT&T account holders and 65.4 million former account holders.

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

Was I Affected?

The company should have notified affected AT&T customers by email or letter.

AT&T reset customer passwords, and individuals were prompted to change them. The company will also cover credit-monitoring costs for applicable parties affected by this latest data breach.

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. In fact, 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 avoiding reusing passwords and other login details across accounts is critical.

How Can I 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.
- 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 you've been notified about a data breach from a company, follow all recommended guidance, especially regarding password resets. In addition, be especially vigilant for phishing scams or similar tricks, which may be tailored using your personal information.