HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 7/11/17

Three Million Wrestling Fans at Risk after WWE Leaves Database Unprotected

The professional wrestling entertainment company "WWE" has just been caught with its spandex leotard down, after a security researcher discovered a plaintext database containing the details of more than three million wrestling fans on an unprotected Amazon Web Services S3 server. The information, which included fans' home addresses, email addresses, ethnicity, earnings, educational background, and the gender and age range of children was simply left on a publicly accessible server, with no requirement for a password or username. In short, anybody with an internet connection could have viewed and downloaded the data. Bob Diachenko of Kromtech, who came across the unprotected database, quickly contacted WWE corporate contacts listed in the database, and the information was secured within a few hours.

But the question remains, of course, of just how long the sensitive data was available for anybody on the internet to peruse and potentially exploit. In a statement, WWE was keen to point out that no passwords or payment card data had been exposed as a result of the security slip-up: "Although no credit card or password information was included, and therefore not at risk, WWE is investigating a potential vulnerability of a database housed on a third party platform. In today's data-driven world, large companies store information on third party platforms, and unfortunately have been subject to similar vulnerabilities. WWE utilizes leading cybersecurity firms to proactively protect our customer data." Hmm. Yes, it's obviously a good thing that passwords and credit card details were not included in the leak of the plaintext database. If that information had been present then things would have been much more serious. But that's not to say that was has leaked isn't evidence of sloppy security. No-one is going to feel comfortable knowing that online criminals and fraudsters could use information like this to extract further information from wrestling fans, or indeed that information about ethnicity, earnings and innocent children was included in the haul.

Every day we put our trust in online companies that they will take proper care of our sensitive personal information, and not simply chuck it up on a publicly-accessible server which doesn't even require the most basic of passwords, let alone layer defenses such as two-factor authentication and encryption. And yet time and time again we are seeing organizations leave data on cloud servers utterly unprotected. Just in the last few days, for instance, we have seen the UK's Automobile Association finally admit that a security lapse left the personal information and partial payment details of some of its members exposed, potentially assisting identity fraudsters.