Online job hunters grapple with misuse of personal data

By Ross Kerber, Globe Staff | October 1, 2007

After he posted his resume online in 2004, Ed Pilarski got more responses than he bargained for.

More than a dozen companies called or e-mailed the retired Verizon Communications Inc. project manager with job offers he did not want or mortgage refinancing deals he did not need.

One caller stood out: A Morgan Stanley financial adviser who allegedly viewed the resume of Pilarski and hundreds of others posted on job-hunting website CareerBuilder.com.

The adviser suggested Pilarski "must have done pretty well financially" at Verizon. Outraged that information in his resume was
Some job recruiters say Pilarski's case is all too common. The misuse of resume data has become a big issue for the fast-growing sites that are now a main source of talent for some industries, as well as a growing risk to individuals as hackers target the vast databases of personal information. Just last month, the online recruiting site Monster.com disclosed that hackers had compromised as many as 1.3 million records.

"It's been a big problem for years," said Susan P. Joyce in Marlborough, editor of job-hunt.org, a compilation of employment links and leads. "People are so trusting of something that calls itself a job board, because they're looking for a job and their shields are down. They'll share information they wouldn't normally share."

Tom McAuliffe, an executive vice president at Sovereign Bank who oversees human resources areas, said he expects to see more security efforts from the job-hunting sites to block abuses. "If applicants don't trust the sites they'll stop using them," he said.

The popularity of recruitment websites has exploded in the past few years. CareerBuilder reported 15.4 million unique users during August, slightly behind traffic to sites affiliated with its biggest rival, Monster.com. Smaller competitors such as Yahoo! Inc.'s HotJobs.com also are growing quickly.

The sites have become a critical recruiting tool for companies such as Sovereign. With 12,000 employees and a high turnover common to the banking industry, Sovereign hires about 2,000 people a year. Online resumes are the company's second-largest source of new hires, after referrals from current employees. About 28 percent of Sovereign's jobs are filled through one of the three career websites, McAuliffe said. Purchasing a license to access resumes on job-hunting websites, and posting openings there, is "the cheapest way to get the message out quickly," he said.

The newspaper industry, after years of losing recruitment ads to Internet competitors, has joined forces. Monster.com's parent company, Monster Worldwide Inc., has a partnership with The New York Times Co., including the Globe and its website, Boston.com. CareerBuilder is owned by Gannett Co., Tribune Co., McClatchy Co., and Microsoft Corp., and has partnerships with America Online and 150 newspapers.

The sites allow job seekers to browse their databases of millions of job openings and sort them by parameters such as location or industry sector. Job seekers also can create and post online resumes for prospective employers to see, which can include personal data such as home and work telephone numbers, e-mail addresses - even Social Security numbers, which some job-seekers include to speed up background checks by potential employers.

Companies that buy access to CareerBuilder.com to find employees must provide their own phone numbers, domain names, and tax identification information to guard against fraudulent use of the data. But Liz Ryan, a career adviser in Boulder, Colo., said it is easy to purchase a password by posing as a small business. Password-borrowing also is common. "Logistically, it's wide open," she said.
And as they have grown, the sites have become attractive targets for thieves and scam artists. Symantec Corp., the California data-security company that first noticed Monster.com’s vulnerability, wrote on its site that the records compromised are "a spammer's dream." Some Monster.com users received so-called "phishing" e-mails that contained victims’ personal information and asked that they download a file to assist in their job search. Instead, the file was a "Trojan horse" that encrypted documents in the victims' computer and left a text file asking for money to decrypt the information.

Both Monster.com and CareerBuilder.com have posted prominent warnings about scams to users urging them to beware of e-mail asking for information such as bank account numbers or Social Security numbers, which can be used for illegal activities such as identity theft. Other abuses can be more annoying than illegal, such as exposing users to junk e-mail or product offers. Neither Monster.com nor CareerBuilder.com made executives available to be interviewed. A Monster.com spokesman did not respond to questions. Via e-mail a spokesman for CareerBuilder wrote that the site "takes the issue of fraudulent activity very seriously" and has taken steps such as hiding information on resumes such as Social Security numbers.

But some career coaches, privacy advocates, and job hunters say the sites could do more. One job seeker, Worcester marketing and Web design consultant Barbara Cowen, said she recently took down a resume she had posted on CareerBuilder.com earlier this year after getting dozens of e-mails offering her financial services products or jobs she was not qualified to take.

"My resume is very personal, and I don't like the idea of just anyone looking at it," she said.

Another job seeker, Boston computer support specialist Charisse Sebastian, said she keeps resumes posted online even though she often gets e-mails offering her inappropriate financial products. She called the contacts unethical, but said she needs to keep her resumes on the career sites.

"It's not that I want to put up with it, I have to," Sebastian said.

In response, many job seekers create new e-mail addresses for their job searches or buy disposable cellphones, said Pam Dixon, executive director of the World Privacy Forum, a research group in San Diego.

Resume data are often sold by direct-marketing companies, Dixon said. One list advertised for sale by a Utah company, Geon Media Group, promises the addresses of thousands of people who have used CareerBuilder.com and similar sites. "This list is perfect for continuing/distance education mailers; as well as those offering products related to self-improvement, business opportunities, sweepstakes & lotteries, credit card offers, and catalog offers," according to a company description. A Geon representative said executives would not comment.

As for Morgan Stanley, a spokesman described the case as an isolated incident. The company is still reviewing the allegations by the secretary of state's office, which is seeking an unspecified fine and possibly other penalties.

The state charged that a financial adviser in Morgan Stanley's High
Street office in Boston, Arlen Jay Fox, obtained perhaps thousands of resumes from job sites to generate sales leads, at first using a co-worker's passwords, then allegedly obtaining a CareerBuilder password from a manager, David Swartz. Neither Fox nor Swartz would comment, said a Morgan Stanley spokesman.

Galvin's investigation began after he was contacted by Pilarski, the retired Verizon manager, who got a call from Fox on Oct. 30 last year. Days earlier Fox had called another person whose information he also apparently gathered from a resume.

According to court papers, the target wrote back: "If I suspend for a moment my nonbelief that you actually work for Morgan Stanley, I would give you this advice: abandon this approach. It is at best damaging to your credibility as well as that of your firm; further, it is intrusive. . . . Now, Get Lost!"

Ross Kerber can be reached at kerber@globe.com.