College Central™ Advice

Don’t Feed Your Résumé to the Sharks

Safety tips for your online job search.

The Net, phishing, and you.

For job seekers, the Internet is essential when it comes to convenience and resources. You search postings, see a great opportunity, and submit your résumé. What could be easier? Answer: identity theft.

2012 alone saw over 12 million cases of identity theft. Students and first-time or desperate job seekers are easy marks for scammers waiting to steal personal data under the guise of a job offer. The fallout can be catastrophic and wreak havoc on your future before it’s even begun. So how do you get your résumé to employers or apply online without compromising your privacy or reputation?

Red herrings.

Understand that no career center or job site can filter out every phony job posting 100% of the time. Ultimately, it’s your responsibility to safeguard your personal information and online job search. Consider these warning signs and precautions:

Spoofing and phishing lures. Fake job offers, alerts, and notices, and official-looking but phony emails that misuse real company logos or mimic real company names, can link to fraudulent sites that use deception to collect personal data or download viruses, spyware, and other malware.

“If it sounds too good to be true...” You know the rest. Avoid offers like “Earn $3,000/wk. No risk! Guaranteed!” “Work at home. Huge returns!” “Earn Six-figures! No Experience Needed!” Really?!?

Paying it forward is not good. You should NEVER have to pay money to apply for or get a job. Be suspicious of sites that require an upfront fee or substantial purchase of inventory or training kits, example: mystery shopper. Don’t pay for anything in advance with a promise of reimbursement. Plus, no company should EVER request that you wire them money; expect 0% return and 100% liability when entities ask you to deposit their check, keep a percentage of the funds, then wire them the balance.

Johnny can’t write. Beware of poor grammar and misspellings in job offers. Reputable companies have people who carefully proof their postings.

Lack of information. Vagueness, no legitimate land address, and nothing but a phone number, are all red flags. Be wary of contact addresses that use publicly available email services rather than an actual “@companyname” email address.

Keep your 411 to yourself. Your name, Social Security number, birthday, even licenses, can be misused to create fake accounts and IDs, apply for loans, or to access your finances. Nor should completing a background check be a prerequisite to a job application. If requests for personal data prior to being hired make you feel uncomfortable, walk away.

Résumé hooks, lines, and sinkers.

READ the privacy policy! Always carefully examine the privacy terms when using any online résumé posting site:

-- it should clearly state how your data is gathered, used, and stored; some sites share info with third parties; verify your levels of security and visibility; check that you can mask your online ID (such as from current employers) and designate who can contact you;

-- be selective of the amount of info you post; monitor all the sites where you post résumés, including social media;

-- delete your résumés once you’re hired; leaving unnecessary personal info out in cyberspace invites scammers;

Résumé writing services should also have clear privacy policies stating how they will share your résumé, plus encrypted pages for online payments. Again, don’t give your SSN, birthday, or financial data.

With online job searches, never stop doing your homework, even after you graduate. Research companies, use common sense, and exercise caution. When in doubt, contact your career center.

Avoid taking—or being—the easy bait, even if you’re desperate. You never know what’s at the other end of the line.

CAREER ADVICE COLLEGE CENTRAL™

In a nutshell:

Online security is never 100% guaranteed, but you can take proper job search precautions:

- **Avoid offers that promise the world with little or no risk—“free” often comes at a price; run, if they ask for money upfront**
- **Guard your SSN, banking, credit, financial, birthday info**
- **Don’t include references; protect their privacy, as well**
- **Google companies, visit sites independent of links in the ad**
- **Use privacy settings; restrict your social media page access**
- **When in doubt regarding protocol, contact HR directly or your college career center**

With plenty of phishing going around, be the one that got away!

CollegeCentral.com/ncstatecollege

Visit the above URL to access our school’s exclusive jobs database **and MORE!**