Student guide to protecting yourself and your personal data when applying for vacancies

Introduction:

The following information will help you spot signs of and protect yourself against fraudulent activity, but please note that activities are becoming increasingly sophisticated, so you should seek advice if anything doesn't seem right, before you proceed.

We aim to ensure that vacancies published on MyCareerHub are suitable for students and graduates and are from legitimate companies and organisations. However, it is ***your responsibility*** to consider the advertised details and undertake your own research before you apply, and to be alert to possible fraudulent activity during and following the application process. If you are concerned about an advert on MyCareerHub please contact the Careers Team.

Protecting your personal data:

When you send your personal data to an external employer/organisation, such as when you send a CV/application or make an enquiry via email, your personal data will be processed according to the privacy policies of the employer/organisation. It will be your responsibility to protect your personal data, not the responsibility of the Careers and Employability Service. Here are some simple steps you can take to protect yourself.

1. **Don't overshare:** When applying for jobs, sharing CVs, or making enquiries, only include personal data that is required. Sensitive personal data should not be included on your CV, cover letter or in any general enquiry emails. Sensitive personal data includes: your ethnicity, religion, trade union status, political affiliations, any health data, data relating to your sexual life, criminal offences or financial information.

2. **Check the organisation's privacy policy:** Read the organisation's privacy notice to check how they will use your personal data. Privacy notices will contain key information, such as how an employer/organisation will use your data, how long they will retain your data, and who they will share your data with. Some employers may share your CV or application with parent companies or affiliates, so it is important you check their privacy information before you share your personal data. If you have questions about a company's privacy policy or processes you should contact the employer/organisation directly.

3. **Be wary of any unsolicited requests for your data which appear to be from recruiters:** If you receive an unsolicited request for your personal data from somebody claiming to be a recruiter, make sure to do your research into the organisation before you reply, they could be trying to obtain your data for fraudulent activities, such as identity theft. Check that the company is genuine by carrying out an internet search to find any official websites and check that the email address advertised on the official website is the same as the email address you have been contacted by. See our Phishing Guidance for ways to protect yourself from phishing.

4. **Always double check the email address you are sending your data to before hitting send:** When sharing your personal data, particularly when sending a CV, always take time to double check the email address is correct. It is easy to make mistakes such as adding the wrong suffix to the email address, such as using '.com' rather than '.org'.

Checklist for spotting fraudulent organisations and vacancies:

It is important to exercise caution throughout the job application process and remain alert upon receiving a job offer and starting a new job.

1. **Fully check the company/organisation details provided**: it is good practice to check a company is legitimate by looking them up on Companies House, the Charity Register (England) or the Scottish Charity Register. You can also check the web address provided to verify legitimacy. If possible, it is also useful to check when the organisation website was published. Check the registered address of the organisation correlates with records on Companies House and on their website.

2. **Fully check the contact details provided**: It is particularly important to examine the domain of the email address. If it does not match the employer's website it could indicate that the contact is fraudulent. Only use contact information which is clearly connected to the organisation advertised. Never contact someone using their personal email address (i.e. gmail).

3. **Be aware of types of fraudulent and criminal activity to help you spot issues:** we cannot cover all of it here, and activities are becoming increasingly sophisticated, but here are some examples to be aware of:

    a. Being asked to receive and/or make payments from and into your personal bank account.
    b. Being asked to move money into other currencies, including crypto.
    c. Being asked to pay to complete a disclosure/security check via a link provided by the advertiser.

4. **CHECKLIST - Here are some common signs to look out for** (from Gov.uk):

    a. Illegitimate companies or illegitimate emails
    b. Suspicious contact details
    c. Poorly written job advert
    d. Unrealistic salaries
    e. Job offers without an interview
    f. Being asked for money

5. **What to do if you think you have fallen victim to a job scam**

    If you suspect you have been targeted, please report it via the JobsAware portal. They will investigate and take further action if necessary. If you initially saw the advert on our MyCareerHub system, please also contact us to let us know: careers@abdn.ac.uk .

    If you have parted with money as part of a suspected job scam, contact the police and your bank. They will take the matter further.