Cloudbleed: What You Need To Know About The Latest Data Breach

For as easy as it makes most aspects of our lives, the internet is far from simple. Services you've never heard of can make a huge impact on your life. That's what we learned from last week's data leak from Cloudflare, a distributed computing technology service. The leak has been dominating headlines, where it's earned the name "Cloudbleed," an homage to 2014's "Heartbleed" leak.

While Cloudbleed is nowhere near as serious, it still represents a threat to the security of millions of people. Cloudflare was used by many popular websites. Here's what you need to know to keep yourself safe.

What happened?

Cloudflare is what's called a content management service. It serves as a middleman in a lot of internet information exchanges. For example, your browser sends a request to a webpage, which is routed through one of Cloudflare's servers. Cloudflare verifies that it's a legitimate request as opposed to a bot or malicious attack, then passes the request on to the website. The website sends data back to you through Cloudflare. Cloudflare provides security against various kinds of attacks, so websites are safer and faster.

The problem is that Cloudflare didn't always clean up one request before moving on to the next. Bits of data were being sent along with web pages that contained information from previous requests. Some of these bits of data included sensitive information, like usernames and passwords.

No one attacked Cloudflare. This was just a bug in their code that resulted in the accidental release of sensitive data. This means it's less likely that compromised information will be used maliciously, but it doesn't mean Cloudbleed can be ignored.

Who's affected?

Cloudflare was a very popular service for websites. Over seven million sites used Cloudflare at the time of the leak. Some of the biggest names on the list are fitness site Fitbit, dating site OkCupid, and review service Yelp. Perhaps the biggest danger was from password manager 1password, which may have revealed password information to other sites. 1password was quick to point out that only encrypted data had been released, so the danger to its users is very small.

The timeframe of the leak goes as far back as September 2016, so if you've used one of these sites in the past five months, your personal information may have been released. Since it becomes part of a website, it can then be stored by search engines. Yahoo, Google and Bing have worked together to eliminate the storage of personal information, and Cloudflare has fixed the bug in its code.

While a lot of data could have been affected, not much of it actually was. About one in every 3.3 million web requests turned up unwanted data. Some of that was just information, like messages from dating sites or hotel bookings. Very little of the compromised data was password information. Still, since it's hard to prove your data wasn't affected, it's best to act as though your login information is compromised.

What do I need to do?

There are three steps every internet user needs to take right now. First, change your passwords. It's very unlikely that anyone has not used a Cloudflare site, and that use could mean risk in a data breach. Create new, strong, unique passwords for each site. One good strategy is to put together four words that you think about when you look at the service. This creates a password that's easy for you to remember, but difficult for a machine to guess.

Second, keep an eye on your account statements. Most often, identity thieves will use information to try to make illegal purchases or cash advances. If you notice any suspicious activity, report it immediately.

Third, where you can, enable two-factor authentication. Two-factor authentication adds another layer of security between would-be thieves and your accounts. In order to log in to your service, you'll need both a password and a one-time code, usually sent to email or a cellphone. Using two-factor authentication not only stops thieves in their tracks, but it also notifies you that someone is trying to gain access to your accounts.

While Cloudbleed isn't the biggest danger on the internet, it's still a good reminder that we need to keep our guards up while surfing the web. Just because a page uses a password doesn't mean it's always secure. Of course, Cloudbleed also reminds us of one of the ironclad rules of internet security: When in doubt, change your passwords!

Your Turn: What practices do you use to stay safe online? Let us know your best tips in the comments!

SOURCES*:

https://sciencealert.com/here-s-what-you-need-to-know-about-the-massive-cloudbleed-data-breach

https://www.lifehacker.com.au/2017/02/cloudflare-cloudbleed-bug-exposes-sensitive-data-who-is-affected/

https://www.cnet.com/how-to/cloudbleed-bug-everything-you-need-to-know/

This article is for you complements of MembersAlliance Credit Union – 3/15/2017

Please feel free to share!

MembersAlliance CREDIT UNION
You can rely on us!

2550 S. Alpine Rd. Rockford, IL 61108 – Phone 815-226-2260

https://www.membersalliance.org/