Questions & Answers about the data compromise

How was the data compromised?

The hackers obtained passwords by monitoring district computers and capturing keystrokes, according to U.S. Computer Emergency Readiness Team, which notified the S.C. Information Sharing & Analysis Center.

The hackers were able to capture keystrokes from district computers and determine district passwords for the state systems that store the district's student and employee information.

The hacking was an intentional and sophisticated criminal action to obtain protected information, officials say.

The passwords gave the hackers access into the records on the state system of more than 25,000 students and more than 2,500 employees.

What was compromised on the State System?

Database information on the current and former students and employees may have been compromised, including names, birth dates, social security numbers, addresses and phone numbers.

No credit card or bank account information appears to have been compromised.

Do I need to take action now?

To date, there is no evidence that any confidential information has been used illegally. If you would like to take additional measures to protect yourself, you should consider the following information.

- ◆ Be vigilant and carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved and contact the Federal Trade Commission for further guidance.
- ◆ Tips on how to guard against misuse of personal information can be found on the Federal Trade Commission website at www.ftc.gov. This site should help you to determine what to look out for with regard to your personal financial information.
- ◆ You DO NOT have to close your bank account or cancel your credit cards. You may want to review your credit report. By law, you are entitled to one free credit report each year, and this report can alert you to any suspicious activity on your accounts. To request a free credit report from one of the three major credit bureaus – Equifax, Experian, or TransUnion – contact their fraud protection departments at either the phone number or address or go to the website: www.annualcreditreport.com.
- ◆ A fraud alert with the National Credit Bureau is a more proactive measure you can take to protect yourself, if you feel it is necessary. You can request that the three major credit bureaus place a fraud alert on your credit bureau records. A fraud alert is a message that credit issuers receive

More on next page

when someone applies for new credit in your name. The message tells creditors that there is a possible fraud associated with the social security number and gives them a phone number to call (yours) before issuing new credit.

You can contact the fraud alert departments at any one of the three major credit bureaus:

TransUnion

Direct Line for reporting suspected fraud:
1-800-680-7289
Fraud Victim Assistance Department
PO Box 6790
Fullerton, CA 92634
Phone 800-916-8800 / 800-680-7289
http://www.transunion.com

Experian

Direct Line for reporting suspected fraud:
1-800-397-3742
Credit Fraud Center
PO Box 1017
Allen, Texas 75013
888-EXPERIAN (888-397-3742)
http://www.experian.com

Equifax

Direct Line for reporting suspected fraud:
1-800-525-6285
Fraud Division
PO Box 740250
Atlanta, GA 30374
800-685-1111 / 888-766-0008
http://www.equifax.com

Why did this happen to me?

This is a random crime. We have no reason to believe that any specific individual was targeted.

Again, this sophisticated hacking could only have been doen by professional hackers.

How can the district prevent this from happening in the future?

New malicious software programs are constantly being written and implemented worldwide.

Our Computer Security Taskforce is working to put in place even more safeguards against such hacking attempts.

Our Information Technology Department is also continually upgrading our system with the most current antivirus software available to protect our school district. We monitor the development of new viruses and provide protection for our system as soon as new viruses are detected.

We are also working in cooperation with law enforcement to take all appropriate investigative actions.

How did school district detect this incident?

The U.S. Computer Emergency Readiness Team notified the S.C. Information Sharing & Analysis Center, which notified the district.