The Dangers of Sharing Too Much Information - The WWE Data Breach

July 6, 2017 - Just in case you are not familiar with the WWE, which stands for World Wrestling Entertainment, the company has millions of subscribers. And at least three million of them had their data exposed in a data breach announced two days ago. The breach provides a case study in why it's a bad thing to share too much personal information with any company you do business with.

What's clear from the data breach is that WWE has reams of data on their target audience. The breach exposed names, addresses, email addresses, income information, data on the ages of children and links to some social media posts. About the only thing that was missing was credit card information.

Some of this information may have been purchased by the firm, but a lot of it probably willingly provided by WWE fans. The database that contained the information was unencrypted and according to the company that discovered the breach - Kromtech - could be accessed by anyone who knew the internet address for the database.

The breach didn't contain data that would allow for financial identity theft, such as credit card or social security numbers. But it certainly contains enough information for a determined criminal to start down that path. Just the fact that income information was released would make it fairly easy for criminals to draw up a target list for the best identities to steal. And since anyone with access to the database also has access to the home addresses of people listed, they can target victims in their general geographic area. If that happens, it's a simple matter of picking the best ID theft candidates from the list and then driving to their house and rummaging through the trash. Chances are pretty good that a criminal with the right mindset would eventually be successful.

If you have any reason to believe that your data was included in this breach, you need to start watching your credit report carefully. And if you know someone who is a wrestling fan, make sure they are aware of the breach. The long term effects of this type of data breach are hard to quantify. At this point, it is unknown whether anyone with criminal intent actually accessed the database.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS