

Latest Massive Data Breach Could Break Up Some Marriages

November 17, 2016 - According to a report on LeakedSource.com, a data breach at Friend Finder Networks, Inc. has exposed the account information on 412 million people. If the report turns out to be accurate it would be one of the largest data breaches in history. It would also be likely to cause relationship issues for millions of people. That's because the company runs the largest adult "hook-up site" on the internet and several well-known adult content sites.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

The new data breach would be the second data breach for the company within the past year. The first breach, which was reported by CNN in May, exposed a wide variety of highly personal information on 3.5 million users.

Based on various reports, it would appear that after the May data breach, the company didn't make changes to the way in which it was storing its data. LeakedSource reports that newly registered users of the company's websites had their information stored without any encryption at all.

The breach may also have ramifications for some government civilian and military employees. According to the report, there were more than 5,600 .gov email addresses and 78,000 .mil email addresses in the company's database. Subscriptions to adult websites can be used to strip security clearances from government employees and contractors. That's because such subscriptions can be used as leverage for blackmail.

Normally, LeakedSource allows anyone to search its database for specific email addresses. For the time being, they have not made the breached information from this breach searchable. But that may change. Regardless of this, there is nothing to say that they won't work with journalists and the federal government to identify people who fit specific profiles

that may have had their information included in the breach. It is highly likely that the federal government will want to find out which of its employees were registered users on these sites. It is equally likely that government contractors and state & local governments will want access to this information.

Former users of the company's sites may also find they have "some splainen to do." Thatâ€™s because the database appears to include deleted account information on more than 15 million people.

After the Ashley Madison data breach last year, we would have thought that consumers would understand the substantial risks they take when registering on "red light district" websites. That's apparently not the case.

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