Tips for a Safe Online Job Search

Excerpts from an article by Teena Rose

Conducting a job search using the Internet has definitely transformed how job seekers contact hiring companies. With the Internet's convenience, however, a breeding ground for scam artists continues to grow each year, as well. Identity thefts have increased to an overwhelming 10 million cases per year, and many of them are the result of "phishing"—not surprisingly, the employment industry is under attack, as well.

Phishing is an attempt to extract personal information through what appears to be authentic emails. If you are job searching, an email from a seemingly interested recruiter, for example, may not raise a red flag with you. You may think that the contact person and company listed are legitimate, yet looks can be deceiving. Knowing what to look for and how to spot fraud (or potential areas for abuse) can be the best deterrent to ensuring you have a safe experience while conducting your job search.

1. Be leery of submission invitations.

Scammers and spammers follow the same patterns. Mass emails are sent to an enormous list of recipients. Not everyone on the "hit list" is searching for a new job; however, only a small number of people need to be convinced, or tricked into believing, that the email is authentic in order for the scam to be deemed successful. You might, for instance, receive an email from a recruiter who states, "We saw your resume on the Internet, and we find your skill set to be perfect for one of our clients. Please complete our online application through the below link."

Before you respond, ask yourself a series of questions. Did you send your resume to this recruiter? Visit the company's Web site (***type the Web address into your browser, avoid clicking the link in the email***). Upon further examination, are they reputable? How did they hear about you?

Better yet, call the company. Always proceed with caution when you receive a cold-contact email from someone.

2. Avoid responding to requests for personal information, such as a social security or credit card number.

Let's say you receive an email from what appears to be a well-known job bank. The email states that your account needs your contact and payment information to be updated in order for service renewal. You click on the link and you're taken to a page that looks, feels, and "smells" right. You proceed by submitting the requested information.

The link appeared safe, but you were taken to a site designed to defraud you. Reputable companies will rarely ask for personal information via email, so examine every incoming email for validity.

3. When purchasing a service through the Internet, ensure information is encrypted when you hit the "submit" button.

Encryption, in short, ensures the private information you submit online is kept safe. When at your browser, you can recognize an encrypted form when the root URL starts with "https:" instead of "http:" or seeing the padlock present in the bottom right corner of your screen. Purchasing from companies having added security measures in place can ensure your private information avoids the hands of ill-willed people. Learn more about encryption by reading Jeff Tyson's article titled, "How Encryption Works" at www.howstuffworks.com.

4. Read and understand the privacy policy of sites you patron.

The Better Business Bureau possesses a strict policy for members who do business online. A privacy statement must be displayed on the company's Web site, no exceptions.

A privacy statement outlines what type of customer information is collected and how it's used. Alliances and partnerships, for example, may arrange for Company A to sell or pass on client information to

Company B. No matter how basic or detailed the information, however, the company must have the logistics spelled out in their privacy policy.

5. Tell!

Reports show an estimated 80% of online fraud goes unreported. If the proper authorities aren't aware of the magnitude of fraud that actually exists on the Internet, then getting the much-needed funds to battle the problem will take more time. The Internet Fraud Complaint Center (ifccfbi.gov) has an online complaint feature for individuals to report phishing attacks. The IFCC report process requires basic information, including information on the perpetrator and type of fraud.

In addition to filing a complaint, forward the fraudulent email to the legitimate company. Phishing is smearing the good names of countless companies, and notifying the company about the scam can also help the fight. Companies being brought onboard will ensure well-rounded efforts to stop this epidemic.

Avoid giving your information out freely. With safe online practices, you'll get the best return from your job-search efforts—instead of spending hours filing a police report and calling credit bureaus and credit card companies.