# Stay Alert: How to Spot Scam Recruiters on LinkedIn & Job Boards

As you begin networking and applying for new opportunities, it's important to stay alert for fake recruiters, phishing attempts, and job scams, especially on LinkedIn, email, and text message outreach. Legitimate recruiters and employers should always be able to provide clear company information, a real job description, and a professional hiring process.

## Red Flags to Watch For

### Unprofessional Email Addresses

Be cautious if a recruiter reaches out from a personal or generic email such as:

- Hotmail
- Gmail
- Yahoo
- AOL
- Outlook.com

A legitimate recruiter usually emails from a company domain, for example:
name@company.com
name@staffingfirm.com

While there are occasional exceptions for independent recruiters, they should still have a professional website, LinkedIn presence, and company branding.

### They Won't Tell You the Company Name

A real recruiter should be able to provide:

the organization name
a company website link
the hiring manager or department context
why your background aligns
a formal written job description

If they avoid sharing this information, stay cautious.

### Requests for Money = Immediate Red Flag
### Never pay anyone for:

- resume reviews
- LinkedIn changes
- interview access
- guaranteed job placement
- background checks upfront
- training before employment
- equipment deposits
- software downloads

A legitimate recruiter or employer will never ask you to pay to be considered for a role.

# Pressure to Move Too Fast

Be cautious if they:

- rush you into providing personal information
- ask for your Social Security number too early
- request banking information before an offer
- pressure you to accept immediately
- avoid formal interviews
- only communicate by text or WhatsApp

A real hiring process includes:

- recruiter screen
- formal interview(s)
- clear job details
- written offer
- onboarding paperwork after acceptance

# Poorly Written Messages

Scam outreach often includes:

vague job titles
unrealistic pay
poor grammar
no mention of why you were selected
copy/paste generic outreach
“remote work from home data entry” offers with unusually high pay

If the message feels generic and does not reflect your actual background, be cautious.

# Verify the Recruiter Profile

Before responding, check:

- do they have a real LinkedIn profile?
- does the company page exist?
- are there legitimate followers/employees?
- do they have mutual connections?
- does their work history make sense?
- do they post real content?

If something feels off, trust your instincts.

# Final Safety Reminder

If something feels rushed, secretive, overly flattering, or too good to be true, pause before responding.

Your experience is valuable, and legitimate employers will respect a professional and transparent process.

**Reach out with any questions:**

Ashley Millan | ALM@theaceconsultinggroup.com | 312-868-0948 | Cell: 708-800-8275