NEIGHBORHOOD WATCH NEWSLETTER, JULY 27, 2020

DID YOU ORDER GROCERIES ONLINE?

Lately, any time you leave your home, you risk being exposed to the coronavirus.

Consequently, people are shopping for supplies and groceries online more than ever. Thanks to advancements in same-day shipping and delivery, you can even get fresh groceries brought to your door in a matter of hours. **Tap or click here for our complete guide to online grocery shopping.**

But consumers aren't the only ones paying attention to the online shopping boom. **Hackers and scammers are targeting delivery services for personal data**! It's been learned that one of the largest grocery delivery services has been hit by a massive data leak. Making matters worse is that the company claims no data breach has occurred, and nobody knows how it happened.

According to Buzzfeed News, data from what appeared to be hundreds of thousands of Instacart customers emerged on at least two dark web marketplaces. A total of 278,531 accounts were listed for sale, and the data doesn't appear to be old or outdated, either. In fact, some profiles appear to contain data as recently as the day before the listings were officially posted to the Dark Web.

% • Folate
10%
values are based on a 2,000
daily values may be higher
your calorie needs:
2,000 2,500
80g 25g 300mg 2,400mg 375g 30g
WHEAT FLOUR (FLOUR, NIACIN, REDUCED
FOLIC ACID), CHEDDAR CHEESE
CANOLA AND/OR SUNFLOWER OIL
YEAST EXTRACT, WHEY, AUTOLYZED
PAPRIKA EXTRACT FOR
CHEESE (MILK, CULTU

If that wasn't concerning enough, Instacart's response to the matter was even more chilling. Speaking to Buzzfeed News, an Instacart spokesperson stated they were "not aware of any data breach at this time," and speculated that the data may have come from account phishing efforts outside of the platform.

In order for that logic to make sense, that would mean hackers behind the leak were compiling and separating phished data from wider campaigns. To Instacart's credit, the service does have millions of subscribers and were the site itself breached, it's likely the number of stolen accounts would be far larger.

But even still, it's worrying that Instacart doesn't have an explanation as to why this data is floating around in the first place.

The stolen data includes several pieces of personally-identifying information like names, order histories and the last four digits of subscribers' credit card numbers. On their own, these data points may not pose too much risk, but combined and matched with other pre-existing leaks, it might be possible for hackers to use the data to commit fraud.

Worried if you were part of a previous data breach? Tap or click here to discover a site that wills how you your risk.

If You Use Instacart. How Can You Protect Yourself And Your Data?

Unfortunately, it doesn't appear that Instacart has notified potential victims if their data is being sold on the Dark Web at this time. So if you use the platform, you should act under the assumption that your data is at risk and take the necessary steps to protect yourself.

To get started, you should **first make sure you're not part of any other data breaches.** You don't want the Instacart hackers matching your data with other leaks to gain even more access to your accounts.

To check if you were targeted by another hack or breach, visit **HaveIBeenPwned. On the website, type in your email address and verify if your accounts have been discovered in any additional breaches**. **Tap or click here for more details on HaveIBeenPwned**.

If you find you've been exposed previously, **log into your email account and immediately change your email password. If you share that password with any of your other online accounts, change those too as soon as you possibly can.** Otherwise, hackers may try to crack all your accounts with the data they have on hand.

Lastly, **check if any of your accounts offer two-factor authentication as a security feature.** This will block hackers from going into your accounts any further without physical access to your smartphone. **Tap or click here to see how to set up 2FA.**

(SOURCE: JAMES GELINAS, KOMANDO.COM)