SCAM-PAK

AMICA CENTER
FOR CAREER EDUCATION
Explore • Connect • Discover

The old adage is very useful:

If it looks too good to be true, then it probably isn't true!

career.bryant.edu
401-232-6090

Revised: 3/2/2023

Fraudulent and Scam Job Postings

The Amica Center for Career Education offers the Bryant Career Connection (BCC) as a resource for employers to connect with Bryant students and alumni seeking internships, co-ops, part-time jobs, and full-time positions. We strive to keep fraudulent postings and scams off BCC by using some common "red flags" that are considered suspicious. "Red flags" don't automatically remove a job posting – we research the company and posting if suspicion arises and then make a decision. You should research suspicious companies or postings, too – or don't apply. We are sharing these "red flags" below, so you too, can attempt to identify such scam or fraudulent postings. Our position: never apply to a suspicious job or internship.

The following "red flags" are general markers shared to help you conduct a safer job search and to help you protect your identity. These red flags in no way cover all possible instances of fraud or all the red flags. Please always use your own discretion when applying to a position or interacting with a potential employer.

Fraudulent job postings try to take your money or your personal information. The scammers really don't care about you. The jobs often look like easy and convenient ways to make money with very little effort.

➔ **The old adage is very useful: If it looks too good to be true, then it probably isn't true!** ←

Contents:

Core essentials to avoiding a job posting scam or phishing attempt:

1. Do not give your personal bank account, PayPal account, Zelle, Venmo, or other online payment account, or other credit card numbers to a new employer.
2. Do not agree to have funds or paychecks direct deposited into any of your accounts by a new employer – you should know them first. (Most employers give the option of direct deposit or a paycheck, and make these arrangements during your first day or week of *actual* employment, on site – not before.)
3. Do not forward, transfer, send by courier (e.g.: FedEx, UPS), or "wire" any money to any employer, for any employer, using your personal accounts(s).
4. Do not transfer money and retain a portion for payment.
5. Do not respond to suspicious and/or "too good to be true" unsolicited job/internship emails.
6. Do not respond to suspicious emails.
7. Unsolicited job offers are 99.99% a scam, unless from someone you actually know. But check!
8. Do not click on links or open attachments unless you trust the sender and the content.
9. Report phishing emails using the "report" function of your email system.
10. Solicitations via LinkedIn and other similar sites should be treated with care.

If you are ever concerned about a job or internship posting,
the Amica Center will help you research the posting.

How to identify a potentially fraudulent job or internship postings

Red Flags: The "employer" asks for, or posts….	But in truth,…
You must provide your credit card, bank account numbers, PayPal account, or other personal financial documentation.	**Legitimate opportunities will not ask for this kind of information on an application or via email or by phone.**
The posting appears to be from a reputable, familiar company (often a Fortune 500 Company). Yet, the domain in the contact's email address does not match the domain used by real representatives of the company.	**Legitimate recruiters are directly associated with the company for whom they work. Therefore, the email addresses used should match the company's domain.**
The contact email address contains the domain @live.com or uses "mail" in the domain name: joeybaloney@mail.targat.com	**The email should always come from an official email address that reflects the organization's domain or a subsidiary of the organization. Employer email addresses from Gmail, Yahoo!, etc., all suggest the employer does not have an official company domain and may not be a legitimate enterprise; research is required to verify status. NOTE: It is possible a small company simply has not purchased a domain. To check, go to the state public corporate database (where they filed to be a company) and check their legal status and contact info.**
The "employer" is using a personal email address instead of a company email address	**Same as above – the email should be associated with the company. Employment communications are always official – so why not use an official email address?**
You get an email or text that says they were going to send a check through the mail but there were several delivery failures by the courier, and they now need to send payment electronically, asking for your banking information to do so.	**Sounds transparent, BUT: The mail = USPS, not a courier service (DHL, FedEX, etc.). Plus, why use a courier when it only costs a stamp? (USPS likes to investigate mail fraud…). Sending a check via a courier is designed to make you feel special. Asking for your bank information because of "delivery failures" is a ploy, designed to take advantage of your trust.**
You are asked to forward payments, by wire, courier, bank transfer, check, or through PayPal…	**This is a clear red flag. Never forward payments – they want to access your bank account(s) and your money!**
The position requires an initial investment, such as a payment by wire service or courier (EX: UPS, FedEx, DHL).	**Legitimate opportunities never ask for an initial investment. Never! Some network marketing companies may ask you to pay a fee (or "pay a deposit") to obtain their sample product for demonstration. We do not post such positions.**

	When they are asking for money so you can have a job/internship, this is a clear red flag.
The "company" website is not active, does not exist, or re-routes users to another website unaffiliated with the "company," even though the "employer" listed a URL or website in the job/internship announcement	**This is a significant red flag because if they listed the website and it is not working or does not exist, or if the URL goes to another unassociated website, then the employment opportunity is most likely not real.**
The posting includes many spelling and grammatical errors.	**If the employyr kant spel, du u reely wanna werk 4 them? Poor spelling and grammar suggests the job/internship announcement was written by a non-professional and therefore the opportunity is probably not a legitimate.**
A high salary or wage is listed for a job that requires minimum skills	**This is designed to entice you, to get you to apply. Think wisely – how many legitimate companies can afford high wages for low skilled jobs? Why would they pay these wages? Think critically!**
The position states you will be working from home* *Newer work arrangements, because of the pandemic, have made remote work much more common. Learn to differentiate legitimate opportunities from scam opportunities.	**This is a red flag because most formal jobs have you working at an office or out of an office, using the office as your base. "Working from home" may be one of those "convenience hooks" that takes advantage of people who want an easy job situation because of their busy schedules.** **COVID-19 has ushered in remote/virtual work options, so working from home may be legitimate. You may be a "1099 independent contractor" rather than a regular "W2" employee - meaning – you will be responsible for all your tax liabilities. Always carefully research these jobs.**
Flashy responses to COVID-19	**With Covid-19 now a reality, more opportunities are being offered remotely. Scammers are taking advantage of this situation and they know students need money. Some are using flashy, eye-catching marketing techniques to draw attention. Be very careful and fully vet remote/virtual opportunities and the organizations that present them.**
Key terms and phrases are used that suggest access to the top level of company management and you are a student (examples: CEO, Co-founder, CFO, COO, etc.)	**It is possible selected candidates will have access to top level management personnel of a company, but typically this does not happen when you are a student. The times it does happen is when there is a specific management training program, for example, that is designed to have C-level leaders meet future leaders within the company. These programs are formalized and have printed documentation (brochures, part**

	of the recruiting materials, etc.) Just so you know: even seasoned employees often have infrequent access to the top. Some fraudulent job postings entice applicants with such lofty access – it sounds so good! Exception: very small start-ups, where the CEO is also the accountant, the coder, and the custodian, and…
The job/internship is for a start-up business, a new small private company, and entrepreneurial enterprise just getting off the ground…	**These are red flags simply because new business efforts are used by scam artists as an exciting creative hook – because you get to be in "on the ground level." These may be very legitimate opportunities – you just have to research them very carefully.**
The position initially appears as a traditional job...but upon further research, it sounds more like an independent contractor opportunity.	**Independent contractor jobs ("1099 type self-employment") mean you will be self-employed and accountable for associated federal IRS and state tax obligations. You will not have benefits and are not really an employee of the company. A contract needs to be made with the parent company. No contract? Don't apply!**
You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).	**Stop! Legitimate employers do not need to use your bank account! This is an old scam with some new twists. Don't allow "employers" to use your bank account since these checks are often fraudulent and will bounce, leaving you to cover the consequences.** **In-home "check processing services" are a recent version of this scam.**
You receive an unexpectedly large check (checks are typically slightly less than $500, generally sent or deposited on Fridays).	**Remember this old and very true piece of wisdom: If it sounds too good to be true, then it probably is not true!!! These checks typically bounce –but you are held responsible for all the bank charges and any money you have used, wired, or processed.**
You are asked to provide a photo of yourself.	**In the United States, most legitimate jobs do not ask for a photo. Usually, the "employer" does not know this standard of practice in the US, indicating they are posting from another country.** **On some very special applications a photo may need to be attached – but this only happens with profession-specific jobs and is actually very rare. Be careful as photos can be used for selection reasons not associated with your skills, abilities, and knowledge. Example: acting, modeling, etc.**

The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys. Check Writing and Processing.	**It is not to say that every envelope stuffer job you come across is a fraudulent posting! However, these positions often offer flexible hours and pay -- and they may be after your information… Be Cautious!**
The posting neglects to mention what the responsibilities of the job actually are. Instead, the description focuses on the amount of money to be made.	**Legitimate employers will provide a good description of the job responsibilities and duties to see if you are a good fit for the position. The description should state the work location. They will do this openly and willingly. And any "employer" who hesitates…. Be careful!**
The employer responds to you immediately after you submit your résumé. Typically, résumés sent to an employer are reviewed by multiple individuals, or not viewed until the posting has closed. Note; this does not include an auto-response you may receive from the employer once you have sent your résumé.	**Legitimate employers take their time to sort through applications to find the best candidates. Fraudulent jobs are just looking for your personal information, not your skills, which is why they respond immediately. They are hoping an immediate response makes you feel special – a trick used to get you to share personal information.**
Watch for anonymity. If it is difficult to find an address, actual contact information, a name, the company name, etc. - this is cause to proceed with extreme caution.	**Fraudulent postings are despicable and are designed to take you in without you knowing you are being scammed, so the scammers will try to keep themselves well-hidden.**
The employer contacts you by phone, however, there is no way to call them back. The number is not available or disconnected.	**A legitimate business wants to be reachable for clients, business partners, and applicants -- so the number <u>will</u> be active!**
The company's website does not have an index that tells you what the site is about; or does not contain information about the job you are interested in. Scammers often create quick, basic web pages that seem legitimate at first glance, but lack real details and "depth."	**Legitimate organizations and companies will use their website to attract clients and customers, not just potential employees.** **Check the URL – is it a real company website?**
The employer tells you that they do not have an office in your geographic area and will need you to help them get a "new" office up and running	**Sounds exciting, right?! BUT - These postings often include a request for your banking information, supposedly to help the employer make transactions. What they want is access to your bank account and your money.**
You never applied to the job: a. but the employer asks personal information so they can complete a background check	**If you did not apply, then you are not an actual candidate of the legitimate company. (One has to apply to a job to be a candidate.)** **a. Never give personal information unless you applied and this is a next step in the application**

b. yet the employer asks for an interview c. yet the employer claims "the job is yours!" d. and the employer claims they found you through the career center e. the employer says they found you through Handshake	**process (typically, background check requests occur on-site)** **b. If you didn't apply, why would you interview?** **c. Again – if you didn't apply…** **d. The Amica Center does not send out student resumes. We don't share student information.** **e. This is possible, if you make your profile public and available for searches. Check your settings.**
Google the employer's phone number, fax number and/or email address. Checked LinkedIn to see if they are listed. If it does not appear connected to an actual business organization, this is a red flag.	**You can use the Better Business Bureau (http://www.bbb.org/us/consumers/), and AT&T's Anywho (http://www.anywho.com/) to verify organizations.** **Come into the Amica Center – we have other resources, too!**

The old adage is very useful:

If it looks too good to be true, then it probably isn't true!

If you are ever concerned about a job or internship posting, the Amica Center will help you research the posting. Come in or call: 401-232-6090

Phishing – What You Need to Know

Phishing is a type of scam used to trick you into divulging sensitive information. Scammers will typically pose as a legitimate company or internal entity in order to steal financial information, account credentials, or personal information.

Below is an email from Bryant's Information Services notifying users about a phishing attempt. Notice how tricky the scammer was – posing as Bryant's Helpdesk and asking for login credentials. The email was clearly a scam.

A number of people have reported receiving messages from the Bryant Helpdesk (helpdesk@bryant.edu) with the subject line: **Irregular Activity Detected- Duo Security Upgrade Required Immediately request: 47291**

These messages are asking the user to reply and supply their user name, password and email address.

These messages **ARE NOT** from Bryant's Helpdesk. If you hit reply, you will see the address the reply is being sent to is help.desk@tech-center.com

If you receive one of these messages, please delete it and do not reply!

If you have any questions, please contact the Campus Technology Services (CTS) support centers as follows:
Faculty/Staff: Helpdesk x6111 or via email at helpdesk@bryant.edu

Students: Laptop Central x6550 or via email at laptopcentral@bryant.edu

Thank you,
Bryant Information Services

Some Common Signs of Phishing

1. You receive an unexpected email from an unknown sender (a person or organization)
2. You receive an email from someone you know but the content makes no sense:
    a. Not their kind of work
    b. Asking for info that's not their business
    c. Asking you to reveal login credentials or personal information
    d. Seems just plain odd
3. You receive an email that conveys a high urgency, urging you to act now
    a. Because the "opportunity" will go away within a short period of time
    b. Because others are also competing against you and they may "win"
    c. Because your social security number has been compromised
4. You receive an email that threatens you if you don't act now
    a. They claim your "account" will be locked if you don't reply
    b. They claim they'll have you arrested if you don't reply
5. You receive an email saying you won money and you need to claim now or it'll be given away
6. You receive an email asking you to claim part of an inheritance
7. The email contains an unexpected attachment, prompting you to enable the macros
8. Website links or email addresses contained in the email look almost right

Researching Possible Scams

Research the company to see if they are legitimate. Many people check companies through websites like the state's business office, Better Business Bureau, local Chambers of Commerce, and other listings.

Example:

Rhode Island Corporate Database (use the state where the business claims to be based): **http://business.sos.ri.gov/CorpWeb/CorpSearch/CorpSearch.aspx**

BBB: https://www.bbb.org/us/consumers/

Chambers of Commerce: https://www.uschamber.com/chambers/directory

ATT: https://www.anywho.com/

If you contact the company directly, you can ask if the person actually works there. Don't share personal information unless you are confident that the person and the company they work for are legitimate.

If you search the internet using key phrases, such as "fraudulent job postings" or "Scam job postings," you'll come up with many online articles and reports, such as:

https://toughnickel.com/scams-fraud/Job-Hunting--10-Red-Flags-that-the-Job-Post-in-Craigs-List-may-be-a-Scam

If you Google the company name with the word "scam" in the phrase (e.g., "ACME Inc scam"), you will get a variety of internet hits associated with the company. Know that some of the links that come up may be just chatter – but there may also be articles or references to actual scam activity.

Also try: https://www.ripoffreport.com for scam reports.

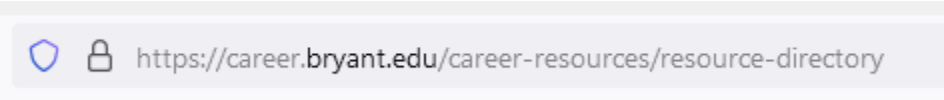
If you find a good research site for us to list or include in this booklet, let us know. Let us also know of any scam job postings you identify. Contact the Amica Center at: 404-232-6090

Protect Your Personal and Private Information

For job applications, you should not provide your credit card number, bank account number, PayPal account, social security number, or any PIN number over the phone or online.

Some job applications may ask you to provide your Social Security number and date of birth, but this information is not solicited over the phone or email. This information is typically a part of a formal job application that candidates complete on site and in writing, the day of their first in-person and on-site interview.

Always check to see if the URL: and site are secured. Looked for the "s" in :https://….." Also look for the protection icons preceding the URL:



Always know with whom you're sharing personal information -- and how it will be used. If someone asks for sensitive personal information, get the person's name, the company they work for and the phone number. If they get squirmy when you ask – something's up!

What to do if you discover you've been scammed

If you have encountered a fraudulent job posting, please contact the Amica Center at 401-232-6090 so we can remove the employer from the system.

You should immediately contact the Bryant University's Department of Public Safety at: 401-232-6001. DPS will work with you and determine if state police need to be involved.

If you have sent money to a fraudulent employer, you should contact your bank, credit union, and/or credit card company immediately to close the account and dispute the charges.

If the incident occurred completely over the Internet, you should file an incident report with the: http://www.cybercrime.gov/, by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357), or:

https://reportfraud.ftc.gov/#/

The list of red flags above and the comments and suggestions are not necessarily comprehensive and definitive; they are provided to assist you with your job search and to help you be aware of fraudulent and scam job postings.