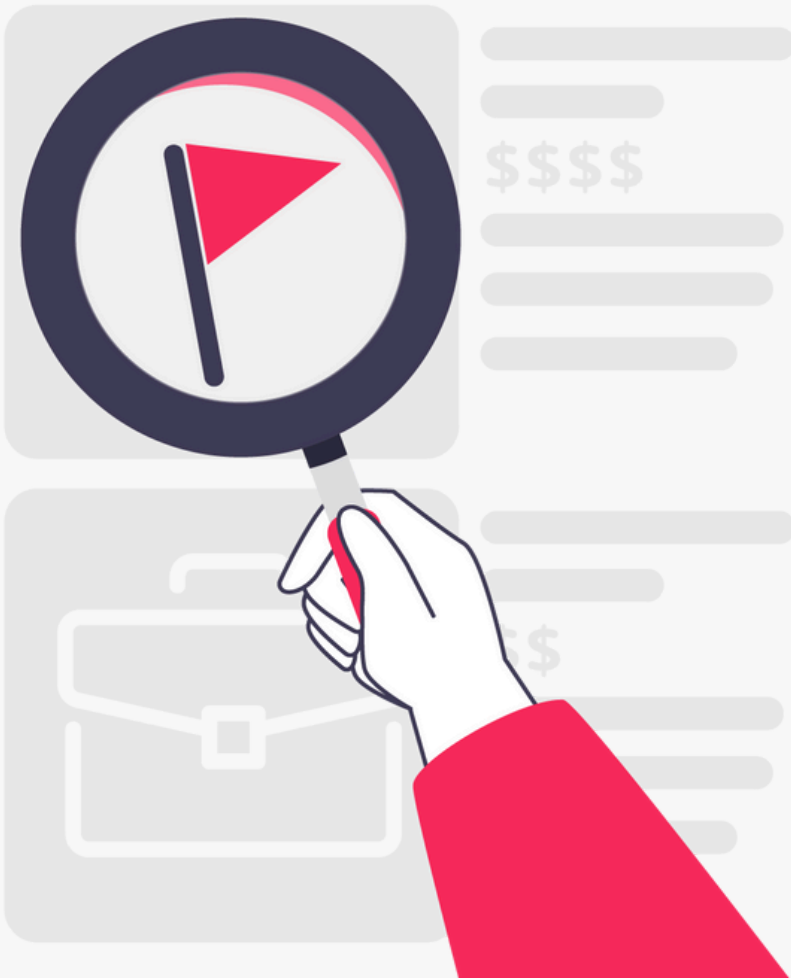


How to **SPOT RED FLAGS** in a Career Advertisement



ABOUT  EduAdvisor

Career Advantage Programme (ECAP)



The EduAdvisor Career Advantage Programme is a premium initiative exclusively available to students who have enrolled in university through EduAdvisor.

Tailored to prepare you for the demands of today's job market, this programme offers early access to career resources that will help you navigate internships and enter the workforce with confidence.

The programme provides personalised guidance, including internship search support, expert career tips, networking events, and one-on-one mentorship. Our goal is to ensure you're not just academically ready but career-ready as well.

Take control of your future with EduAdvisor's Career Advantage Programme — where your success story begins!

SERVICES BY ECAP



Internship Search

A specialised search engine designed to help you discover incredible internship opportunities that align with your field of study, ensuring you find the right match for your future career.



Mentorship Programme

Gain personalised guidance from professionals and mentors within your field of study who can help you navigate your career path and achieve success.



Career Tips & Content

Access tips and valuable career insights through curated content that covers everything from job search strategies to acing interviews, all tailored to help you thrive in your chosen field.



Career & Networking Opportunities

Participate in exclusive events designed to connect you with industry leaders, alumni, and fellow students, helping you stay on top of trends.



WHY MUST YOU LOOK OUT FOR RED FLAGS?

Reduce Stress



By knowing the signs of a scam or a problematic job, you can avoid frustrating job experiences, whether it's a company that overworks its employees or a scam that drains your resources.



Protect Your Personal Information

Avoid sharing sensitive details like your IC number or bank account information with scammers who may exploit your personal data.



Save Time

By recognising misleading or fake job listings early, you can focus on applying for legitimate roles that align with your career goals.

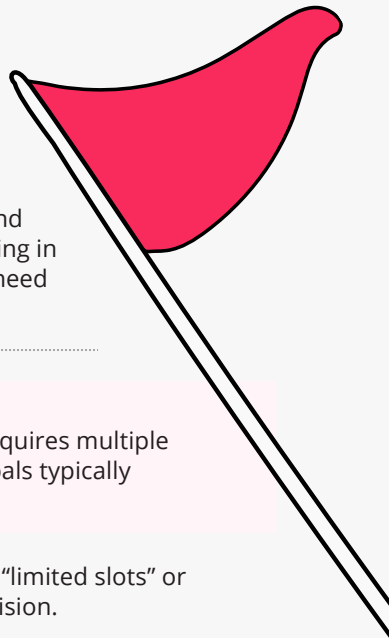


Improve Job Search Confidence

The more you practise identifying red flags, the more confident you'll become in your job search. You'll feel empowered to make the right decisions, knowing you've done your research.

RED FLAGS IN JOB ADVERTISEMENTS

Learning how to identify red flags during your job search and trusting your instincts can help you avoid the pitfall of landing in a toxic workplace. Here are some job search red flags you need to be aware of.



-  **Complicated application process:** A position that requires multiple interview processes with unclear explanations and goals typically indicates a disorganized company.
-  **High-pressure tactics:** Job ads that use phrases like “limited slots” or “urgent hiring” might be trying to rush you into a decision.
-  **Lack of work-life balance:** Job ads that require you to work overtime or after hours could indicate poor management and disregard for employees’ personal lives.
-  **Spelling and grammar mistakes:** Errors in spelling, grammar, or punctuation could indicate a lack of professionalism or attention to detail.
-  **Vague job descriptions:** Minimal details about responsibilities, qualifications, or expectations.
-  **Unrealistic requirements:** Entry-level jobs requiring years of experience or excessive qualifications.
-  **Immediate hiring without interviews:** Legitimate companies typically require multiple steps before hiring.
-  **Unprofessional communication:** Using informal methods like SMS or WhatsApp to contact job seekers, which is not typical for professional recruitment.



HOW TO AVOID TOXIC EMPLOYERS



Have an attention to detail

Read the job requirements carefully. Ensure it provides a clear description of duties and responsibilities.

If the posting doesn't explain the job in detail or appears too demanding for the position (e.g. asking for years of experience for an entry-level internship), reconsider applying.



Maintain private and confidential information to yourself

Legitimate employers will never ask for sensitive personal information, such as your IC number, bank account details, or passwords, in the early stages of recruitment.

If you have work experience prior, they also won't request to see your previous payslips. Keep in mind that your past payslips are part of an NDA between you and your previous workplace.



Use official sites to job hunt

Use sites like legitimate and credible job sites like LinkedIn, Job Street and such as these sites can provide insight into the company's legitimacy, current employees and overall work culture.



Always research the company

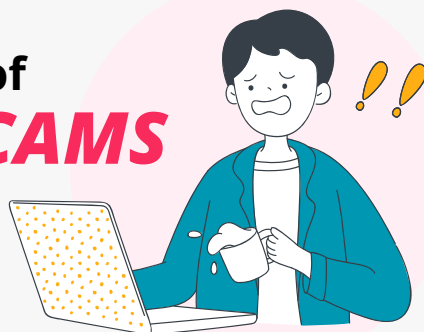
Check if they have a legitimate website, address, and social media profiles. If they don't provide it, be cautious as it could be a fraudulent listing.



Check for Reviews

Before applying, search for reviews on websites like Glassdoor, JobStreet, or even social media. A lack of reviews or overwhelmingly negative feedback is a sign to avoid the job.

Beware of ***JOB SCAMS***

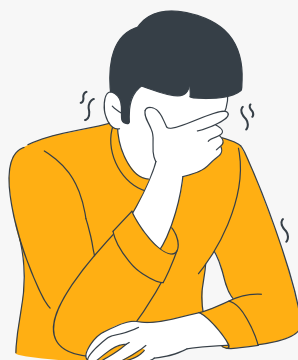


AND TACTICS

Looking for your first internship can be exciting but in our current digital market, it's also important to stay cautious. Nowadays, some scammers target students and fresh graduates with **fake job offers on social platforms like WhatsApp, Telegram, Facebook and Instagram**. These offers usually **promise high pay, flexible hours, or fast cash for little effort** — things that seem too good to be true because they usually are! In reality, they're **using your data to further their fraudulent activities** such as financial or identity theft, phishing or forced labour.

So, how do scammers operate?

Scammers use **stolen identities, fake profiles, and stolen company logos to create trust**. They often **rely on urgency, pressuring you to act quickly** by saying the opportunity is limited or time-sensitive. They **may even use professional platforms like LinkedIn and pose as recruiters** from a well-to-do organisation to appear legitimate. Understanding these tactics and examples can help you stay alert during your internship search. Here are the types of common job scams you must know to protect yourself from their tactics.





How To Spot ***JOB SCAMS***

WATCH OUT FOR THESE TACTICS:

1 Job vacancy postings via an online messaging service

Scammers often pretend to represent well-known companies, recruitment agencies, or even government bodies through instant messaging services. They may pitch you “exclusive” job opportunities **through foreign or unrecognised numbers** to get your attention.



Quick Tips

These scammers typically acquired your number through data leaks. If this happens, do not reply to their messages, block and report the sender on the same platform so they can't reach you.

2 Fake job listings

Watch out for fake job ads that often appear on social media platforms, fake websites or even legitimate job portals. Their social media has unreasonably high followers with low engagement posts. Not only do these listings promise high salaries, but they may also ask you to pay upfront fees, such as “processing” or “registration” fees to apply or secure a role.



Quick Tips

Never pay to apply for a job. You can also report the account for possible scams to prevent others from falling victim.

3 Pyramid schemes

These scams involve job offers that require you to pay a fee and recruit others to join. Instead of legitimate work, the focus is on signing up more people to earn commissions.



Quick Tips

Avoid any job that focuses on recruitment and paying for access. If the recruiter insists, be firm on declining the offer and remove yourself from the situation if necessary.

4 Work-from-home scams

These jobs offer high pay for minimal effort, such as completing online surveys or typing tasks. Your responsibilities typically involve data entry related to data breaches and phishing scams. These offers usually have no clear job details and the description sounds too good to be true.



Quick Tips

Do not engage with these offers, never share any personal information or click any links that come with the ad. Report the scam to the relevant authorities or platform.

5 Fraudulent overseas job offers

Involve fraudulent recruiters offering fake international job opportunities for high salaries, luxurious benefits, and exciting career opportunities abroad. These schemes are often used to steal money, obtain personal information, or trick victims into illegal activities like human trafficking or forced labour in cyber-scams.



Quick Tips

Beware of 'too good to be true' offers. Overseas work opportunities don't come easy and are always offered to individuals with extensive work experience in specific industries. Research the organisation for more information and reviews or avoid it at all costs.

The Differences Between

Toxic Workplace

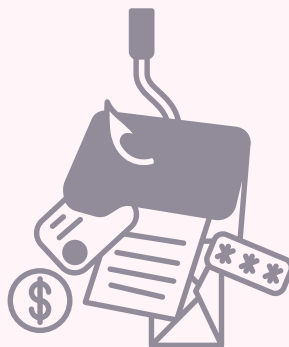
vs

Job Scam



An established organisation that exhibits poor management and leads to burnout.

- High employee turnover
- Micromanagement
- Lack of work-life-balance
- Bullying and harrasment
- Poor communication
- Gossip and cliques
- A noticeable decreased in morale among staffs



Fraudulent job offers that promises non-existent or misleading positions.

- Unsolicited job offers
- Generic job descriptions
- Poorly written job descriptions and unprofessional email address
- High-pressure tactics to secure the position
- Request for personal information and the initial stages

Avoid Falling Victim to ***JOB SCAMS!***

While recognising red flags can help you avoid scams, it's essential to remain vigilant as scammers continuously evolve their tactics. Here are some practical tips to protect yourself from falling victim to job scams.

Research the Company



Take time to verify the legitimacy of the company. Look for an official website, LinkedIn page, or social media accounts. Pay attention to details like the company's email domain (e.g., @companyname.com) and contact information. If the email address seems off, like using personal domains (e.g., @gmail.com), it could be a red flag.

Protect Your Personal Information



Never share sensitive information such as your bank details, IC number, or passport details with recruiters unless it's for official onboarding after you've signed an offer letter. Legitimate employers won't ask for personal details during the application process.

Look For Employee Reviews



Platforms like Glassdoor and JobStreet have reviews where employees and candidates share their experiences with a company. These insights can help you assess the legitimacy of the organisation.

Ignore Job Offers You Didn't Apply For



If something about the job or recruiter feels off, trust your gut. Scammers often use pressure tactics, like insisting you act quickly or lose the opportunity. Legitimate employers will give you time to think and respond.

Avoid Falling Victim to ***JOB SCAMS!***

While recognising red flags can help you avoid scams, it's essential to remain vigilant as scammers continuously evolve their tactics. Here are some practical tips to protect yourself from falling victim to job scams.

Trust Your Instincts



If something about the job or recruiter feels off, trust your gut. Scammers often use pressure tactics, like insisting you act quickly or lose the opportunity. Legitimate employers will give you time to think and respond.

Verify Website Security



Always ensure that websites asking for your details are secure. A legitimate website should have "https://" at the beginning of its web address, not "http://".

Never Pay To Work



Legitimate employers will never ask you to send money, whether for training materials, equipment, or application processing fees.

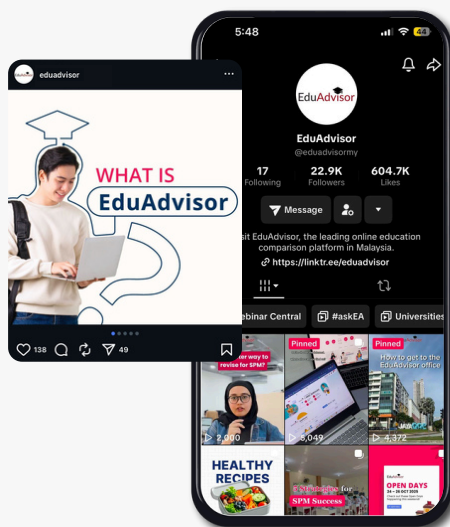
Consult Someone You Trust



If a job offer seems too good to be true, share it with someone you trust who might offer valuable advice or identify red flags you may have overlooked.

Follow our social media

Stay up to date with our content.



EduAdvisor

info@eduadvisor.my | +603 7931 2212