

1.3 Million Montana Residents Now Victims of State-Owned Computer Data Breach

June 24, 2014 - 1.3 million residents of Montana may have had their personally identifiable information stolen by hackers. The data was stored on a computer owned by the state's Department of Public Health and Human Services. The state is in the process of notifying victims but the notification of the hack is less than timely. The computer was hacked nearly 1 year ago but the hack wasn't discovered until last month.

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 state began sending notification to victims this week via the US Mail. Victims are being told that there is no evidence that their data has actually been accessed or used but is offering one free year of credit monitoring service to those being notified. They have also setup a hotline that residents can call for more information on the hack. The number for that hotline is 800-809-2956.

The breach was discovered by an outside contractor who noticed what he considered to be suspicious activity. After further research, the hack was confirmed.

The computer involved contained millions of records with highly personal information. Names, birth dates, social security numbers and a wide variety of other data were stored on it. The state has said that it doesn't believe that any of this data was actually accessed by the hackers, but they are also saying that they may never know the purpose of the hack or what files were accessed.

Anyone receiving a notification from Montana that their data was stored on the computer would be wise to take some precautions. These include carefully reviewing credit card and bank statements and checking their credit report regularly.

Anyone who believes that they may have actually been victimized in this hack should call the hotline number mentioned above for further details.

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