College Central™ Advice

Scam I Am

Real and potential job search and employment schemes.

Financial and social media breaches are not the only ways to compromise personal information. Spam, spoofing, phishing, spear phishing, smishing, pharming are all tactics scammers use to manipulate victims into handing over sensitive data. Combined with pandemic unemployment, increased remote working, and promises of quick, lucrative rewards for little or easy work, deceptive practices can make job seekers ideal targets for e-muggers. Click a bad link, provide confidential details before securing the job offer and you could be dealing with malware, identity theft, and lost money, time, and energy.

Digital or not, it's still snake oil

Our document "*Don't Feed Your Résumé to the Sharks*" outlined safety tips for your online job search. Be proactive and informed: research organizations; read the About Us on company websites; check out their personnel and social media presence; read reviews and complaints; Google scams; go to the Federal Trade Commission and Better Business Bureau for data, profiles, and ratings; contact your career/employment center; use common sense and trust your instincts. Beware of offers and those who require you to foot a fee or front money; request sensitive, personal data—your SSN, birthday, bank account info, credit card details, credit report, W-2 and 1099 forms—*before* you're hired; interview via email, text, chat, or instant messaging; use generic email addresses rather than top-level company domain names; or hire without asking for job qualifications, references, applications, or interviews. Here are just some examples of employment schemes.

1. Repackaging/shipping scams. You receive, repackage, and reship products for a fee. Simple, right? And easily done from home. However, the items are stolen. The check for your efforts never arrives. *You*—unwitting or not—have committed mail fraud and, as an accomplice, may even be charged with theft. Ask yourself: why wouldn't a reputable company simply ship *direct* to a customer?

2. Data entry/Rebate processing. These can be actual starting roles for those with little or no experience, or who want flexibility. However, real businesses don't promise lavish wages for the work; require purchase of data lists, essential materials, or training in order to do work for them; or have you market the company and products as part of the job.

3. Money transfers. Fake employer sends you a large check to deposit, then asks you to return a portion due to "overpayment." Their check bounces; *you* have to pay the bank back the full amount, plus fees. And you're out whatever you sent. That's theft. And your loss. Or, scam entity sends funds to your bank account, then asks you to forward it to another account. That's money laundering.

4. Medical billing. Fraudsters may promise lucrative income and quick certification, or charge substantial fees for non-working software and fake client lists.

5. Stuffing envelopes. Machines can do this cheaply and automatically—no non-refundable fee or manual stuffing required.

6. Product/craft assembly. You purchase materials from an entity that promises payment for each approved assembled unit. However, your work oddly never passes inspection, you're never paid, and you end up stuck with (useless) inventory.

7. Multi-level marketing (MLM)/Pyramid schemes. Instead of a salary, members promote products and recruit others for commissions from sales. Few see high returns; many lose money. Illegal schemes recruit for cashflow, not legitimate sales.

8. Bait and switch. You find out that the job you're applying for isn't what was advertised. You're even pressured to sign on the dotted line and accept the offer.

9. Shady job placement services. They don't deliver on promises but gladly take your money while promoting fake or outdated jobs.

10. Government fees. There is *never* an application fee or a testing fee to apply for a government or U.S. Postal Service job. Federal job openings and information are *free* and open to the public.

In a nutshell:

There's *always* someone looking to benefit at your expense. Beware of:

- **Offers/links for "easy money"**
- **Unsolicited emails; postings with poor grammar/typos; lack of organization/job details; generic email addresses**
- **Requests for sensitive data early on, prior to being hired**
- **Upfront fees or outlay of money to secure a job offer; pay-for-performance promises**
- **Requests to repackage items or transfer money**
- **Faceless interviews via email, chat, text, instant messaging**

Scams continue to evolve. Don't let down your guard. Don't be pressured into anything. Research industry wages. When in doubt, check it out—*thoroughly*. Remember, if it sounds too good to be true, it probably is.

CollegeCentral.com/CCNschoolURL

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