Data Breach Affects Students, Parents and Applicants to Univ. of Nebraska & NE State Colleges

June 13, 2012 - Late last month the University of Nebraska issued a letter announcing a significant data breach that affects all of their campuses and all current and past students going back as far as 1985. After the announcement it was also discovered that the breach included information for current & past students and past applicants at three Nebraska State College campuses.

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 breach also includes two other groups of people. Anyone who has applied to the university within the past three years. And the parents of current or past students, or those who have applied over the past three years, who also requested federal student aid. In all, it is a breach that could affect more than 650,000 people all across the country.

According to the school, the attack was "sophisticated" but that may actually turn out to be an overestimate of the hacker's ability There is no doubt that the information released in this breach is a treasure trove for ID thieves and fraudsters. It includes names, addresses, social security numbers, phone numbers and in some cases, bank account information. Absolutely everything that is needed to commit identity theft. And in some cases, absolutely everything that is needed to start draining bank accounts right away.

But as it turns out, the primary suspect in the case is an undergraduate student at the University of Nebraska in Lincoln - the name of the suspect has not been released. And that suspect was identified relatively quickly by the school because he/she didn't bother to mask the IP address from which the attack on the school was launched. This means that the university's systems were not even protected from within their own network.

The university was also forced to admit that the targeted data wasn't even encrypted. If true, it is a startling admission that the school is doing little to protect the personal information of students, applicants or their parents. There is really no acceptable excuse leaving the type of data that was breached here on an internet accessible computer system without any encryption.

According to the school, the breach was closed down within 16 hours of its discovery. The fact that they were able to identify a suspect very quickly means that it is unlikely that the data had time to be used for identity theft. But there is still the possibility that some of the stolen data was sold or transferred in a black market transaction.

Anyone who thinks that they may have been affected in this data breach should be reviewing their bank account statements closely and should also place a fraud alert on their credit file. Anyone who has reason to believe that the university had access to their bank account numbers would be wise to open new accounts. And if you don't need access to instant credit, you should seriously consider placing a credit freeze on your file. This is the most effective way of preventing credit related identity theft.

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