

Letter e-mailed to a Monster.com user, August 30, 2007

Letter e-mailed to a USAJOBS.gov user, August 31, 2007

1 monster.com

Dear Valued Monster Customer,

Protecting the job seekers who use our website is a top priority, and we value the trust you place in Monster. Regrettably, opportunistic criminals are increasingly using the Internet for illegitimate purposes. As is the case with many companies that maintain large databases of information, Monster is from time to time subject to attempts to illegally extract information from its database.

4 As you may be aware, the Monster resume database was recently the target of malicious activity that involved the illegal downloading of information such as names, addresses, phone numbers, and email addresses for some of our job seekers with resumes posted on Monster sites. Monster responded to this specific incident by conducting a comprehensive review of internal processes and procedures, notified those job seekers that their contact records had been downloaded illegally, and shut down a rogue server that was hosting these records.

8 The Company has determined that this incident is not the first time Monster's database has been the target of criminal activity. Due to the significant amount of uncertainty in determining which individual job seekers may have been impacted, Monster felt that it was in your best interest to take the precautionary steps of reaching out to you and all Monster job seekers regarding this issue. Monster believes illegally downloaded contact information may be used to lure job seekers into opening a "phishing" email that attempts to acquire financial information or lure job seekers into fraudulent financial transactions. This has been the case in similar attacks on other websites.

5 We want to inform you about preventive measures you can take to protect yourself from online fraud. While no company can completely prevent unauthorized access to data, we believe that by reaching out to job seekers like you, the Company can help users better defend themselves against those who have attacked Monster as well as other databases.

We are committed to maintaining an ongoing dialogue with all of our job seekers about Internet security and the steps Monster is taking to protect its job seekers. The Company has placed a security alert on Monster sites offering information to educate you about online fraud. This information can be found at <http://help.monster.com/besafe/>. We have also included information on Internet safety and examples of fraudulent "phishing" emails at the bottom of this letter.

Monster has launched a series of initiatives to enhance and to protect the information you have entrusted to us. Some of these steps are being immediately implemented, while others will be put into place as appropriate.

We believe these actions are the responsible steps to protect the trust you place in Monster. We are also working with Monster's hundreds of thousands of employer customers to ensure a safe and effective online job search. We will continue to share information with you about the enhancements we are making as we serve as your online career resource partner. We invite you to keep reading to learn more about how to use the Internet safely.

Sincerely,

Sal Iannuzzi
Chairman and CEO
Monster Worldwide

7 **11**

USAJOBS®
"WORKING FOR AMERICA"

Dear USAJOBS User,

3 Recently, malicious software, known as Infostealer.Monstres, was used to gain unauthorized access to the Monster.com resume database to steal the contact information of job seekers. Monster Worldwide is the technology provider for the USAJOBS website and regrettably, some of the contact information captured came from USAJOBS job seekers.

6 The information captured included name, address, telephone number, and email address. Monster Worldwide has assured the U.S. Office of Personnel Management that Social Security Numbers were NOT compromised because of IT security shields USAJOBS has in place.

Access to the data was obtained through the use of a private sector Monster customer's computer using legitimate employer credentials. OPM is working closely with Monster to quickly protect the USAJOBS data. Monster Worldwide already has identified and shut down a rogue server that was accessing and collecting the job seeker contact information. Further safeguards are being put into place.

We ask you to remain alert for counterfeit "phishing" emails that may appear to come from Monster.com asking you to click on a link. **USAJOBS will NEVER request personal information via unsolicited email (i.e. not a response to an email sent by you). Monster has also assured us THEY will NEVER ask any site users to download any software, "tool" or "access agreement."**

9 Please also be on the alert for fraudulent email that advertises positions managing financial transactions, or cashing checks. These emails are attempting to engage job seekers in a money laundering or bad check scam.

If you receive a suspicious email regarding your USAJOBS search, email it, with the full "header" information intact, to us at: mayday@fedjobs.gov. Instructions on obtaining header information can be found at: http://www.spamcop.com/help_with_headers/.

"Phishing" and Internet fraud is an issue that, from time to time, can affect any Internet user or business. We remain committed to safeguarding the integrity of the information provided by job seekers. If you have any questions, please contact mayday@fedjobs.gov.

Sincerely,

Steve Connelly
Program Director, USAJOBS