



TIPS FOR AVOIDING JOB SCAMS

When you're looking for a job, you need to know the signs of a job scam. With more people using online job boards and looking for remote jobs, many scammers will spam email boxes with job opportunities. As much as we'd like them to, jobs do not fall from the sky. Job opportunities without a formal application process is a big, red flag.

If you receive an unsolicited email directly from an individual about a job, be cautious. Even if the person claims to be a faculty or staff member at MGA who wants to hire you, be cautious. You will only receive job emails from a staff member from the Center for Career & Leadership Development (CCLD), and our employers always want you to apply and interview before they offer a position. Faculty and staff who have opportunities in their departments will have their opportunities posted to the MGA HR Website, which also requires a formal application process. If an employer who uses Handshake is reaching out to you, it will come to your email box with the Handshake branding. Still not sure? Email us at careerservices@mga.edu, and we'll take a look at it with you.

When using a verified job board such as Indeed and even Handshake, most job announcements are the real thing, but you will occasionally find some that may not be legitimate, even on a verified job board. **Keep up with which boards you are using and be careful about the personal information you are submitting to these sites.**

Follow these tips and trust your instincts – if it sounds too good to be true, then it is! If you find something on Handshake that seems to be a scam, notify the CCLD immediately at careerservices@mga.edu.

Quick Tips for the Application Process

- Common red flags include unrealistic wages, multiple misspellings and grammar errors, email address with misspellings or incorrect domain, an email domain that doesn't match the website domain, and vague job information.
- Do not share your social security number, driver's license, passport, or other personal identification during the application/pre-hire process.
- Do not share your banking information. You should only set up direct deposit with an employer once you have accepted a job offer and have reported to your first day of work, in-person or remotely, at a legitimate business.
- Do not accept a job if you have never spoken to a representative over the phone, in person, or over video. Text or email-only communication is a big, red flag! For remote jobs, be extra cautious.
- If someone is willing to hire you by just having you email them, that's a huge red flag. A company that doesn't want to interview you before hiring you is too good to be true.
- If a company contacts you as soon as you apply, be cautious. And if you didn't apply and they are emailing you outside of a job applicant system like Handshake or others you are using, do not engage!
- Verify the company's location, products, and services.
- Be cautious if the application must be sent to a non-company email domain, especially for a large company.
- Not sure of something you have found and need advice? Email us at careerservices@mga.edu.

Beware of this Common Scam: Job postings for Personal Assistants who will need to run errands and deposit money in their personal banking account are popular. Even if they contact you with your school email, do not reply.

You should also research the organization and know the information below before interviewing and accepting a job:

1. Research the company website. After reading about them, can you articulate the programs, services, or products the organization provides? You can also use resources such as D&B Hoovers, accessible through the MGA Library's Databases at <https://app.hoovers.dnb.com/> while you are on campus. You can also search for companies, as well as real student, reviews about the company on Handshake.
2. How long has the company been in business?
3. What is the physical address of the company? Even an online company should have a physical address. Go one step further and do a Google search to see an image of the physical building.
4. Know who the company leadership is and do some research on them.
5. Have you spoken to your potential manager or other company representatives via phone (not texting) or video chat?

6. When you receive an offer, ask for it in writing. Be sure you understand the payroll schedule, salary, and benefits before you accept the position. If you have not had a face-to-face discussion yet, do not accept the job until you do.

Navigating Remote Opportunities

Many legitimate companies offer remote opportunities, but scammers will use remote jobs as a way to take advantage of job seekers. Plus, even for a remote job, a face-to-face video interview is standard. It's important to verify the legitimacy of the organization before you complete electronic paperwork and a face-to-face meeting is part of that verification.

The Truth about Remote Jobs: Remote jobs are very competitive because everyone wants them. If someone is willing to just give you a remote job without receiving a formal application from you and then interviewing you, it's not real. **No one should ask for your social security number, driver's license, or banking information as part of the application process.**

When an organization officially hires you after an interview, you will complete federal forms such as a W-4 and I-9. Then and only then should you share your social security number and driver's license number. Do not email this information. If you will be paid through direct deposit, the organization's human resources representatives should work with you to complete direct deposit information. **Never email your banking information.**

If the job is remote, they should have a secure process for verifying your federal and state identification information and for collecting your banking information for direct deposit.

Not a Scam, but Something Seems Off

Sometimes a job or the person you're interacting with about a job just doesn't seem ethical. Trust your instincts and walk away from the situation. If you encounter someone like this on Handshake or at an MGA campus recruiting event, contact us at careerservices@mga.edu as soon as possible.

What if You are Already Involved in a Scam?

According to the Federal Trade Commission (FTC), someone involved in a job scam should follow these steps:

- File a complaint with the FTC at <https://www.ftccomplaintassistant.gov/#crnt&panel1-1>. They currently have a specific complaint process for Covid-19 scams.
- You should contact the local police so that they can conduct an investigation. **If you are a current student, you may file a report with the MGA University Police at 478-471-2414.** You can also use the Report-A-Crime form online - <https://www.mga.edu/police/report-a-crime.php>.
- If you sent money to a fraudulent employer, contact your bank or credit card company immediately to close the account and dispute the charges
- You should contact the three major credit reporting companies to place a flag on your credit reports regarding suspicious activity.