



January 6, 2010

An important message for our staff:

I want to inform you of a cyber attack on one of the district's servers. We do not believe that sensitive personal information was accessed, but we can't rule out the possibility. Because even a slight possibility of compromise exists, I felt it was important to notify you of the breach and of steps you can take to protect against misuse of your personal information. I realize this news is troubling, and sincerely apologize for any potential inconvenience or worry this may cause.

What Happened?

Computing staff recently noticed unusual activity on a department's server and immediately shut down the server as a precaution. Our initial analysis indicates that the activity was likely an attempt to strike at an outside server, using 4J's server for what is known as a "denial-of-service attack."

What Was Exposed?

The involved server contained a list of 4J employee names, home phone numbers and district employee identification numbers, but did not contain other personal information. The server is connected to other servers that do contain personal information, however. While there are safeguards protecting these servers and we have no indications that they were accessed, we cannot at this time rule out the possibility that they may have been compromised.

What Can You Do?

Although unlikely, it is possible that the individuals responsible may have accessed current and former staff members' names, addresses, dates of birth, social security numbers, and bank account information for direct deposits. Due to the possibility that an unauthorized person has obtained your personal information, we want to bring this issue to your attention and provide specific steps you can take to protect yourself from the possibility of identity theft or other misuse of your personal information. The Federal Trade Commission suggests steps you can take to protect your financial accounts, protect against fraud, monitor for fraudulent activity, and report suspected fraud—please see attached.

What Is 4J Doing?

A thorough investigation of the security breach has been initiated, police have been notified, and the district has taken measures to further safeguard the involved server. We are continuing to assess our information security systems to make certain that we have all appropriate measures in place to ensure your personal information is secure.

I sincerely regret any inconvenience this may cause to you. The district remains committed to safeguarding the integrity of your personal information. To ensure you are fully informed, we have set up a webpage, email and phone line where you can get more information. If you have questions you may visit www.4j.lane.edu/databreach, send email to databreach@4j.lane.edu or call 541-790-7730, and someone will respond to your inquiry.

Regards,

George Russell
Superintendent

What To Do If Your Personal Information Has Been Compromised

We do not believe that sensitive personal information was breached in this attack, but because it is possible, you may want to take steps to monitor and protect your financial accounts. The Federal Trade Commission (FTC) has provided specific steps you can take to protect yourself from the possibility of identity theft or other misuse of your personal information when there is a possibility that an unauthorized person has obtained your information.

Protect Your Financial Accounts: If the compromised information includes details about your financial accounts (for example, if you have your paycheck directly deposited to your bank account), the FTC recommends that you consult with your financial institution about whether to close the bank or brokerage accounts immediately or first place passwords on any accounts that you have open (or change existing passwords) and have the institution monitor for possible fraud. For good password security, avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

Protect Against Fraud: When accessed information may have included your social security number, the FTC recommends that you call one of the three nationwide consumer reporting companies to place a free 90-day fraud alert on your credit reports—you only need to call one of the companies, which will alert the other two. This alert can help stop someone from opening new credit accounts in your name.

Equifax: 1-800-525-6285

Experian: 1-888-EXPERIAN (397-3742)

TransUnion: 1-800-680-7289

Monitor For Fraudulent Activity: When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one free credit report from each of the companies. The FTC says it is prudent to wait about a month after your information may have been stolen before you order your report, since suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, such as inquiries from companies you did not contact, accounts you did not open and debits on your accounts that you cannot explain. Check that the information—including your Social Security number, address(es), name or initials, and employers—is correct.

Report Suspected Fraud: Finally, if you find any suspicious activity related to your financial accounts or on your credit reports, call your local law enforcement agency immediately.

Learn More: For more information about how to prevent identity theft, please see <http://www.ftc.gov/idtheft>.