

19 August 2008

By: Denisa Ilascu, Internet / SEO News Editor



Subscribers' private information leaked on the Princeton Review website plus.maths

[Student Private Information Leaked on Preparatory Firm Website](#)

Princeton Review published confidential data by accident

Princeton Review, an organization that helps students prepare for tests and admission to universities, is responsible for leaking private information on its subscribers, as the [New York Times](#) reports. For seven weeks, some of the information that should have remained in the private database of Princeton Review, has been available for everyone who registered to the website by simply introducing an email address. The organization has been hired to evaluate the progress of students from public schools in Sarasota, Florida. The file that offered an overview of the pupils' activity comprised their names, birthdays, ethnicities and their grades on the Florida Comprehensive Assessment Test. This examination shows the students' skills in mathematics, reading, science and writing. All these details have been made public by mistake, along with other sensitive information regarding learning disabilities, or whether English was the students' mother language or not. The schools in Sarasota were not the only ones affected by the failure in the security system of Princeton Review. The names and birthdays of approximately 74,000 students from the public schools in Fairfax County, Virginia, were revealed in the same way. "Some of the information is said to have been accessible through search engines like Google. You have to wonder - if companies are making it this easy to discover information about individuals, why do identity thieves go to all that effort of writing spyware?" [commented](#) Senior Technology Consultant at the security company Sophos, Graham Cluley. The most intriguing thing about the incident was that it was discovered by another preparatory firm, as it was performing a survey to see how competition was doing. When finding that all the data, which were not supposed to ever be made public, were available on the Princeton Review website, the institution, on the condition of being allowed anonymity, broke the story to the Washington Post. The Sophos researcher railed against this approach. "If you need an encouragement to make sure that your house is in order and your data secure, and the threat of identity thieves isn't enough for you, then maybe the thought that a business rival might take your blunder to the press will do it."